ЦЕНТРАЛЬНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Збірник праць молодих науковців ЦНТУ

Випуск 10

Кропивницький – 2020

ЦЕНТРАЛЬНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Збірник праць молодих науковців ЦНТУ

Випуск 10

Кропивницький – 2020

Збірник праць молодих науковців ЦНТУ. – Вип. 10. – Кропивницький: ЦНТУ, 2020 – 857 с.

Збірник праць молодих науковців складається зі змісту, статей та тез студентів та магістрантів по матеріалам дипломних робіт.

Рекомендовано до друку Науково-технічною радою Центральноукраїнського національного технічного університету, протокол № 6 від 25.06.2020

РОЗДІЛ І

УДК 336.7

Ю. Андріюк, магістр гр. ФС-18МЗ
Центральноукраїнський національний технічний університет

ТЕОРЕТИЧНІ АСПЕКТИ УПРАВЛІННЯ ЛІКВІДНІСТЮ КОМЕРЦІЙНИХ БАНКІВ

У статті проаналізовано основні теоретико-методологічні особливості управління ліквідністю банків в сучасних умовах. Визначено поняття, суть та значення ліквідності для банків, необхідність її регулювання та управління. Зазначено основі принципи, якими має керуватися у своїй діяльності банк, щоб запобігти надмірному підвищенню ризику ліквідності. Підсумовано, що ліквідність комерційного банку здебільшого визначається такими якісними чинниками, як структура та стабільність ресурсної бази і структура та якість портфеля активів.

банківський менеджмент, управління, ліквідність, завдання, принципи, зобов'язання, банк, активи, пасиви, власні та залучені кошти, ресурси банку, ресурси-витрати, відсотковий ризик і ризик ліквідності, кредитний та ринковий ризики, регулятивні вимоги щодо управління пасивами банків.

Постановка проблеми. За останні роки докорінним чином змінилися погляди на банки та банківську діяльність. З одного боку, це пояснюється змінами умов функціонування банків, а з другого, - дедалі очевиднішими стають процеси інтеграції банківських систем, посилення фінансової конкуренції, розвиток інформаційних технологій та висока волатильність фінансових ринків. А такі фактори, як відсутність достатньої кількості платоспроможних позичальників, альтернативних кредитуванню напрямів інвестування коштів, недостатній рівень довіри суб'єктів економіки до банківської системи, ставлять перед вітчизняними банківськими установами надзвичайно складні завдання. Особливо це стосується вдосконалення процесів управління банківською ліквідністю на всіх її рівнях. Адже втрата банком своєї ліквідності може стати причиною втрати банком коштів, призвести до проблем у фінансово-господарській діяльності чи навіть банкрутства клієнтів банку.

Аналіз досліджень і публікацій. Дослідженням питань ліквідності комерційних банків, вивченням підходів до її регулювання та управління займалися такі відомі науковці, як А. М. Герасимович, М. І. Савлук [1], А. М. Мороз, М. Ф. Пуховкіна [2], Л. О. Примостка [3], Дж. Ф. Сінкі, Е. Дж. Долан, П. С. Роуз, О. І. Лаврушин [4], М. М. Ямпольский. Аналіз опублікованих практичних напрацювань з цього питання дають змогу зробити висновок про те, що в умовах фінансово-економічної нестабільності регулювання та управління ліквідністю є життєво важливим для забезпечення ефективної банківської діяльності.

Формулювання цілей статті. Головними цілями статті є теоретичне обґрунтування поняття, необхідності та значення ліквідності, розширення системи заходів з регулювання та управління ліквідністю банків.

Виклад основного матеріалу дослідження. Ліквідність банку - це його здатність швидко і в повному обсязі задовольняти невідкладні потреби у грошових коштах. Найбільший попит на ліквідні засоби виникає у банків з двох основних причин:

- через зняття клієнтами коштів зі своїх рахунків;
- надходженням кредитних заявок, які банк вирішує задовольнити [5, с. 588].

Поняттю «ліквідність комерційного банку» у спецлітературі даються різні визначення. З одного боку, ліквідністю вважається здатність банку виконувати свої

зобов'язання у визначений термін [1-2]. Причому це стосується не тільки повернення вкладених коштів та виплати відповідного відсотка, але й з видачі кредитів. Деякі автори пропонують визначення ліквідності як здатності банку виконати свої зобов'язання перед клієнтами з урахуванням майбутнього вивільнення коштів, вкладених в активні операції, і можливих позик на грошовому ринку [3-5].

З іншого боку, під ліквідністю розуміють співвідношення сум активів і пасивів з однаковими термінами [6, с. 709]. Також ведеться мова про більш ліквідні і менш ліквідні активи банку з позиції можливості швидкого перетворення їх у кошти. В інструктивних матеріалах НБУ ліквідність банку трактується як здатність банку забезпечити своєчасне виконання своїх грошових зобов'язань, яка визначається збалансованістю між строками і сумами погашення розміщених активів та строками і сумами виконання зобов'язань банку, а також строками та сумами інших джерел і напрямів використання коштів (надання кредитів, інші витрати) [7-9].

Таким чином, ліквідність комерційного банку означає його можливість вчасно й повно забезпечувати виконання своїх боргових та фінансових зобов'язань перед усіма контрагентами, визначається наявністю достатнього власного капіталу банку, величиною та оптимальним розміщенням коштів за статтями активу та пасиву балансу з урахуванням відповідних строків.

Ліквідність тісно пов'язана (а іноді і змішується) з поняттям платоспроможності, яке тлумачиться як здатність банку своєчасно і в повному обсязі відповідати за своїми зобов'язаннями. Ліквідність банку значною мірою визначає його платоспроможність, яка залежить і від ряду інших чинників, таких як розмір капіталу, спеціалізація та диверсифікація банківських послуг, загальний рівень ризиковості діяльності, співвідношення власних і залучених коштів.

Сутність проблеми ліквідності полягає в тому, що попит на ліквідні засоби рідко дорівнює їх пропозиції в будь-який момент часу, тому банк постійно має справу або з дефіцитом ліквідних коштів, або з їх надлишком.

Дефіцит ліквідних засобів призводить до порушення нормативних вимог центральних банків, штрафних санкцій і, що найнебезпечніше для банку - до втрати депозитів.

Система управління ризиком ліквідності в українських банках найчастіше передбачає існування трьох рівнів:

– стратегічне управління ліквідністю здійснюється шляхом розробки фінансового плану на поточний рік у частині структури депозитної бази та рівня дохідних активів;

– тактичне управління ліквідністю, що здійснюється Комітетом управління активами та пасивами. На нарадах якого аналізується поточний стан ліквідності банку, структура активів та пасивів за строками до погашення, сталість залишків на поточних рахунках клієнтів, ситуація на фінансових ринках та її вплив на ліквідність банку;

– оперативний менеджмент ліквідності здійснюється щоденно управлінням ризиків шляхом приведення у відповідність поточних виплат та надходжень банку, визначення щоденної потреби в ліквідних коштах та вибір раціональних джерел їх поповнення для прийняття обґрунтованих управлінських рішень [1, с. 462].

Так можна виділити основні завдання оперативного управління ліквідністю:

– контроль за дотриманням обов'язкових нормативів ліквідності;

– визначення планового періоду дія оцінювання потреб ліквідності;

– розподіл планового періоду на інтервали згідно з термінами виконання активів та зобов'язань;

– групування активів і пасивів банку за термінами;

– прогнозування обсягів та строків проведення активних і пасивних операцій банку в межах обраного періоду;

– обчислення розриву ліквідності (фактичного та прогнозованого) у кожному із зафіксованих інтервалів;

– обчислення сукупного (кумулятивного) розриву ліквідності протягом планового

періоду;

– складання плану дій у разі виникнення дефіциту або позитивного сальдо ліквідності;

– моніторинг ліквідної позиції банку [3, с. 146].

Ефективна система управління має постійно забезпечувати достатній рівень ліквідності за мінімальних витрат, тому набуває важливого значення застосовуваний банком інструментарій управління ліквідністю, зокрема методи оцінювання потреби в ліквідних коштах, доступність джерел їх поповнення для кожного банку, стратегії управління ліквідною позицією. Отже, у цій ситуації актуальним є питання управління ризиком ліквідності.

Ризик ліквідності – це ризик того, що банк не зможе виконати свої зобов'язання за виплатами при настанні строку їх погашення у звичайних або непередбачених умовах. Ризик ліквідності включає неможливість управляти незапланованим скороченням або змінами в джерелах фінансування. Ризик ліквідності також виникає внаслідок нездатності розпізнати або врахувати зміни кон'юнктури ринку, які впливають на здатність швидко реалізувати активи з мінімальною втратою їх вартості [10, с. 29].

Надмірна ліквідність породжує дилему «ліквідність – прибутковість», адже найбільш ліквідні активи не генерують доходів. Якщо фактична ліквідність значно перевищує необхідний рівень або встановлені нормативи, то діяльність банку негативно оцінюється акціонерами з погляду не повністю використаних можливостей для отримання прибутку [11, с. 633]. Імовірність настання ситуації невідповідності між попитом і пропозицією ліквідних коштів називають ризиком незбалансованої ліквідності. Очевидно, що ризик ліквідності майже завжди супроводжує банківську діяльність.

Управління ліквідністю спрямоване на досягнення достатнього рівня ліквідних активів та підтримку диверсифікованої ресурсної бази, а також на дотримання банківського законодавства та нормативно-правових актів щодо управління ризиком ліквідності [1, с. 463].

З огляду на винятково важливу роль ліквідності в життєдіяльності банків та підтримці рівноваги банківської системи в цілому в багатьох країнах органами банківського нагляду та законодавством передбачено встановлення норм ліквідності. Банки зобов'язані підтримувати показники ліквідності не нижчими від певного рівня (норми), що визначається з урахуванням нагромадженого досвіду та конкретних економічних умов у країні. Такий метод спрямований насамперед на здійснення контролюючої функції за станом ліквідності комерційних банків, але іноді спонукає керівництво банків до послаблення уваги до даної проблеми і сприйняття її не як власної, а такої, що може бути вирішена через втручання центрального банку і надання стабілізаційних кредитів [12, с. 28]. Як показує зарубіжний і вітчизняний досвід, така позиція є глибоко помилковою і призводить здебільшого до трагічних наслідків, коли банк перестає існувати. Після втрати ліквідності відновити репутацію банку та довіру до нього з боку клієнтів практично неможливо.

У багатьох зарубіжних країнах, показники ліквідності банків розраховуються за співвідношенням активних і пасивних статей балансу, згрупованих за строками, і є обов'язковими для виконання всіма банками (Японія, Франція, Великобританія, Росія, Німеччина) [6, с. 711]. Проте, у деяких країнах, наприклад у США, немає обов'язкових нормативів ліквідності, і банки самостійно вирішують дану проблему. Але органи банківського нагляду постійно здійснюють контроль за станом ліквідності і оцінюють якість управління нею в ході перевірок на місцях за рейтинговою системою «CAMEL», де ліквідність розглядається як один з найважливіших показників діяльності.

Централізований підхід до регулювання банківської ліквідності використовується і Національним банком України через встановлення обов'язкових нормативів [7].

НБУ обрав шлях поступової децентралізації процесу управління ліквідністю банків. Якщо на етапі формування банківської системи регулювання здійснювалось через встановлення ряду економічних нормативів ліквідності, якими визначались як суми, так і строки залучення та розміщення коштів (до одного місяця, до трьох місяців), то в даний час

відповідність строків регулюється банками самостійно, а кількість обов'язкових нормативів ліквідності скоротилась до трьох.

Управління банківською ліквідністю варто розглядати як складний багатоетапний та безперервний процес, що є сукупністю підходів і методів, за допомогою яких здійснюють діагностику та планування ліквідності (через аналіз та коригування внутрішніх чинників) і тому досягається оптимальне співвідношення між активами та зобов'язаннями за обсягами, термінами та валютами, що дає змогу банкам обмежити рівень ризику незбалансованої ліквідності та досягти максимізації прибутковості за умов обов'язкового дотримання її нормативів [14, с. 79].

З банківською ліквідністю пов'язане широке коло питань, які не можуть бути вирішені лише встановленням мінімальних вимог до рівня ліквідних коштів. Додержання нормативів є необхідною, але не достатньою умовою ефективності процесу управління ліквідністю. Ефективна система управління має постійно забезпечувати достатній рівень ліквідності при мінімальних витратах, тому важливе значення мають методи управління ліквідністю, методи оцінювання потреби в ліквідних коштах та доступність джерел їх поповнення для кожного банку. Вибір найприйнятніших підходів до управління ліквідністю залишається прерогативою керівництва банку і залежить від ряду внутрішніх та зовнішніх чинників [15, с. 414].

У процесі управління перед менеджментом кожного конкретного банку постають завдання глибокого розуміння сутності проблем ліквідності, пошуку оптимальних методів управління, організації адекватних систем контролю та оцінювання потреб у ліквідних засобах, забезпечення доступних джерел їх поповнення, створення власних систем управління ліквідністю.

Вирішуючи зазначені завдання, необхідно враховувати не лише можливості банку та потреби клієнтури, а й такі чинники, як політична та економічна ситуація в країні, стан грошового ринку, наявність та досконаліть законодавства, надійність клієнтів та партнерів, рівень ризиковості банківських операцій, розвиток ринку цінних паперів, компетентність фахівців тощо. Для вітчизняних банків процес створення ефективних систем управління ліквідністю ускладнюється кризовими явищами в економіці, недостатнім рівнем кваліфікації та досвіду банківських кадрів.

Щоб запобігти надмірному підвищенню ризику ліквідності, менеджмент банку має керуватися у своїй діяльності такими принципами:

– пріоритетність ліквідності, у тому числі й при виборі напрямків розміщення коштів;

– постійність аналізу потреб банку в ліквідних засобах з метою уникнути як їх надлишку, так і дефіциту;

– планування та прогнозування дій банку в разі виникнення незбалансованої ліквідності та кризових ситуацій;

– взаємозв'язок ризику ліквідності з іншими сферами діяльності, такими як залучення та розміщення коштів, а також управління ризиком відсоткових ставок [1, с. 468].

Стан ліквідності комерційного банку здебільшого визначається такими якісними чинниками, як структура та стабільність ресурсної бази і структура та якість портфеля активів.

Хоча ризик ліквідності може виникнути внаслідок проведення активних операцій, але більша частина проблем ліквідності виникає за межами банку і пов'язана з його клієнтами. Ризик ліквідності клієнтів трансформується в ризик ліквідності банку.

Процес управління ліквідністю має включати постійний аналіз ресурсної бази з погляду стабільності та ймовірності зняття клієнтами коштів зі своїх рахунків. Результати аналізу структури, динаміки та рівня стабільності депозитної бази можуть бути екстрапольовані на майбутнє і використані при оцінюванні потреби в ліквідних активах, які банк має підтримувати, щоб знизити ризик ліквідності.

З метою підтримки фінансової стабільності та підвищення стійкості банківської системи до можливих шоків ліквідності Правлінням НБУ 15 лютого 2018 року затверджено

новий пруденційний норматив для українських банків – коефіцієнт покриття ліквідністю або LCR (англ. Liquidity Coverage Ratio) – це співвідношення високоякісних ліквідних активів банку до суми, необхідної для покриття підвищеного відтоку коштів з банку протягом 30 днів. Він відображає рівень стійкості банку до короткострокових шоків ліквідності – характерного для кризових періодів явища, коли відбувається значний відтік коштів клієнтів [7].

Виконання нормативу свідчитиме, що банк забезпечений ліквідністю в обсязі, достатньому для повного виконання ним зобов'язань протягом 30 днів в кризових умовах. Враховуючи значний рівень доларизації української банківської системи, банки повинні будуть дотримуватися нормативу LCR як у національній, так і в іноземних валютах.

Наразі банки готові до впровадження LCR, враховуючи наявний структурний надлишок ліквідності у банківському секторі та високу дохідність державних цінних паперів, які входять до складу високоякісних ліквідних активів.

Висновки. На даний момент для економіки України особливо актуальною є проблема забезпечення ліквідності банківських установ.

Ліквідність надзвичайно важлива для банків, як складова фінансової стійкості. Кожен банк для забезпечення своєї стабільності має бути впевненим, що у будь-який момент зможе задовольнити потреби своїх кредиторів і позичальників. Для цього йому потрібно підтримувати відповідність між активними та пасивними статтями балансу, між строками повернення кредитів та строками закінчення депозитів. Усі ці процеси включає система управління ліквідністю банку. Стабільне функціонування та подальший розвиток банків залежить від здатності банку організувати ефективне регулювання та управління ліквідністю. Від належного управління ліквідністю залежить не лише спроможність банку розраховуватись за своїми зобов'язаннями, але і задовольняти існуючий попит на ресурси для здійснення активних операцій. Крім того, дотримання встановлених вимог ліквідності є основним свідченням надійності банківських установ, а, отже, і їх ділової репутації.

Щоденна робота з підтримки достатнього рівня ліквідності є неодмінною умовою самозбереження і виживання банків та забезпечує їх стійкість та стійкість банківської системи загалом. Без якісного управління банківські установи не зможуть надавати послуги щодо обслуговування фізичних і юридичних осіб, належним чином здійснювати кредитну та інвестиційну діяльність, тому підтримка ліквідності повинна мати найвищий пріоритет у роботі менеджменту банків. Раціональне управління залученими коштами створює умови для підтримання відповідного рівня ліквідності банків та довіри клієнтів, а отже і впевненість у власній фінансовій стійкості та і забезпечення фінансової стійкості банківської системи в цілому.

Список літератури

1. Аналіз банківської діяльності: Підручник / А.М. Герасимович, М.Д. Алексеєнко, І.М. Парасій-Вергуненко та ін.; За ред. А.М. Герасимовича. - К.: КНЕУ, 2004. - 599 с.
2. Банківські операції : підручник /за ред. А.М. Мороза. - К. : КНЕУ, 2008. - 384 с.
3. Примостка Л.О. Фінансовий менеджмент у банку: підруч.; 2-ге вид., доп. і перероб. / Л.О. Примостка. - К.: КНЕУ, 2004. - 468 с.
4. Банковская система в современной экономике: монография / [под ред. О. И. Лаврушина]. - М.: КНО- РУС, 2013. - 800 с.
5. Катан Л.І. Управління ліквідністю комерційних банків / Л.І. Катан, Ю.С. Марченко // Молодий вчений. - 2017. - № 5 (45). - С. 588-591.
6. Кочетигова Т.В. Зарубіжний досвід управління ліквідністю комерційного банку / Т.В. Кочетигова, Д.С. Кожухар // Глобальні та національні проблеми економіки. - 2016. - Вип.11. - С. 709-712.
7. Інструкція про порядок регулювання діяльності банків в Україні: постанова Правління Національного банку України від 28.08.2001 р. № 368 (зі змінами та доповненнями) [Електронний ресурс]. - Режим доступу: http://zakon5.rada.gov.ua/laws/show/z0841-01
8. Положення про надання Національним банком України стабілізаційних кредитів банкам України // Постанова Правління НБУ від 13.07.2010 р. № 327. [Електронний ресурс]. - Режим доступу: http://zakon2.

rada.gov.ua/laws/show/z0540-10
9. Про затвердження Положення про застосування Національним банком України стандартних інструментів регулювання ліквідності банківської системи: Постанова Правління НБУ від 17.09.2015 р. № 615. [Електронний ресурс]. - Режим доступу: http://zakon5.rada.gov.ua/laws/show/v0615500-15
10. Тарасевич Н.В. Управління ліквідністю банку в сучасних умовах / Н.В. Тарасевич, В.О. Матвієнко // Наукові дослідження розвитку світової економіки: пропозиції, теорії: збірник наукових праць з актуальних проблем економічних наук. - 2015. - Ч. 2. - С. 29-35.
11. Литвинюк М.В. Ліквідність банку та банківської системи як показник ефективності діяльності банку та її вплив на прибутковість комерційного банку / М.В. Литвинюк, В.І. Давиденко // Економіка і суспільство. - 2017. - Вип. 10. - С. 631-636.
12. Євенко Т.І. Управління ліквідністю банківських установ / Т.І. Євенко // Економічний часопис-XXI. - 2013. - № 1-2. - С. 27-30.
13. Значення економічних нормативів по системі банків України: Офіційний сайт Національного банку України [Електронний ресурс]. - Режим доступу: https://bank.gov.ua/control/uk/puЬlish/artide?artJd=34661442&cat_ id=34798593
14. Хіміч Н.О. Управління ліквідністю комерційних банків України в умовах нестабільності фінансових ринків / Н.О. Хіміч // Регіональна економіка. - 2008. - № 3. - С. 76-83.
15. Фатюха В. Удосконалення методів управління ліквідністю комерційного банку/В. Фатюха, О. Самченко // Економічний аналіз. - 2011. - Вип.8. - С. 413-415.

УДК 331.08

К. Бакума, магістр гр. ПА(АДМ)-18МЗ
Центральноукраїнський національний технічний університет

СУЧАСНІ ТЕХНОЛОГІЇ УПРАВЛІННЯ ПЕРСОНАЛОМ В СИСТЕМІ БАНКІВСЬКОГО МЕНЕДЖМЕНТУ

Визначено сутність поняття технологія управління персоналом банківської установи. Систематизовано та розкрито зміст сучасних технологій управління персоналом банків.
технології управління персоналом, банківський менеджмент, HR-менеджмент, ефективність.

Постановка проблеми та її актуальність. Банківські установи сьогодні працюють у динамічному непередбачуваному середовищі, яке створюється нестабільними ринковими відносинами, нестійкими політичними, економічними та соціальними процесами. Необхідність вирішення численних проблем адаптації банків до економічних, науково-технічних, технологічних, інформаційних і соціальних змін в суспільстві спонукає менеджерів до впровадження ефективних технологій управління надійністю персоналу банку. Сьогодні кожному HR-менеджеру, який намагається ефективно використовувати людський потенціал важливо розуміти призначення технологій управління персоналом та їх типологію. Це вагомий та дієвий інструмент ефективного управління персоналом та основна складова системи банківського менеджменту.

Аналіз останніх досліджень і публікацій. Теоретичні та практичні аспекти побудови ефективної системи менеджменту персоналу є об'єктом розгляду у працях таких вчених, як: О. Ареф'єва, Т. Базаров, З. Варналій, О. Грішнова, Г. Десслер, М. Єрмошенко, О. Кириченко, О. Ляшенко, Н. Мехеда, Г. Назарова, Н. Підлужна, І. Чумарін, Н. Швець та ін. Зростання впливу людського фактору на діяльність банківських установ обумовило необхідність пошуку сучасних шляхів підвищення ефективності використання персоналу.

Цілі статті. Метою статті є визначення місця управління персоналом в системі банківського менеджменту та оцінка ефективності технологій управління персоналом, які використовуються банківськими установами.

Виклад основного матеріалу. Різноманітні зміни в банківській системі та економіці загалом створюють потребу в нових управлінських знаннях, посилюють інтерес до системи формування персоналу з високими професійно-кваліфікаційними характеристиками, орієнтованого на досягнення кінцевої мети. Підготовка компетентного персоналу, здатного до продуктивної роботи, його раціональне структурне і просторове розміщення, зміна культури управління, врешті-решт, залежить від ефективності функціонування кадрової служби і є запорукою досягнення успіху банку.

Специфічною особливістю банківських установ є виключно важливе значення людських ресурсів для успішного їх функціонування. Банки, як правило, представляють собою крупні установи з точки зору чисельності працюючих у них. Крім того, фінансові та інформаційні ресурси надають лише тимчасову конкурентну перевагу. Історія розвитку банківської справи може навести багато прикладів розорення банків, що володіли значними фінансовими ресурсами, і навпаки, прикладів стрімкого злету невеликих банків. Визначальним фактором їхніх злетів та падінь були саме люди, банківські працівники. Тому можна сказати, що якщо в банку є ефективно діючий персонал, то він зможе залучити й фінансові кошти, отримати необхідну інформацію, і такий банк буде процвітати. Якщо ні - не допоможуть ніякі фінансові вливання.

Сучасні тенденції розвитку управління банківським персоналом спрямовуються на застосування різноманітних методів трудової мотивації, кадрової політики, корпоративної культури, шляхом актуалізації потреб, залучення працівників до участі в управлінні, прибутках, надання умов для розвитку особистості та реалізації творчого потенціалу.

Банківська стратегія управління персоналом, передбачає створення механізму ефективної кадрової політики, яка забезпечує: наближення інтересів банку до інтересів його працівників (і навпаки); об'єктивну та всебічну оцінку людських можливостей, доцільне використання їх у банку, створення умов для розвитку й реалізації трудового потенціалу персоналу, системи гнучкої адаптації працівників до кон'юнктури ринку; тісний взаємозв'язок форм стимулювання зі складністю та результативністю праці.

В умовах жорсткої конкуренції, що супроводжує розвиток ринкової економіки, необхідно постійно удосконалювати технологію управління, швидко оволодівати набутими в теорії та практиці знаннями, знаходити нові неординарні рішення у динамічній ситуації, враховувати специфічні особливості діяльності банківських установ. Лише такий підхід до управління забезпечує переваги у конкурентному середовищі.

Таким чином, банківський менеджмент – це управління банком в умовах ринку, що означає:

- орієнтацію банківської установи на попит і потреби ринку, на запити клієнтів і організацію таких банківських продуктів і послуг, які користуються попитом і спроможні забезпечити отримання запланованого прибутку;
- постійне прагнення до підвищення ефективності банківської діяльності з метою зменшення витрат і одержання оптимальних результатів;
- коригування цілей, завдань і програм банку залежно від кон'юнктури ринку;
- необхідність використання сучасної інформаційної бази (комп'ютерних мереж та зав'язків з валютною і фондовою біржами, іншими кредитно-фінансовими інструментами) з метою здійснення багатоваріантних розрахунків для прийняття обґрунтованих і оптимальних рішень;
- раціональний добір персоналу та впровадження ефективних технологій управління персоналом [1, с. 48-49].

Технологія управління персоналом банку визначається як хронологічно упорядкована сукупність дій або впливів на персонал, яка спрямована на забезпечення балансу інтересів, прагнень і мотивів працівників та цілей діяльності банківської установи. Базою технологій

управління персоналом є стимул працівника до праці, а способом спонукання до неї можуть виступати примус, маніпуляція, договір та зацікавленість. Технології управління персоналом можуть застосовуватися постійно, періодично або одноразово; вони можуть спрямовуватися на персонал банку в цілому, на окремі групи персоналу, на керівництво певного рівня або на окремих фахівців [2].

Сучасний організаційний процес управління персоналом в банківській системі України є трирівневим. На рівні Національного банку України функціонує департамент кадрової роботи, який формує концепцію, принципи, політику стратегії роботи з персоналом у банківській системі та здійснює методичну допомогу службам персоналу окремих банків. На другому рівні знаходяться організаційні структури служб персоналу комерційних банків, які координують та організаційно забезпечують реалізацію концепції, принципів, політики стратегії роботи з персоналом у власній системі. На третьому рівні знаходиться мережа відділень та філій банків, де практично розробляється та втілюється конкретна політика банку з управління персоналом [3].

На сьогодні найактуальнішими технологіями управління персоналом в банківській системі є наступні:

- технології позикової праці;
- навчальні технології;
- технології підбору та найму персоналу;
- технології підвищення ефективності роботи персоналу;
- технології контролю праці персоналу;
- інформаційні технології.

Щоб конкретно і наглядно зрозуміти особливості та складові кожної з вищезазначених груп управлінських технологій, їх характеристику представимо в таблиці 1.

Таблиця 1 – Характеристика технологій управління персоналом [4]

Технологія управління персоналом	Особливості технології	Підсистема управління персоналом
Персонал-технології позикової праці		
Лізинг персоналу	Форма тимчасового або строкового залучення персоналу, що дає змогу вирішити проблеми підприємства в умовах зміни пріоритетних напрямів діяльності; в умовах необхідності зменшення витрат на персонал, але потреба у ньому залишається. Залучення персоналу для тимчасової зайнятості	Аналіз та планування персоналу, підбір та наймання персоналу, організація трудових відносин, атестація та ротація персоналу
Аутсорсинг	Передача здійснюваних у межах підприємства завдань, функцій і процесів, зокрема деяких непрофільних функцій спеціалізованій компанії. Пов'язано це з тим, що окремі функції (інформаційні, маркетингові, фінансові тощо) працівники спеціалізованих компаній виконують краще	
Аутстаффинг	Співробітники, що раніше числилися в штаті компанії-замовника, переводяться в організацію, що надає послуги з аутстаффінгу, тобто дана організація оформлює у свій штат вже наявний персонал підприємства і стає формальним роботодавцем, що дає змогу вирішити питання тимчасового вивільнення працівників, для яких	

	на даний момент немає праці	
Навчальні персонал-технології		
Коучинг	Здійснюється методом безпосереднього навчання менш досвідченого працівника більш досвідченим в процесі їх взаємодії. Відбувається у формі наставництва, консультування. Ефективний інструмент персонального та особистісного розвитку, який сприяє розкриттю та реалізації внутрішнього потенціалу людини, й підвищення на цій основі ефективності праці.	Навчання та підвищення кваліфікації персоналу, мотивація персоналу
Персонал-технології підбору та найму персоналу		
Хедхантинг	Кадрові агентства здійснюють пошук висококваліфікованих фахівців вищої ланки з урахуванням особливостей діяльності замовника, вимог до кандидатів, робочого середовища, використовуючи прямі методи пошуку	Підбір та наймання персоналу, оцінювання персоналу
Рекрутинг	Кадрові агентства здійснюють пошук кваліфікованих фахівців середньої ланки з урахуванням вимог до особистісних та професійних якостей кандидатів, використовуючи наявні бази кандидатів й надаючи об'яви в ЗМІ	
Скрининг	Кадрові агентства здійснюють пошук необхідного допоміжного та обслуговуючого персоналу нижньої ланки, враховуючи формальні ознаки: стать, вік, освіту, досвід роботи тощо. Кадрові агентства отримують резюме кандидатів й віддають їх замовнику, який сам приймає рішення щодо відбору персоналу	
"Плетіння мереж" та прямий пошук	Консультант використовує власні зв'язки для пошуку кандидатури, у другому випадку – разом із замовникам визначається компанія, в якій може працювати необхідний працівник, з'ясовується його можлива посада, потенційним претендентам робиться ділова пропозиція	
Персонал-технології підвищення ефективності роботи персоналу		
Реінженіринг	Радикальна перебудова (перепроектування) бізнес-процесів підприємства для отримання істотних ефектів. Його використання може сприяти як підвищенню ефективності управління персоналом за рахунок удосконалення цього процесу, а також дасть змогу підвищити ефективність праці персоналу підприємства (підвищити її продуктивність, якість тощо)	Створення умов праці
Персонал-технології контролю праці персоналу		
Таємний покупець	Метод прихованого спостереження за роботою персоналом, яке проводить підготовлена особа в якості клієнта. Його використання дає змогу	Оцінювання персоналу, атестація та ротація

	встановити рівень дотримання працівниками правил і норм під час здійснення професійних обов'язків, стандартів обслуговування клієнтів, а також виявити компетентність персоналу	персоналу, мотивація персоналу
Інформаційні персонал-технології		
Автоматизована інформаційна система управління персоналом	Набір певного програмного забезпечення та технологій, використання яких дає змогу автоматизувати і вдосконалювати бізнес-процеси управління персоналом	Усі підсистеми управління
АРМ працівника	Професійно-орієнтований програмно-апаратний комплекс, який складається із технічних засобів автоматизації та організаційних форми їх експлуатації. АРМ забезпечує вирішення завдань працівника без- посередньо на його робочому місці	Правове та інформаційне забезпечення процесу управління персоналом, створення умов праці

У сучасних умовах триває процес розвитку та оновлення концепції управління персоналом, при цьому удосконалюються як технології управління персоналом, так і методи та інструменти, що використовуються. Працівник із його особистісними та професійними характеристиками від об’єкта управління перетворився в об’єкт вивчення з метою розробки та застосування таких технологій, які дадуть змогу створити найкращі умови для реалізації потенціалу працівників та максимального задоволення їх очікувань та потреб. З огляду на це, необхідна активізація використання сучасних персонал-технологій, які відповідають умовам бізнес-середовища, а також дають змогу вирішувати поточні питання трудової діяльності персоналу, вони сприяють підвищенню ефективності управління персоналом банківських установ.

Висновки. Отже, персонал є найбільш складним об’єктом управління банківської установи, оскільки, на відміну від інших об’єктів управління, персонал – це люди, які мають можливість самостійно приймати рішення, діяти, критично оцінювати пред’явлені вимоги, мають суб’єктивні інтереси та інше. Персонал є рушійною силою будь-якої банківської установи. Часто керівники вітчизняних банків основну увагу приділяють фінансовим та операційним питанням, проблемам матеріально-технічного забезпечення, не приділяючи при цьому достатньої уваги людям, які забезпечують роботу банку в усіх напрямках. Ці помилки занадто дорого обходяться і керівникам, і працівникам, які є частиною загального механізму управління. Без людей немає організації. Без висококваліфікованих фахівців жодна банківська установа не зможе досягти своєї мети і бути успішною. За таких умов, впровадження ефективних технологій управління персоналом в системі банківського менеджменту набуває першочергового значення.

Список літератури

1. Кириченко, О. Банківський менеджмент [Текст] : навч. посібн. [для студ. ВНЗ] / О. Кириченко, І. Гіленко, А. Ятченко. – К. : Вид-во "Основи", 2008. – 671 с. -ISBN 987-569-698-366-2
2. Лихолобов Е.А. Технології управління персоналом в контексті формування організаційної поведінки / Е.А. Лихолобов // Управління проектами та розвиток виробництва: Зб.наук.пр. – Луганськ: вид-во СНУ ім. В.Даля, 2011. – № 2(38). – С. 60-67. - Режим доступу: http://www.pmdp.org.ua/images/Journal/38/11leafop.pdf

3. Сушко Н. М. Менеджмент персоналу в банках: навч. посіб. [Електронний ресурс] / Н. М. Сушко. – К.: Центр учбової літератури, 2008. – 142 с. – Режим доступу : http://www.lib.nau.edu.ua/booksfornau/2008/Menedjment_personalu_v_bank-Sushko.pdf
4. Третьяк О. П. Сучасні персонал-технології у системі управління персоналом на підприємстві / О. П. Третьяк // Науковий вісник НЛТУ України. - 2014. - Вип. 24.4. - С. 389-397. - Режим доступу: http://nbuv.gov.ua/j-pdf/nvnltu_2014_24.4_66.pdf

УДК 021.6

В. Барабаш, магістр гр. ІС-18М
Центральноукраїнський національний технічний університет

ІНФОРМАЦІЙНІ РЕСУРСИ БІБЛІОТЕКИ ЗАКЛАДУ ВИЩОЇ ОСВІТИ: ОСВІТНЬО-ВИХОВНИЙ АСПЕКТ

У статті досліджено інформаційні ресурси бібліотеки ЗВО як джерело розвитку інтелектуального та духовного потенціалу студентства.
інформаційні ресурси, бібліотека ЗВО, бібліотечний фонд

Актуальність статті. У світі, де панує матеріальне, нависла загроза бездуховності. Справді, основою життя людини завжди були і мають залишатися одвічні людські цінності, серед яких: добро, любов, справедливість творчість, свобода та інші [1].

У цьому контексті незаперечним бачиться роль і місце бібліотек навчальних закладів загалом і бібліотек ЗВО зокрема, як чинника формування молодого покоління нашої держави.

Щороку в Україні, за експертними оцінками, кількість користувачів бібліотек ЗВО перевищує півтора мільйона осіб, які беруть у користування більше 105 млн. прим. різного роду документів, включаючи художні твори. Серед бібліотекарів нашої країни з вищою освітою понад п’ять тисяч осіб, разом з тим, 1700 працівників такої освіти не мають. Загальна кількість АРМ становить близько семи з половиною тисяч. Злагоджену роботу книгозбірень забезпечує одна з бібліотек столичних закладів вищої освіти України [9].

Мета статті. Дослідити потенціал документного ресурсу бібліотеки Центральноукраїнського національного технічного університету як джерела інформаційного та духовного розвитку студентства.

Розробкою питань, пов'язаних з особливостями діяльності бібліотек ЗВО, вивченням проблем формування та функціонування бібліотечних інформресурсів у різний час займалися вітчизняні та зарубіжні науковці, зокрема: Н. І. Апшай, І. О. Білоус, В. М. Белінська, Ю. М. Столяров, Р. Я. Ріжняк, Т. С. Юхновець та інші.

Бібліотека як основний культурно-інформаційний підрозділ університету великого значення надає придбанню та розповсюдженню культурних, духовних і етичних цінностей серед студентської молоді. Реалізується це на основі функцій бібліотеки вищого навчального закладу. Так, акумулююча функція передбачає накопичення та структуроване збереження інформаційних ресурсів бібліотечної установи. Сутність сервісної функції полягає у можливості забезпечувати інформацією про існуючі фонди та дозволяє здійснювати зручний пошук локальних і віддалених джерел інформації. Інші функції, до яких дослідниця В. Белінська зараховує науково-методичну, навчальну, просвітницьку та інші, дозволяють бібліотеці університету не тільки проводити науково-дослідну роботу у сфері інноваційних інформаційно-бібліотечних технологій, а й здійснювати освітньо-культурну діяльність [5].

Інформаційний ресурс бібліотеки технічного університету формується насамперед документами з технічних, природничих, економічних наук, що безперечно пов’язано із основними напрямками підготовки фахівців ЗВО. Із відкриттям в університеті нових

спеціальностей (серед яких – «Інформаційна, бібліотечна та архівна справа») фонд бібліотеки поповнився новими надходженнями, покликаними забезпечити грунтовну підготовку майбутніх фахівців (наприклад, виданнями таких відомих науковців у сфері документно-інформаційної комунікації, як Ю. І. Палеха, Н. О. Леміш, С. Г. Кулешов, Н. М. Кушнаренко та інші.

Почасти документний ресурс бібліотеки складається із документів довідково-інформаційного спрямування, окрему частину фондів становлять видання художньої літератури, що зумовлено потребами виховання студентської молоді.

Структуру бібліотечного фонду створюють одночасно декілька ознак, що знаходяться між собою в нисхідних ієрархічних зв'язках. Вибудовувати бібліотечний фонд починають із найбільш значущих для даної бібліотеки ознак. Потім їх ранжують, тобто розподіляють за ступенем важливості. Так, для одних фондів важливим насамперед є зміст документів, для інших – їх форма, ще для інших – їх призначення, для наступних – унікальність документів тощо [9]. До основних фондів бібліотеки ЦНТУ належать видання різних типів та видів, а саме: періодична література; книги; електронні фонди [7]. Основою бібліотечного ресурсу книгозбірні ЦНТУ становлять книжкові видання – 402324 екземплярів науково-навчальної літератури, монографій, підручників, посібників, довідників, атласів, альбомів, буклетів та ін. Технічна та економічна література становить основний масив документів бібліотеки ЦНТУ. Окремі групи представляють художня література та рідкісні видання [7]. Інформаційний ресурс бібліотеки ЦНТУ включає приблизно 35 тис. комплектів періодичних видань, у тому числі колекцію реферативних журналів з природничих та технічних наук, що зберігаються в читальній залі періодичної літератури [7].

Як слушно зауважує Н. Зелінська, періодичні видання наукового змісту формують наукове співтовариство, згуртовуючи не тільки фахівців, а й тих, хто цікавиться новинами науки. Дослідниця виокремлює й інші властивості наукової періодики, зокрема здатність концентрувати значний обсяг наукової інформації, сприяти розвиткові науки, спонукати членів вченої спільноти до публікації наукових розвідок тощо [6].

Інформаційний ресурс бібліотеки ЦНТУ формують також спеціальні фонди, до яких належать фонд НДР і ДКР та фонд дисертацій і авторефератів. Саме специфіка основної діяльності навчального закладу спричинила до концентрації у фондах бібліотеки такого важливого типу документів як неопубліковані. Фахівці-бібліотекознавці підкреслюють, що неопубліковані документи найчастіше перші, а іноді і єдині джерела нової інформації з наукових і технічних питань. За своїм значенням вони не поступаються опублікованим документам, а у деяких випадках навіть переважають їх – за новизною інформації, її конкретністю, стислістю, оперативністю [9].

Результатом науково-дослідних та дослідно-конструкторських робіт є нові технології, дослідницько-конструкторські знахідки, які зумовлюють подальший розвиток перспективних галузей науки і техніки.

Формування фонду НДР і ДКР у бібліотеці ЦНТУ було започатковано наприкінці сімдесятих років минулого століття [7]. Як доречно зазначають автори колективної монографії Технічна освіта на Кіровоградщині: історичний нарис, обсяг науково-дослідних робіт викладачів університету є досить вагомим і значущим [11], тому зазначені фонди є потужною інтелектуальною складовою як бібліотеки, так і університету.

Бібліотека ЦНТУ за рахунок плідної наукової діяльності фахівців університету, поряд із науковими та науково-технічними бібліотеками країни, є фондоутримувачем дисертаційних досліджень та авторефератів переважно технічної, природничої та економічної тематики. Створення фонду дисертацій та авторефератів у бібліотеці ЦНТУ започатковано у дев'яностих роках минулого століття. У складі фонду – 130 одиниць дисертаційних досліджень на здобуття наукових ступеней кандидата та доктора наук. Окрім цього, у розпорядженні бібліотеки приблизно 300 авторефератів дисертацій. Зміст наукових робіт відображає основні тенденції розвитку економічної та технічної галузі країни [7].

Бібліотека Центральноукраїнського національного технічного університету є активним учасником комунікацій університету, пов'язаних із святкуванням ювілейних дат та представленням досягнень і здобутків студентів та викладачів аналізованого вишу. Так, за активного сприяння бібліотечних фахівців було створено нарис історії технічної освіти на Кіровоградщині, де окремі сторінки присвячені розвитку університетської книгозбірні [11]. У рамках майбутніх урочистостей до 90-річчя університету планується також перевидання вищезгаданого дослідження та видання, присвяченого видатним особистостям в історії ЦНТУ. У зв'язку з окресленим напрямком роботи бібліотеки доречним вважаємо також формування фонду «Ювілеї та ювіляри» та створення відповідної бібліографічної продукції.

Висновки. Отже, документний ресурс бібліотеки ЦНТУ становить собою цілісну, грамотно структуровану органічну систему, що робить його незамінним у навчально-виховному й науково-дослідницькому процесі та дозволяє використовувати цей ресурс найкращим чином.

Список літератури

1. Андрущенко В., Т. В. Андрущенко, В. Л. Савельєв Конституціалізація освітнього простору Європи: аксіологічний вимір В. П. Андрущенко. К. : «МП Леся», 2014. 460 с.
2. Апшай Н. Стратегічні засади розвитку бібліотек вищих навчальних закладів в умовах інформатизації Вісник Книжкової палати. 2004. № 6. С. 23–25.
3. Барабаш В. А., Глєбова Л. В. Інформаційний ресурс бібліотеки університету як фактор формування ціннісних орієнтацій майбутніх фахівців Соціум. Документ. Комунікація: збірник наукових статей. Вип. 4. Серія «Історичні науки» / ред. колегія: Коцур В.П. (голов. ред.) та ін. Переяслав-Хмельницький, 2017. С. 159–175.
4. Беззуб І. Бібліотека вищого навчального закладу у формуванні інформаційної культури студента Наукові праці Національної бібліотеки України імені В. І. Вернадського. 2012. Вип. 33. С. 94–105. URL: http://library.znu.edu.ua/articles/1263.ukr.html (дата звернення 23.012019).
5. Белінська В. М. Бібліотека – інформаційний ресурс освіти: стан та перспективи розвитку вузівських бібліотек. Матеріали регіональної міжвузівської науково- практичної конференції. Бібліотека ЧДІЕУ. Чернігів. 2009. С. 4–7. URL: http://library2.stu.cn.ua/Files/images/konferentsii/Nauk-prakt%20konf%2004.12.09.pdf (дата звернення 23.012019).
6. Зелінська Н.В. «Традиційна» періодика у системі сучасної наукової комунікації: тенденції та перспективи. Наука України в світовому інформаційному просторі. 2011, 5. С. 12–15 .
7. Основні фонди URL: http://library.kntu.kr.ua/fixed-assets.html (дата звернення 11.12. 2018).
8. Ріжняк Р.Я. Розвиток інформатики та інформаційних технологій у вищих навчальних закладах України у др. половині XX – на поч. XXI ст.: монографія [за заг.ред. В. М. Орлика]. Кіровоград: «КОД», 2014. 426 с.
9. Столяров Ю.Н. Библиотечный фонд: Учебник. М. : Кн.палата, 1991. 271 с.
10. Стратегія розвитку бібліотечної справи в Україні до 2025 року «Якісні зміни бібліотек задля забезпечення сталого розвитку України. URL: http://mincult.kmu.gov.ua/control/uk/publish/article?art_id=244956883&cat_id=24490984 (дата звернення 20.06.2018).
11. Технічна освіта на Кіровоградщині: історичний нарис. Кіровоград: «Імекс-ЛТД», 2009. 240 с.
12. Юхновец Т. С. Информационные ресурсы библиотек как обязательный инструмент образовательного процесса. URL: http://elib.bsu.by/bitstream/123456789/19464/1/p_387-388.pdf. (дата звернення 15.01. 2019).

УДК 369.542

І. Бондаренко, магістр гр. ФС-18МЗ
Центральноукраїнський національний технічний університет

НЕДЕРЖАВНІ ФІНАНСОВІ ІНСТИТУТИ В СИСТЕМІ СОЦІАЛЬНОГО ЗАХИСТУ НАСЕЛЕННЯ

У статті досліджено основні теоретичні аспекти фінансового забезпечення соціального захисту населення через недержавні фінансові інститути. Проаналізовано сучасний стан та розвиток недержавного пенсійного забезпечення, висвітлено роль страхових компаній, які здійснюють страхування життя в Україні. Запропоновано напрямки подальшого розвитку накопичувальної складової пенсійного забезпечення з метою покращення фінансування соціального захисту населення.

пенсійна система, недержавний пенсійний фонд, страхова компанія, банківська установа, недержавне пенсійне забезпечення, страхування пенсій

Постановка проблеми. Загальновідомо, що найбільшу частку у фінансуванні соціального захисту населення становлять кошти державного та місцевих бюджетів. Однак реалії сьогодення свідчать про дефіцитність бюджетів усіх рівнів та недостатність коштів для фінансування соціальних гарантій. Другим масштабним джерелом фінансування соціальних видатків є кошти страхових фондів, ключовим з яких являється Пенсійний фонд України. Проте, складна демографічна ситуація, кризові процеси в економіці, тінізація заробітної плати, посилення трудової міграції населення призвели до його дефіцитності. У зв'язку з цим вагому роль у подоланні низки соціальних ризиків відіграють недержавні інститути, роль яких у формуванні фінансових ресурсів соціального захисту залишається недостатньою, а їх потенціал у підвищенні добробуту українців недооцінений.

Аналіз останніх досліджень і публікацій. Істотний внесок у дослідження фінансово-економічних аспектів розвитку системи соціального захисту населення зробили такі відомі вчені, як: Л. Баранник, В. Дем'янишин, Л. Лисяк, Е. Лібанова, А. Мерзляк, Д. Міщенко, К. Павлюк, М. Ріппа, Н. Савицька, О. Степанова та інші. Дослідженню питань функціонування недержавного пенсійного забезпечення присвячені наукові праці Т. Говорушко, Т. Дідковської, І. Мірошниченко, О. Надієнко, О. Данілюка, В. Шульги, Л. Казаренко, Д. Третяк та інших. Попри вагомий доробок учених у цій сфері, треба зазначити, що питання фінансового забезпечення соціального захисту осіб пенсійного віку та пошук ефективних інструментів його удосконалення в Україні потребують ґрунтовних подальших досліджень. Актуальним сьогодні є залучення до цього процесу недержавних фінансових інститутів.

Метою статті є дослідження теоретичних аспектів фінансового забезпечення соціального захисту населення через недержавні фінансові інститути та розробка пропозицій щодо розвитку системи недержавного пенсійного забезпечення.

Виклад основного матеріалу. Ст. 46 Конституції України гарантує громадянам «право на соціальний захист, що включає право на забезпечення їх у разі повної, часткової або тимчасової втрати працездатності, втрати годувальника, безробіття з незалежних від них обставин, а також у старості та в інших випадках». Фінансовою основою для реалізації цього права є кошти загальнообов'язкового державного соціального страхування, які формуються з внесків громадян і роботодавців, а також бюджетні кошти та інші джерела соціального забезпечення [3].

Вітчизняна система соціального захисту населення об'єднує три головні складові:

– соціальне страхування (пенсійне, від нещасних випадків на виробництві, медичне, на випадок тимчасової втрати працездатності);

– соціальна допомога (допомога непрацездатним і малозабезпеченим громадянам, житлові виплати);

– соціальні гарантії (прожитковий мінімум, мінімальний розмір заробітної плати, мінімальний розмір пенсії, індексація грошових доходів тощо).

Найбільшу частину соціальних видатків спрямовують на виплату пенсій, обсяг яких постійно зростає та у 2018 р. становив 99,4 млрд. грн. Високими є й темпи зростання

видатків Пенсійного фонду України, які тільки у 2018 р. збільшилися на 67,1 млрд. грн. Така ситуація насторожує, адже відбувається зростання дефіциту Пенсійного фонду України, який у 2018 р. сягнув свого максимуму за останніх 12 років (28 %) [7]. Основним джерелом доходу більшості пенсіонерів України є солідарна система, але виплат з неї недостатньо, щоб забезпечити гідний рівень життя на пенсії: станом на 01.01.2019 середня пенсія становила 2646 грн. або $95 (у 2018 році – 42 % чистої середньої заробітної плати, з якої сплачені внески).

Очевидно, що українська пенсійна система перебуває в гострій фінансовій кризі та потребує негайних кардинальних реформ, а не "косметичних заходів", таких як спрямування коштів від розмитнення автомобілів на "євромерах" до Пенсійного фонду [7].

Недержавне пенсійне забезпечення, як передбачено законодавством, здійснюється:

– недержавними пенсійними фондами (НПФ) шляхом укладення пенсійних контрактів між адміністраторами пенсійних фондів і вкладниками таких фондів;

– страховими організаціями шляхом укладення договорів страхування довічної пенсії, страхування ризику настання інвалідності або смерті учасника фонду;

– банківськими установами шляхом укладення договорів про відкриття пенсійних депозитних рахунків для накопичення пенсійних заощаджень у межах суми, визначеної для відшкодування вкладів Фондом гарантування вкладів фізичних осіб.

Порівняльна характеристика фінансових послуг з недержавного пенсійного забезпечення, що надаються різними фінансовими інститутами наведена в табл. 1.

Таблиця 1 – Порівняльна характеристика фінансових послуг з недержавного пенсійного забезпечення, що надаються різними фінансовими інститутами [1; 2]

	Вид фінансової послуги	Пенсійні кошти	Види пенсійних виплат
Недержавний пенсійний фонд	пенсійний контракт	сума зобов'язань недержавного пенсійного фонду перед його учасниками	- пенсія на визначений строк; - одноразова пенсійна виплата; - довічний ануїтет (за умов укладення договору страхування довічної пенсії зі страховою організацією)
Страхова компанія, що здійснює страхування життя	страхування ренти (ануїтетів)	страхові резерви страховика	- одноразова пенсійна виплата; - пенсія на визначений строк; - довічна пенсія (довічний ануїтет)
Банківська установа	пенсійний депозитний вклад	розмір вкладів	- одноразова пенсійна виплата

Станом на 30.06.2019 р. в Державному реєстрі фінансових установ містилася інформація про 63 НПФ та 22 адміністратори НПФ (станом на 30.06.2018 р. - 62 НПФ та 22 адміністратори) [6].

Основні показники діяльності НПФ та темпи їх приросту наведені в таблиці 2.

Таблиця 2 – Динаміка основних показників діяльності недержавних пенсійних фондів [6]

Показники	Станом на:			Темпи приросту станом на: (%)	
	30.06.2017	30.06.2018	30.06.2019	30.06.2018/ 30.06.2017	30.06.2019/ 30.06.2018
Кількість укладених пенсійних контрактів, тис. шт.	66,5	63,7	72,7	-4,2	14,1
Загальна кількість учасників НПФ, тис. осіб	838,0	846,2	860,8	1,0	1,7
Загальна вартість активів НПФ, млн. грн.	2248,7	2536,7	2892,9	12,8	14,0

Пенсійні внески, всього, млн. грн.	1945,6	1937,7	2071,9	-0,4	6,9
у тому числі: - від фізичних осіб	110,0	143,6	195,9	30,5	36,4
- від фізичних осіб-підприємців	0,2	0,2	0,2	0,0	0,0
- від юридичних осіб	1834,6	1793,4	1875,3	-2,2	4,6
Пенсійні виплати, млн. грн.	685,2	753,4	878,6	10,0	16,6
Кількість учасників, що отримали/ отримують пенсійні виплати, тис. осіб	83,2	80,2	82,7	-3,6	3,1
Сума інвестиційного доходу, млн. грн.	1227,3	1536,7	1945,4	25,2	26,6
Прибуток від інвестування активів недержавного пенсійного фонду, млн. грн.	956,4	1 240,0	1587,1	29,7	28,0

Станом на 30.06.2019 р. адміністраторами НПФ укладено 72,7 тис. шт. пенсійних контрактів, що більше на 14,1 % (9,0 тис. шт.) порівняно зі станом на 30.06.2018 р. Найбільше контрактів укладено з вкладниками фізичними особами (65,8 тис.шт., або 90,5 %). Як свідчать дані табл. 1 загальна кількість учасників НПФ значно перевищує кількість укладених пенсійних контрактів. Така ситуація може свідчити про лише номінальну кількість учасників у реєстрах НПФ, які не уклали пенсійних контрактів і не сплачують пенсійних внесків.

Одним із основних якісних показників, які характеризують систему НПЗ, є сплачені пенсійні внески. Сума пенсійних внесків станом на 30.06.2019 р. становить 2 071,9 млн. грн., збільшившись на 6,9 % (134,2 млн. грн.) в порівнянні з аналогічним періодом 2018 року. Порівняно зі станом на 30.06.2017 р. сума пенсійних внесків станом на 30.06.2018 р. зменшилась на 0,4 % (7,9 млн. грн.).

Пенсійні виплати (одноразові та на визначений строк) станом на 30.06.2019р. становили 878,6 млн. грн., що на 16,6 % більше в порівнянні з аналогічним періодом 2018 року, при цьому одноразові виплати зросли на 8,4 %, пенсійні виплати на визначений строк – на 35,7 %. Сукупно недержавними пенсійними фондами станом на 30.06.2019 р. було здійснено пенсійних виплат (одноразових та на визначений строк) 82,7 тисячі учасників, тобто 9,6 % від загальної кількості учасників, які отримали/ отримують пенсійні виплати.

Загальна вартість активів, сформованих НПФ, станом на 30.06.2019 р. становила 2892,9 млн. грн., що на 14,0 %, або на 356,2 млн. грн. більше в порівнянні з аналогічним періодом 2018 року та на 28,6 %, або на 644,2 млн. грн. більше в порівнянні з аналогічним періодом 2017 року.

Для НПФ властиво формувати портфель, до якого входять об’єкти інвестування з мінімальним ступенем ризику. Тому особливого значення набуває вибір інвестиційних інструментів, використовуючи які НПФ зможуть забезпечити захист грошових коштів населення від інфляційних процесів і при цьому отримувати визначений приріст капіталу. На українському ринку недостатній вибір інвестиційних інструментів. Станом на 30.06.2019 р. переважними напрямами інвестування пенсійних активів стали цінні папери, дохід за якими гарантовано Кабінетом Міністрів України (47,3 %) та депозити в банках (36,4 % інвестованих активів). Розмістити пенсійні активи в такі прості, консервативні інструменти фінансового ринку можна й без дорогого посередництва адміністраторів пенсійних фондів, компаній з управління активами та зберігачів. Загальний дохід, отриманий від інвестування пенсійних активів, станом на 30.06.2019 р. становив 1 945,4 млн. грн., збільшившись у порівнянні зі станом на 30.06.2018 р. на 408,7 млн. грн., або на 26,6 %.

Незважаючи на позитивні тенденції функціонування НПФ, приріст доходу та збільшення обсягів акумульованих пенсійних активів, частка останніх залишається мізерною. Порівняно з бюджетом Пенсійного фонду України обсяг активів усіх НПФ не досягає 1 %. Варто зауважити, що причини не достатньо високих показників діяльності НПФ сформульовано майже десятиліття тому. Це: несприятлива макроекономічна ситуація, відсутність розвинутих ринків капіталу й надійних фінансових інструментів, низький рівень доходів населення та нерозуміння необхідності заощаджувати на пенсію, а також недостатнє пропагування важливості (навіть відсутність інформації про існування) недержавних пенсійних схем.

На жаль, можна констатувати, що сьогодні більшість цих причин досі не усунена, а деякі проблеми розвитку недержавного пенсійного забезпечення посилились. Українські НПФ надто дорогі для учасників, не викликають довіру в населення та маловідомі пересічному громадянину України, щоб бути надійним фундаментом для накопичувального рівня пенсійної системи. Але треба зазначити і позитивні зрушення, які стосуються підвищення рівня дохідності пенсійних фондів, зростання інформованості та зацікавленості населення щодо системи накопичувального пенсійного забезпечення, підвищення попиту на фінансові послуги НПФ, страхових компаній.

Тому більш нагальною потребою є реформування та пожвавлення ринку капіталу взагалі та створення нових фінансових інструментів, що відповідають потребам довготермінового інвестування пенсійних коштів.

Згідно із сучасним визначенням страхування життя характеризується як вид особистого страхування, який передбачає обов'язок страховика здійснити виплату відповідно до договору страхування за настання смерті в період дії договору або дожиття застрахованої особи до закінчення договору, а також за настання нещасного випадку або захворювання [9].

Нині у страховій сфері розрізняють ризикове (у разі смерті або втрати працездатності), накопичувальне (страхова сума виплачується страхувальнику за дожиття ним до зазначеного терміну або у разі смерті застрахованої особи його спадкоємцям) та змішане (поєднує в собі риси ризикового та накопичувального страхування, а також може включати страхування від нещасних випадків) страхування життя.

З огляду на проблеми функціонування державної складової пенсійної системи, постійний дефіцит бюджету Пенсійного фонду, перспективним напрямком соціального захисту є накопичувальне страхування дожиття до пенсійного віку з наступною довічною виплатою щомісячної пенсії у встановленому розмірі.

Однак, в Україні цей вид страхування не досить розвинений.

До проблем, що перешкоджають розвитку страхування життя слід віднести: негативну історію страхування життя в Україні в пострадянський період; відсутність надійних інвестиційних інструментів та гарантій збереження вкладених коштів; низькі доходи громадян та відсутність вільних коштів; недовіру населення до страхових компаній; низький рівень економічного розвитку країни, інфляція, нестійкість національної валюти; недосконале законодавство; низьку страхову культуру населення, страхових посередників і деяких страховиків.

Динаміка основних показників діяльності страхових компаній, що здійснюють страхування життя за 2016–2018 рр. наведено в таблиці 3.

Таблиця 3 – Динаміка основних показників діяльності страхових компаній, що здійснюють страхування життя за 2016–2018 рр. [5]

Показники	Станом на:			Темпи приросту станом на: (%)	
	31.12.2016	31.12.2017	31.12.2018	31.12.2017/ 31.12.2016	31.12.2018/ 31.12.2017

Кількість страхових компаній «life», од.	39	33	30	-15,4	-9,1
Кількість застрахованих фізичних осіб, осіб	4165014	4076718	4473911	-2,1	9,7
Резерви зі страхування життя, млн. грн.	7828,2	8389,6	9335,1	7,2	11,3
Величина зміни резервів із страхування життя (млн. грн.)	1000,7	983,0	1018,3	-1,8	3,6
у тому числі, яка відповідає: інвестиційним доходам, що застосовуються для розрахунку страхових тарифів, млн. грн.	220,7	227,1	246,1	2,9	8,4

Кількість страховиків зі страхування життя зменшилась за період, що аналізується. Однак, порівнюючи основні показники діяльності страхових компаній «life» та НПФ (табл. 2), можна помітити, що при значно меншій кількості страховиків вони значно випереджають НПФ за такими показниками, як кількість застрахованих осіб, розмір страхових резервів і сума інвестиційного доходу.

Страхові компанії здійснюють недержавне пенсійне страхування шляхом укладення договорів страхування довічної пенсії, страхування ризику настання інвалідності або смерті учасника фонду. Пенсійне страхування передбачає, що страхова організація гарантує застрахованій особі виплати, які пов'язані з досягненням пенсійного віку. Особливістю і одночасно перевагою такого виду забезпечення додаткової пенсії є те, що за договором можливо встановити вік початку виплати ануїтету, а також укласти договір страхування на дожиття, що є неявною альтернативою пенсійного страхування. Також серед конкурентних переваг страховиків зі страхування життя слід особливо зазначити таке: можливість здійснювати довічну виплату пенсії (на відміну від банків та НПФ), гарантія мінімального розміру майбутньої пенсії, обов'язкові виплати вигодонабувачам у разі смерті застрахованої особи, висока надійність фінансових гарантій, що забезпечується жорстким державним контролем за діяльності у сфері страхування життя; диференціація страхового продукту залежно від потреб страхувальника; розвинена мережа фінансових консультантів; професійна підготовка та досвід фахівців зі страхування життя [8].

Отже, наразі система недержавного пенсійного забезпечення не заохочує населення до ефективних заощаджень на пенсію. Вона надто дорога й не забезпечує належного інвестиційного доходу. Участь населення в ній мізерна, сприйняття більшістю громадян – негативне.

Систему індивідуальних пенсійних заощаджень можна запроваджувати лише за наявності певних передумов. По-перше, населенню треба добре розуміти недержавні фінансові установи та інструменти й довіряти їм. По-друге, мають бути надійні фінансові інструменти та фінансові ринки для стимулювання внутрішніх інвестицій і створення робочих місць. По-третє, зважаючи на високі адміністративні вимоги накопичувальної системи, приватний сектор повинен мати значний адміністративний потенціал.

У короткостроковій перспективі, зважаючи на час, який потрібен для розвитку ринків капіталу та розроблення надійних фінансових інструментів для інвестування пенсійних активів, уряд має розглянути можливість запровадження неоподатковуваних, добровільних, автоматичних індивідуальних ощадних пенсійних рахунків у банках. Такі рахунки можна запровадити за зразком простої системи індивідуальних пенсійних рахунків (ІПР) у Сполучених Штатах. Щоб забезпечити розумні та обмежені фінансові стимули (податкові пільги) для розміщення заощаджень на кшталт ІПР на банківських ощадних рахунках чи в державних облігаціях, потрібно внести необхідні зміни до законодавства. Банкам можна було б дозволити пропонувати ці фінансові продукти малим інвесторам/населенню з

невеликою платою за послуги. Знімати кошти з добровільних пенсійних рахунків (ІПР) можна дозволити або після досягнення певного віку, або якщо настане певна подія в житті (хвороба або придбання житла) [4].

В умовах слабкого рівня розвитку системи недержавного пенсійного забезпечення доцільно створити умови для розвитку та однакові «правила гри» для всіх організацій, що беруть участь у цьому секторі, охоплюючи недержавні пенсійні фонди, страхові компанії та банки. Їх рівноправна конкуренція на фінансовому ринку сприятиме розвитку системи недержавного пенсійного забезпечення. І лише споживач буде визначати, кому доручити свої пенсійні заощадження [10, с. 93].

Уряду необхідно більше уваги приділяти нагальній потребі підвищення фінансової обізнаності громадян шляхом надання їм належної фінансової інформації та просвіти, щоб вони знали про пенсійні заощадження та варіанти підвищення рівня їхнього фінансового добробуту на пенсії. Таку просвіту, що має на меті змінити ставлення та поведінку населення щодо заощаджень, треба запроваджувати із середньої школи.

Список літератури

1. Закон України «Про недержавне пенсійне забезпечення» від 09.07.2003 № 1057-IV. URl: https://zakon.rada.gov.ua/laws/show/1057-15.
2. Інформація про стан і розвиток недержавного пенсійного забезпечення України // національна комісія, що здійснює державне регулювання у сфері ринків фінансових послуг. URL: https://www.nfp.gov.ua/ua/Informatsiia-pro-stan-i-rozvytok-nederzhavnoho-pensiinoho-zabezpechennia-Ukrainy.html.
3. Конституція України : Закон України від 28.06.1996 року № 254к/96-ВР. URL : https:// zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80.
4. Недержавне пенсійне забезпечення в Україні: оцінка та рекомендації. Проект USAID «Трансформація фінансового сектору», липень 2019р. URL: http://www.fst-ua.info/wp-content/uploads/2019/07/Voluntary_Private_Pensions_in_Ukraine-Assessment_jul2019_ua.pdf
5. Підсумки діяльності страхових компаній за 2018 рік. URL: https://forinsurer.com/files/file00654.pdf.
6. Підсумки розвитку системи недержавного пенсійного забезпечення станом на 30.06.2019р. URL: https://www.nfp.gov.ua/files/OgliadRinkiv/NPF/NPF_II_kv%202019.pdf.
7. Приймак І., Вишивана Б. Недержавне пенсійне забезпечення в системі соціального захисту населення / І. Приймак, Б. Вишивана // Світ фінансів. - №3(60). – 2019. – с. 121-138.
8. Савицька Н.Л., Жилякова О.В. Оцінка перспективи розвитку ринку страхування життя в умовах реформування пенсійної системи //Н. Савицька, О. Жилякова / Проблеми економіки. - № 1 (39). – 2019. С. 170-175.
9. Страхування життя / Офіційний сайт страхової компанії «ІНГО Україна». URL: http://ingo.kiev.ua/ua/strakhovanie-zhizni.html.
10. Третяк Д. Д. Суперечності розвитку недержавного пенсійного забезпечення в Україні. Вісник КНУ імені Тараса Шевченка. Економіка. 2014. № 154. С. 89–94.

УДК 338.43

Я. Бордюг, магістр гр. ОКД-18-1,4
Центральноукраїнський національний технічний університет

МЕХАНІЗМИ РЕГУЛЮВАННЯ РОЗВИТКУ АГРОПРОМИСЛОВОГО КОМПЛЕКСУ: НАПРЯМИ ВДОСКОНАЛЕННЯ

У статті охарактеризовано складові механізму регулювання агропромислового комплексу, засоби та методи державного регулювання економіки. Наведено напрями регулювання діяльності сільськогосподарських підприємств, а також стратегічні пріоритети перегляду механізму здійснення державної підтримки розвитку агропромислового комплексу.

регулювання, агропромисловий комплекс, механізм, управління

Актуальними питаннями на сьогодні у сфері державного регулювання сільського господарства є проблеми підвищення ефективності державної підтримки виробників сільськогосподарської продукції, яка повинна бути спрямована на: забезпечення прибутковості виробництва на рівні, що забезпечує розширене відтворення; створення сприятливих соціальних умов життя сільських жителів та покращення добробуту їхніх сімей; формування передумов для комплексного розвитку сільських територій; задоволення потреб населення в якісних продуктах харчування; розширення експортного потенціалу країни [1].

Механізм державного регулювання економіки ґрунтується на сукупності взаємопов'язаних фінансово-економічних інструментів, форм, важелів і методів впливу на процес розширеного відтворення з урахуванням цілей та інтересів суб'єктів економічних відносин. Систему засобів та інструментів державного регулювання за спорідненими ознаками можна об'єднати у такі групи:

1. Засоби державного регулювання: адміністративні (стандарти, дозволи, ліміти, заборони, обмеження, нормативи, штрафи); економічні (податки, державні інвестиції, закупівлі, субсидії, дотації, кредити, позички, ціни на сільськогосподарську продукцію); інформаційні (публікації у засобах масової інформації, документи).

2. Інструменти державного регулювання: законодавчо-правові (закони, постанови, укази); нормативно-адміністративні (розпорядження, рішення, вказівки, накази, інструкції, правила, положення, договори); організаційно-економічні (плани, проекти, державний та місцевий бюджети, державне замовлення й державний контракт, договори, цільові програми, прогнози) [2].

Гармонізація розвитку агропромислового комплексу регіону здатна вирішити низку проблем регіонального рівня: підтримка зайнятості, забезпечення надходжень до місцевих бюджетів, підтримка продовольчої безпеки, залучення інвестицій, ефективне використання місцевої інфраструктури тощо. Органи державної влади й управління мають вжити заходів, спрямованих на посилення позитивного впливу механізму регулювання на тенденції й структуру розвитку регіональних агропромислових комплексів, що виступає важливою умовою високої ефективності одночасно і державної аграрної політики, і державної регіональної політики. Вказане особливо важливе в контексті реалізації завдань антикризового регулювання та підтримки експортного потенціалу країни [3].

На рис. 1 наведені базові напрями державного регулювання сільськогосподарських підприємств.

Рисунок 1 – Напрями регулювання діяльності сільськогосподарських підприємств

Джерело: [1]

Стратегічним напрямком має стати перегляд механізму здійснення державної підтримки за рахунок: удосконалення інфраструктури, стимулювання інвестицій, поліпшення якості продукції та підвищення родючості земель, створення державного резерву продовольства, маркетингові і дорадчі послуги тощо. Все це дасть можливість покращити ситуацію в агросфері за умови пришвидшеної діяльності органів влади та цілеспрямованості виділеного фінансування [4].

Список літератури

1. Сербіненко Н.В., Сербіненко К.Г. Трансформація системи державного регулювання агропромислового сектора в умовах нестабільного зовнішнього середовища. Збірник наукових праць Таврійського державного агротехнологічного університету (економічні науки). 2014. №2. С. 200-205.
2. Юрчишина С.І. Фінансова складова в системі державного регулювання розвитку підприємств агропромислового комплексу України. Економічний аналіз. 2017. Т. 27(4). С. 118-123.
3. Захарін С.В., Левчук Н.І., Романовська Т.І. Регулювання розвитку агропромислового комплексу: регіональний рівень. Наукові праці Національного університету харчових технологій. 2015. Т. 21. №5. С. 57-67.
4. Антонова С.Є., Корбутяк В.І. Основні тенденцій державного регулювання розвитку агропромислового комплексу України. Вісник Національного університету водного господарства та природокористування. Економічні науки. 2016. Вип. 1. С. 3-10.

УДК 351.82: 658.012

О. Вдовиченко, магістр гр. УФЕБ-18М
Центральноукраїнський національний технічний університет

ЗАБЕЗПЕЧЕННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ ЗОВНІШНЬОЕКОНОМІЧНОЇ ДІЯЛЬНОСТІ ПІДПРИЄМСТВ ХАРЧОВОЇ ПРОМИСЛОВОСТІ

У статті з'ясовано сутність поняття зовнішньоекономічної діяльності у розрізі економічної безпеки. Розглянуто особливості економічної безпеки зовнішньоекономічної діяльності підприємств харчової промисловості. Визначено основні загрози для підприємств харчової промисловості. Наведений перелік загроз засвідчує, що уникнення кризового стану потребує системного аналізу факторів як внутрішнього так і зовнішнього впливу

економічна безпека, харчова промисловість, підприємство харчової промисловості, зовнішньоекономічна діяльність, загрози, внутрішнє середовище, зовнішнє середовище

Постановка проблеми. Для підприємства будь-якої галузі, яке турбується за свій розвиток та розширення, важливим напрямком підвищення економічної стійкості та економічного зростання є орієнтація на зовнішньоекономічну діяльність. Вибір такого напрямку знаходиться в рамках загальнодержавної стратегії та відкриває перед підприємствами України великі можливості в розширенні каналів збуту. Підприємства харчової промисловості не є виключенням.

Харчова промисловість завжди вважалася для України пріоритетною і стратегічно важливою галуззю, яка здатна забезпечити не тільки потреби внутрішнього ринку, ай світового. Вона є не тільки завершальною ланкою виробництва харчових продуктів, а й інтегратором ефективного функціонування всього продовольчого комплексу. 22 % у структурі реалізації промислової продукції, 47 % у структурі доходу АПК забезпечує пріоритетність досліджень економічної безпеки саме підприємств харчової промисловості [1]. Доступність харчових продуктів, їх якість та екологічність впливають на рівень продовольчої безпеки держави, виступають індикаторами її соціальної стабільності.

Проте разом з тим існує ряд небезпек та загроз, які суттєво впливають на стан економічної безпеки зовнішньоекономічної діяльності підприємств вітчизняної харчової промисловості. Тому забезпечення економічної безпеки зовнішньоекономічної діяльності є надзвичайно актуальним питанням. Саме стан економічної безпеки підприємств харчової галузі багато в чому обумовлює ефективність їх діяльності в ринковій економіці, що призводить до необхідності розгляду проблем забезпечення економічної безпеки їх зовнішньоекономічної діяльності (ЗЕД).

Аналіз останніх досліджень і публікацій. Економічна безпека підприємства турбувала своєю проблематикою багатьох вчених. Дослідниками в даній царині можна вважати Т. Гладченко, Т. Гордієнко, А. Заїчковський, Т. Іванюта, Г. Козаченко, В. Малащенко, Д. Никифорчук, С. Ніколаюк, О. Орлика, В. Пономарьова, Т. Соколенко, В. Третяк, І. Троц, Л. Шваб, Л. Юрович.

Питаннями розвитку зовнішньоекономічної діяльності підприємства займались такі науковці, як І. Багрова, В. Власюк, В. Гриньова, О. Кириченко, В. Козик, Л. Ліпич, Ю. Макогон, А. Мокійц, В. Новицький, Л. Стровський, Т. Циганкова, О. Чугай та багато інших.

Також при аналізі останніх досліджень і публікацій було виявлено певні прогалини у забезпеченні саме економічної безпеки зовнішньоекономічної діяльності вітчизняних підприємств, про що у своїх наукових працях зазначають такі фахівці, як І. Бланк, Т. Васильців, Л. Донець, Г. Козаченко, Ю. С. Погорелов, С. Покропивний,Є. Рудніченко та

інші. Разом з тим, поза увагою залишились питання економічної безпеки зовнішньоекономічної діяльності підприємств саме харчової промисловості.

Цілі статті. Метою дослідження є визначення сутності економічної безпеки здійснення зовнішньоекономічної діяльності підприємств харчової промисловості, а також виявлення загроз економічній безпеці ЗЕД підприємства.

Виклад основного матеріалу. Харчова промисловість є однією із провідних галузей вітчизняної економіки. Вона безпосередньо задіяна в забезпеченні продовольчої безпеки держави, формуванні її експортного потенціалу й здатна позитивно впливати на динаміку економічного зростання України. Підприємства, що представляють харчову промисловість здійснюють зовнішньоекономічну діяльність та є знаними на весь світ.

Ступінь залучення підприємств у зовнішньоекономічну діяльність, з одного боку, є індикатором розвитку національної економіки та її стабільності в цілому, а з іншого, рівня підтримки державою такої діяльності, що проявляється у регуляторних нормах її правового поля. За даними служби статистики України експорт товарів та послуг з України у 2016 р. становив 45112,7 млн. дол. США, а імпорт товарів та послуг у цьому році – 44571,1 млн. дол. США [2].

Зовнішньоекономічна діяльність (ЗЕД) є діяльністю підприємства, у процесі якої відбувається взаємодія з іноземним суб'єктом господарювання; у процесі діяльності виникають та розвиваються зовнішньоекономічні зв'язки (як на рівні підприємств, так і на більш високих рівнях управління), що створюють тим самим підґрунтя для подальшого її здійснення [3]. При збільшенні глибини залучення до міжнародних ринків відбувається якісна та кількісна зміна загроз економічній безпеці ЗЕД підприємства.

Термін «зовнішньоекономічна діяльність підприємства» є загальноприйнятим поняттям, яке регламентовано законом України «Про зовнішньоекономічну діяльність» – це діяльність суб'єктів господарської діяльності України та іноземних суб'єктів господарської діяльності, побудованої на взаємовідносинах між ними, що має місце як на території України, так і за її межами [4].

При здійсненні експортно-імпортних операцій підприємства харчової промисловості зіштовхуються з рядом проблем, що викликають додаткові витрати як з боку виробників, так і з боку споживачів. Якщо внутрішні виробники функціонують в більш жорстких умовах до забезпечення безпеки продукції, то вони матимуть більш високі витрати на виробництво і збут порівняно з виробниками-імпортерами, які виграють за більш низькими цінами внаслідок відсутності строгих форм контролю якості та безпеки продукції.

Споживачі можуть бути готові сплачувати за додаткові характеристики безпеки, але відсутність платоспроможного попиту може призвести до втрати підприємством-виробником ринкових позицій, що в значній мірі знижує рівень його безпеки. З огляду на це економічну безпеку ЗЕД підприємства доцільно розглядати з позиції діалектичного поєднання безпеки споживання та безпеки виробництва, що дозволяє сформувати такий стан господарської діяльності промислового підприємства, що забезпечує захищеність її елементів і зв'язків в умовах деструктивного впливу ринкових, політичних, екологічних та інших чинників при збереженні та підвищенні суспільного добробуту.

На сьогоднішній день існує багато різного роду перешкод щодо здійснення зовнішньоекономічної діяльності вітчизняними підприємствами. Так, Тульчинська С. О. [5] звела їх у наступному переліку:

- недосконалість державного регулювання у сфері зовнішньоекономічної діяльності;
- непрофесійні дії органів виконавчої влади та існуюча корупція;
- низький рівень конкурентоспроможності продукції вітчизняних підприємств, що призводить до того, що більшість продукції вітчизняних підприємств має сировинний характер;
- нестабільна політична ситуація, що су проводжується негативними соціально-економічними явищами;
- нестабільність валютного курсу національної грошової одиниці;

- моральна та фізична зношеність більшої частини виробничих засобів вітчизняних підприємств тощо.

Отже, зовнішня торгівля за основними товарними групами харчової продукції залишається нестабільною та суттєво залежить від коливань попиту та від крупних контрактів окремих підприємств. Послаблення позицій вітчизняних товаровиробників харчової продукції посилює роль імпорту даної продукції з суттєвим зменшенням експорту.

Ці перешкоди в певній мірі створюють загрози економічній безпеці ЗЕД.

До факторів зовнішнього середовища, що впливають на розвиток ЗЕД українських підприємств можна віднести такі:

- зміна впливу факторів часу та простору. ЗЕД, як правило, пов'язана із подоланням великих відстань. Високі темпи технічного прогресу у галузі комунікацій та транспорту дозволяють у значній мірі економити час і кошти, які витрачають на передавання інформації, транспортування товарів, переміщення людей. Досягнення у галузі комунікацій прискорюють взаємодію та дозволяють здійснювати більш оперативний контроль за будь-якими міжнародними операціями. Швидкий обмін інформацією щодо нової продукції приводить до збільшення обсягів продажу на іноземних ринках. Завдяки технологічним нововведенням у транспортній сфері з'явилася можливість переміщувати виробництво з країни в країну, поділяти виробництво компонентів або цілих виробів між країнами з метою оптимізації витрат;
- розвиток інституційних механізмів: удосконалюється діяльність суспільних інститутів, інфраструктура бізнесу. Це стосується, перш за все, ліквідації торговельних бар'єрів, створення нових та розвиток існуючих економічних інтеграційних угруповань;
- зміна конкуренції в світовому господарстві. У зв'язку із зростанням конкуренції на світовому ринку, розвитком системи комунікацій, інформації, транспорту, лібералізацією торгівлі підприємства відчувають все більший вплив міжнародних ринків. На світових ринках міжнародна конкуренція характеризується жорстким загостренням. У зв'язку з цим слід мати на увазі, що українські підприємства не мають такої широкої державної підтримки, як західні фірми, а можливості економічних угруповань (ЄС, НАФТА, АТЕС тощо) значно більші ніж можливості СНД;
- недостатні ресурсні можливості більшості українських підприємств для широкої діяльності на зовнішніх ринках;
- недостатні знання світової практики та відносне відставання у ефективному використанні ринкових механізмів у ЗЕД;
- високий рівень агресивності західних фірм як на світовому так і на внутрішньому ринку України [6, с. 64].

Ці та багато інших загроз створюють умови нестабільності ЗЕД харчової промисловості.

З огляду на це забезпечення економічної безпеки ЗЕД підприємств харчової промисловості потребує комплексної оцінки, яку доцільно представляти як сукупність процесів, методів, інструментів виявлення, попередження, усунення загроз і конфліктів з метою розробки заходів щодо підтримки ефективного функціонування підприємства при відповідному нарощуванні і реалізації експортного потенціалу країни-експортера харчової продукції при узгодженні економічних інтересів з країною-імпортером [7].

Забезпечення економічної безпеки бізнесу повинно розглядатися з позиції сукупності способів найбільш ефективного використання ресурсів і капталу з метою попередження або зниження ризику банкрутства, що гарантує успішність господарських процесів з позиції внутрішніх та зовнішніх критеріїв.

Традиційно при аналізі безпеки сучасного підприємства рекомендовано розглядати: безпеку, пов'язану з типом підприємства; безпеку, пов'язану з життєдіяльністю підприємства; безпеку за складовими частинами сфер його діяльності [8]. Для харчових підприємств забезпечення економічної безпеки розглядається з позицій стабільності його

функціонування, прибутковості, особистої безпеки персоналу та здатності фіксації та управління загрозами. В таких підходах до аналізу та забезпечення не враховано специфіку діяльності підприємств харчового господарства, вплив економічної безпеки окремого підприємства на стан безпеки держави, не розкривається взаємозв'язок між складовими економічної безпеки в умовах ЗЕД.

На основі існуючих визначень та з урахуванням особливостей ЗЕД підприємства, які полягають в економічних відносинах з іноземними підприємствам, пропонуємо визначати економічну безпеку ЗЕД підприємства, як стан найбільш ефективного використання його ресурсів для стабільного функціонування на міжнародному ринку та здатність протистояти впливу небезпечних факторів зовнішнього і внутрішнього середовища з метою забезпечення ефективних взаємовідносин суб'єктів господарської діяльності як на території України, так і за її межами.

Висновок. Таким чином, для стабільного та функціонального розвитку вітчизняних підприємств харчової промисловості необхідно звернути увагу на захист діяльності підприємств від дестабілізуючого впливу внутрішніх та зовнішніх факторів навколишнього середовища. Це можливо лише при підтримці достатнього рівня економічної безпеки зовнішньоекономічної діяльності підприємств. У сукупності з визначенням рівня економічної безпеки ЗЕД та проведенням на його основі системи протидіючих та попереджуючих заходів можливо спрямувати у правильне русло діяльність підприємств для досягнення поставлених цілей. При цьому слід відзначити, що для забезпечення економічної безпеки ЗЕД підприємства харчової промисловості необхідно проводити комплекс заходів, спрямованих на забезпечення захисту підприємства від негативного впливу зовнішнього та внутрішнього оточення, зокрема: розробляти та випускати конкурентоспроможну продукцію, створювати стабільний попит, забезпечувати фінансову стійкість та економічну стабільність підприємств, а також нормативну та правову захищеність, збереження комерційної таємниці, забезпечувати підприємство компетентним керівництвом та персоналом тощо.

Список літератури

1. Семененко О. Г. Аналіз розвитку харчової промисловості України / О. Г. Семененко // Економічний вісник університету. - 2017. - Вип. 33(1). - С. 168-182. - Режим доступу: http://nbuv.gov.ua/UJRN/ecvu_2017_33(1)__23
2. Зовнішньоекономічна діяльність / Державна служба статистики України [Електронний ресурс]. — Режим доступу: http://www.ukrstat.gov.ua/
3. Маслак О. І., Оцінка економічної безпеки підприємства при зовнішньоекономічній діяльності / О. І.Маслак Д. Л. Гришко, Н.Є Пирогов // Вісник КрНУ імені Михайла Остроградського. – 2012. – Вип. 3 (74). – с. 163-169 . - Режим доступу: http://www.kdu.edu.ua/statti/2012-3-1(74)/163.pdf
4. Закон України «Про зовнішньоекономічну діяльність» від 16 квітня 1991 р., № 959-XII. [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/959-12
5. Тульчинська С. О., Кириченко С. О., Дубенець В. П. Напрями активізації зовнішньоекономічної діяльності вітчизняних підприємств. Агросвіт. 2018. № 6. С. 28–31.
6. Зовнішньоекономічна діяльність підприємств: Навчальний посібник / [Козак Ю.Г., Логвінова Н.С. та ін.]; за ред. Ю.Г. Козака, Н.С. Логвінової, М.А. Зайця. – 4-тє вид., перероб. та доп. – К.: Освіта України, 2012. – 272 с.
7. Попова О. Ю. Рівні забезпечення економічної безпеки зовнішньоекономічної діяльності підприємств машинобудування / О. Ю. Попова. // Ефективна економіка. - 2012. - № 6. - Режим доступу: http://nbuv.gov.ua/UJRN/efek_2012_6_3.
8. Ильяшенко С.Н. Составляющие экономической безопасности предприятия и подходы к их оценке/ С.Н. Ильяшенко // Актуальні проблеми економіки.– 2003. – № 3. – С. 12–19.

УДК 657

М. Вотінова, магістр гр. ООУ-18МЗ-1,4
Д. Сімійон, магістр гр. ООУ-18МЗ-1,4
Центральноукраїнський національний технічний університет

ОСОБЛИВОСТІ ДІЯЛЬНОСТІ НЕПРИБУТКОВИХ УСТАНОВ

У статті здійснено дослідження особливостей діяльності неприбуткових установ. Проаналізовані нормативні та законодавчі документи, які регламентують їх діяльність. Вивчено закордонний досвід функціонування неприбуткових установ.

неприбуткові установи, закордонний досвід, бюджетні установи, небюджетні установи, регулювання діяльності

Постановка проблеми. На сучасному етапі у розвинених країн світу істотну роль відіграють неприбуткові організації, що мають на меті соціальні, благодійні, культурні, освітні, політичні, наукові та інші цілі, спрямовані на досягнення суспільних благ. Необхідність реалізації демократичних принципів суспільного розвитку в Україні зумовили потребу в оптимальних змінах загального процесу регулювання діяльності неприбуткових установ.

Незважаючи на поступову автономізацію та збільшення частки самофінансування бюджетних установ, спрямування їх у напрям залучення альтернативних джерел покриття власних видатків, все ж таки бюджетне фінансування найближчою перспективою залишатиметься пріоритетним для більшості неприбуткових організацій України.

Аналіз останніх досліджень і публікацій. Питання діяльності різних видів неприбуткових установ висвітлювались у працях таких учених, як С. Л. Лондар, С. О. Левицька, Я. В. Олійник, О. І. Іваненко, В. П. Хомутенко та ін.. Комплексне дослідження економічної діяльності неприбуткових організацій як окремого об’єкта обліку, особливостей системи їх обліку, методології та організації майже не проводилось. Економіці

житлово-комунального господарства та обліку в ньому присвячені праці Гури Н. О., Качали Т. М., Крамаренко Г. А., Лисенко Н. М., Онищука Г. І., Погорєлової В. В., Полуянова В. П., Семчука Г. М., Чиж В. І.. Колективом авторів під редакцією Пархоменко В. М. та Сопко В. В. була зроблена спроба розробити уніфіковану систему обліку та звітності неприбуткових (громадських) організацій. Теоретичні та практичні основи обліку, організації та складання фінансової звітності в бюджетних установах досліджували Свірко С. В., Левицька С. О., Ткаченко І. Т. Проте потребують подальшого дослідження питання особливостей діяльності неприбуткових бюджетних установ.

Мета статті – дослідження особливостей діяльності неприбуткових установ.

Виклад основного матеріалу. Для вирішення соціальних проблем, які постають перед сучасним суспільством, є необхідним безперебійне функціонування установ і організацій. З цією метою загальноприйнятим у всьому світі є функціонування неприбуткових організацій.

Неприбуткові установи називають третім сектором економіки. Їх значення у соціально-економічному розвитку різних держав важко переоцінити. Метою створення цих установ є досягнення соціальних, благодійних, культурних, освітніх, наукових цілей, захисту прав і законних інтересів громадян, а також їх здоров'я, розвитку фізкультури і спорту, задоволення духовних та інших нематеріальних потреб громадян та у інших цілях, які спрямовані на досягнення суспільних благ. Неприбуткові установи представлені громадськими організаціями, спілками, фондами, асоціаціями тощо.

Усі неприбуткові установи України поділяються на бюджетні і небюджетні. Крім того, їх розрізняють за особливостями оподаткування та ознаками неприбутковості. Діяльність різних груп таких установ регламентується відповідними законами, проте існує багато невирішених питань у частині обліку, звітності та їх оподаткування, що призводить як до проблем у їх діяльності, так і до зловживань з їх боку.

Для неприбуткових установ характерними є неприбутковість, некомерційність; значну їх частину становлять благодійні організації. Склад таких установ та їх класифікація різняться у різних країнах, проте їх об'єднує наявність бюджетних, громадських і релігійних організацій, товариств власників житла тощо. Водночас цільова спрямованість неприбуткових установ у розвинутих країнах дещо відрізняється від українських. Так, діяльність багатьох з них спрямована на захист прав людини, збереження енергії та використання альтернативних її видів.

Теоретичною основою класифікації неприбуткових установ, перш за все, є особливості їх цілей і діяльності. За цією ознакою розрізняють громадські організації, недержавні пенсійні фонди, кредитні спілки тощо. Але для повноти класифікації враховують джерела фінансування, особливості оподаткування тощо.

Відповідно до ст. 85 Цивільного кодексу України непідприємницькими товариствами є товариства, які не мають на меті одержання прибутку для його наступного розподілу між учасниками. При цьому кодексом зазначено, що особливості правового статусу окремих видів непідприємницьких товариств встановлюються законом [4].

Згідно до п. 14.1.121 Податкового кодексу України зазначається, що неприбуткові підприємства, установи та організації – це неприбуткові підприємства, установи та організації, які не є платниками податку на прибуток підприємств відповідно до пункту 133.4 статті 133 Податкового кодексу України. Пунктом 133.4 статті 133 Податкового кодексу України прописано, що не є платниками податку неприбуткові підприємства, установи та організації у порядку та на таких умовах:

- неприбутковим підприємством, установою та організацією для цілей оподаткування податком на прибуток підприємств є підприємство, установа та організація (неприбуткова організація), що одночасно відповідає таким вимогам:

- утворена та зареєстрована в порядку, визначеному законом, що регулює діяльність відповідної неприбуткової організації;

- установчі документи якої (або установчі документи організації вищого рівня, на підставі яких діє неприбуткова організація відповідно до закону) містять заборону розподілу отриманих доходів (прибутків) або їх частини серед засновників (учасників у розумінні Цивільного кодексу України), членів такої організації, працівників (крім оплати їхньої праці, нарахування єдиного соціального внеску), членів органів управління та інших пов'язаних з ними осіб. При цьому не вважається розподілом отриманих доходів (прибутків) фінансування таких видатків, як: доходи (прибутки) неприбуткової організації які використовуються виключно для фінансування видатків на утримання такої неприбуткової організації, реалізації мети (цілей, завдань) та напрямів діяльності, визначених її установчими документами; доходи неприбуткових релігійних організацій використовуються також для здійснення неприбуткової (добродійної) діяльності, передбаченої законом для релігійних організацій, у тому числі надання гуманітарної допомоги, здійснення благодійної діяльності, милосердя.

- установчі документи якої (або установчі документи організації вищого рівня, на підставі яких діє неприбуткова організація відповідно до закону) передбачають передачу активів одній або кільком неприбутковим організаціям відповідного виду, іншим юридичним особам, що здійснюють недержавне пенсійне забезпечення відповідно до закону (для недержавних пенсійних фондів), або зарахування до доходу бюджету у разі припинення юридичної особи (у результаті її ліквідації, злиття, поділу, приєднання або перетворення). Положення цього абзацу не поширюється на об'єднання та асоціації об'єднань співвласників багатоквартирних будинків;

- внесена контролюючим органом до Реєстру неприбуткових установ та організацій.

Відповідно до Податкового кодексу України вимоги положення щодо вимог наявності установчих документів не поширюються на бюджетні установи.

Доходи (прибутки) неприбуткової організації використовуються виключно для фінансування видатків на утримання такої неприбуткової організації, реалізації мети (цілей, завдань) та напрямів діяльності, визначених її установчими документами.

Доходи неприбуткових релігійних організацій використовуються також для здійснення неприбуткової (добродійної) діяльності, передбаченої законом для релігійних організацій, у тому числі надання гуманітарної допомоги, здійснення благодійної діяльності, милосердя.

У разі недотримання неприбутковою або релігійної організацією вимог, визначених пунктом 133.4 статті 133 Податкового кодексу України, така неприбуткова організація зобов'язана подати у строк, визначений для місячного податкового (звітного) періоду, звіт про використання доходів (прибутків) неприбуткової організації за період з початку року (або з початку визнання організації неприбутковою в установленому порядку, якщо таке визнання відбулося пізніше) по останній день місяця, в якому вчинено таке порушення, та зазначити і сплатити суму самостійно нарахованого податкового зобов'язання з податку на прибуток. Податкове зобов'язання розраховується виходячи із суми операції (операцій) нецільового використання активів. Така неприбуткова організація виключається контролюючим органом з Реєстру неприбуткових установ та організацій та вважається платником податку на прибуток для цілей оподаткування з першого дня місяця, наступного за місяцем, у якому вчинено таке порушення.

За період з першого дня місяця, наступного за місяцем, у якому вчинено таке порушення, по 31 грудня податкового (звітного) року така неприбуткова організація зобов'язана щокварталу подавати до контролюючого органу податкову декларацію з податку на прибуток (з наростаючим підсумком), сплачувати податок у строк, визначений для квартального періоду та подавати фінансову звітність у порядку, встановленому для платників податку на прибуток.

З наступного податкового (звітного) року така неприбуткова організація подає податкову декларацію з податку на прибуток і фінансову звітність та сплачує податок на прибуток у порядку, встановленому цим розділом для платників податку на прибуток.

Встановлення контролюючим органом відповідно до норм Податкового кодексу України факту використання неприбутковою організацією доходів (прибутків) для цілей інших, ніж передбачені підпунктом 133.4.2, є підставою для виключення такої організації з Реєстру неприбуткових установ та організацій і нарахування податкового зобов'язання з податку на прибуток підприємств, штрафних санкцій і пені відповідно до норм Податкового кодексу України. Податкові зобов'язання, штрафні санкції і пеня нараховуються, починаючи з першого числа місяця, в якому вчинено таке порушення.

Порядок ведення Реєстру неприбуткових установ та організацій, включення неприбуткових підприємств, установ та організацій до Реєстру та виключення з Реєстру встановлює Кабінет Міністрів України.

До неприбуткових організацій, що відповідають вимогам Податкового кодексу України і не є платниками податку, зокрема, можуть бути віднесені: бюджетні установи; громадські об'єднання, політичні партії, творчі спілки, релігійні організації, благодійні організації, пенсійні фонди; спілки, асоціації та інші об'єднання юридичних осіб; житлово-будівельні кооперативи (з першого числа місяця, наступного за місяцем, в якому відповідно до закону здійснено прийняття в експлуатацію закінченого будівництвом житлового будинку і такий житловий будинок споруджувався або придбавався житлово-будівельним (житловим) кооперативом), дачні (дачно-будівельні), садівничі та гаражні (гаражно-будівельні) кооперативи (товариства); об'єднання співвласників багатоквартирного будинку, асоціації власників жилих будинків; професійні спілки, їх об'єднання та організації профспілок, а також організації роботодавців та їх об'єднання; сільськогосподарські обслуговуючі кооперативи, кооперативні об'єднання сільськогосподарських обслуговуючих кооперативів; інші юридичні особи, діяльність яких відповідає вимогам цього пункту.

Для неприбуткових організацій, які відповідають вимогам Податкового кодексу України та внесені до Реєстру неприбуткових установ та організацій, встановлюється річний податковий (звітний) період.

Не є платниками податку суб'єкти господарювання, що застосовують спрощену систему оподаткування, обліку та звітності, визначені главою 1 розділу XIV Податкового кодексу України [4].

Національний банк України здійснює розрахунки з Державним бюджетом України відповідно до Закону України «Про Національний банк України».

Згідно з п. 2 ст. 3 Господарського кодексу України, господарська діяльність може здійснюватись і без мети одержання прибутку (некомерційна господарська діяльність) [1]. Відповідно до п. 3 ст. 3 ГКУ, «діяльність негосподарюючих суб'єктів, спрямована на створення і підтримання необхідних матеріально_технічних умов їх функціонування... є господарчим забезпеченням діяльності негосподарюючих суб'єктів» [1]. При цьому у ст. 86 Цивільного кодексу України визначено, що непідприємницькі товариства паралельно з основною діяльністю можуть здійснювати і підприємницьку, якщо вона не заборонена законодавчо. Якщо ж діяльність у формі підприємництва суб'єктам господарювання заборонена, вони здійснюють некомерційну господарську діяльність відповідно до гл. 5 Господарського кодексу України.

Відповідно до статті 52 глави 5 Господарського кодексу України некомерційне господарювання – це самостійна систематична господарська діяльність, що здійснюється суб'єктами господарювання і яка спрямована на досягнення економічних, соціальних та інших результатів без мети одержання прибутку.

Некомерційна господарська діяльність здійснюється суб'єктами господарювання державного або комунального секторів економіки у галузях (видах діяльності), в яких відповідно до статті 12 Господарського кодексу України забороняється підприємництво, на основі рішення відповідного органу державної влади чи органу місцевого самоврядування. Некомерційна господарська діяльність може здійснюватися також іншими суб'єктами господарювання, яким здійснення господарської діяльності у формі підприємництва

забороняється законом. Не можуть здійснювати некомерційну господарську діяльність органи державної влади, органи місцевого самоврядування, їх посадові особи.

Згідно до статті 54 глави 5 Господарського кодексу України на суб'єктів господарювання, які здійснюють некомерційну господарську діяльність, поширюються загальні вимоги щодо регулювання господарської діяльності з урахуванням особливостей її здійснення різними суб'єктами господарювання, які визначаються Господарським кодексом України та іншими законодавчими актами.

При укладенні трудового договору (контракту, угоди) суб'єкт господарювання, що здійснює некомерційну господарську діяльність, зобов'язаний забезпечити належні і безпечні умови праці, її оплату не нижчу від визначеного законом мінімального розміру, а також забезпечити інші соціальні гарантії, передбачені законом [1].

З точки зору бухгалтерського обліку, відмінності між неприбутковими установами та комерційними підприємствами (організаціями) насамперед полягають у відсутності процесів виробництва і реалізації продукції (послуг), отриманні значної частини доходів у вигляді цільового фінансування від членів і не членів організації, відсутності статутного капіталу у більшості неприбуткових установ і поставок товарів (робіт, послуг) за основною діяльністю, тобто об’єкта оподаткування ПДВ.

Враховуючи зазначені вище особливості неприбуткових установ, можна дати таке визначення неприбуткової установи: це самостійний господарюючий суб’єкт, який має права юридичної особи і здійснює діяльність, передбачену установчими документами, має самостійний баланс, поточні рахунки в банках, печатку, веде бухгалтерський облік, подає звітність відповідно до законодавства, не має на меті отримання прибутку.

Діяльність більшості неприбуткових установ регулюється відповідними Законами України: «Про об’єднання громадян», «Про свободу совісті та релігійні організації», «Про гуманітарну допомогу», «Про благодійництво та благодійні організації» та ін. Необхідною умовою для отримання статусу неприбуткової організації чи установи є включення до відповідного Реєстру. При цьому неприбутковим установам присвоюється ознака неприбутковості, яка позначається кодами секції S «Надання інших видів послуг» п. 94 [2].

Згідно з Класифікатором видів економічної діяльності (КВЕД), за видом економічної діяльності неприбутковим установам надаються наступні коди:

— 94.11 – діяльність організацій промисловців і підприємців;
— 94.12 – діяльність професійних громадських організацій;
— 94.20 – діяльність професійних спілок;
— 94.91 – діяльність релігійних організацій;
— 94.92 – діяльність політичних організацій;
— 94.99 – діяльність інших громадських організацій, н.в.і.у [2].

Бюджетним організаціям, як неприбутковим установам, відповідно до Класифікатора видів економічної діяльності надаються коди відповідно до специфіки діяльності. Так, сфері освіті присвоюють коди секції P «Освіта»; сфері охорони здоров’я – секції Q «Охорона здоров’я та надання соціальної допомоги»; мистецтво, спорт, розваги та відпочинок - секції R «Мистецтво, спорт, розваги та відпочинок»; тощо. Слід зазначити, що такий підхід до надання кодів КВЕД певною мірою ускладнює отримання статистичної інформації щодо їх діяльності.

Крім того, в Україні законодавчо не визначено органу, безпосередньо відповідального за формування та реалізацію політики у сфері бухгалтерського обліку та фінансової звітності неприбуткових установ, який би забезпечував розробку нормативно-правових актів щодо ведення бухгалтерського обліку та складання фінансової звітності неприбуткового сектору, а також способів методологічного публічного контролю за їх діяльністю.

Неприбуткові установи можуть піти на зловживання, здійснювати дії, що суперечать статутним документам. Але в Україні здійснюється лише нагляд за діяльністю некомерційних організацій: органами легалізації, які контролюють дотримання положень статуту організації; податковими органами, які здійснюють контроль за правильним і

своєчасним поданням податкової та фінансової звітності; - органами прокуратури, які здійснюють контроль в порядку загального нагляду, як це передбачено Конституцією України.

Для забезпечення формування та реалізації політики державного регулювання у сфері бухгалтерського обліку та фінансової звітності неприбуткових установ та належного контролю законності та цільової спрямованості їх діяльності в Україні мають бути встановлені відповідні повноваження. Проведення послідовної державної облікової політики у сфері неприбуткового сектору забезпечить всіх зацікавлених користувачів, перш за все державу, донорів та суспільство, необхідною достатньою, відкритою інформацією про діяльність некомерційних організацій. Ефективність співпраці між владою та некомерційними організаціями в різних країнах досягається через використання різноманітних підходів.

Інтеграція державного і недержавного секторів також різна, але робота ведеться за єдиної мети – формування ефективної системи співпраці держави та громадськості.

Найбільш вдалий та довгий в історичної ретроспективі досвід проведення державної облікової політики щодо регулювання діяльності некомерційних організації мають Сполучені Штати Америки. Регулювання діяльності некомерційних організацій (Non-Profit Corporation) здійснюється на основі податкового законодавства. Податковий кодекс містить критерії надання статусу звільненої від оподаткування організації. Нагляд за діяльністю неприбуткових установ здійснюють спеціальні підрозділи податкових органів, які також проводять аудиторські перевірки правильності витрачання коштів. У разі виявлення порушень такій організації відмовляється у продовженні реєстрації.

З 1973 року для встановлення стандартів фінансової звітності, які регулюють підготовку фінансових звітів неурядовими організаціями було призначено Фінансове Управління Стандартів Бухгалтерського обліку (FASB), яке офіційно визнано Комісією з Цінних Паперів і обмінного курсу (SEC) і Американським інститутом дипломованих громадських бухгалтерів. Місією FASB є створення і вдосконалення стандартів фінансового обліку та звітності неурядових організацій з метою надання корисної інформації інвесторам та іншим користувачам фінансової звітності. З цією місією FASB розробляє стандарти бухгалтерського обліку FASB Codification TM (Кодифікація стандартів бухгалтерського обліку), які є стандартами бухгалтерського обліку та звітності, за винятком тих, які видані SEC, визнані FASB та можуть застосовуватися неурядовими організаціями.

Крім США, вдалий досвід регулювання некомерційним сектором накопичений у Канаді, де він здійснюється комітетом, що об’єднує представників неурядових організацій. Регулювання діяльності некомерційних організацій проводиться, як і в США, на основі податкового законодавства, за яким вони звільнені від сплати податку на прибуток. Реєстрацію і нагляд за діяльністю некомерційних організацій здійснюють уряди провінцій.

Некомерційні організації підзвітні Агентству по доходах і митних зборах (Canada Customs and Revenue Agency), юрисдикцією якого є реєстрація некомерційних організацій на федеральному рівні і прямий контроль за їх фінансовою діяльністю, а також аудиторська перевірка їхньої діяльності. У разі виявлення порушень, некомерційним організаціям відмовляють у подальшій реєстрації.

Різноманітність підходів щодо формування співпраці держави та громадськості у створенні законодавчих умов діяльності некомерційних організацій дає можливість стверджувати про необхідність розробки власних форм встановлення повноважень щодо формування та забезпечення реалізації політики державного регулювання у сфері бухгалтерського обліку та фінансової звітності некомерційних організацій, тим більше що в Україні діяльність некомерційних організацій не розглядається як аналог підприємницьких комерційних суб’єктів господарювання та вони виділені як окремий вид організацій, метою діяльності яких не є отримання прибутку.

Вирішення поставлених питань та ефективність функціонування національної системи бухгалтерського обліку в цілому залежить від синхронізації розвитку її елементів,

забезпечення якої має бути пріоритетом при проведенні загальнодержавної політики у сфері бухгалтерського обліку як частини економічної політики держави. Удосконалення домінуючої інституціональної матриці організації бухгалтерського обліку в частині складу агентів загальнодержавного рівня, які формують та реалізують політику у сфері бухгалтерського обліку, значною мірою сприяє формуванню сприятливого інституціонального середовища та ефективних механізмів поділу повноважень між інституціями щодо регулювання бухгалтерським обліку та складання фінансової звітності як інституціональних чинників макроекономічного регулювання національної системи бухгалтерського обліку.

Проте навіть у такій складній розгалуженій системі нормативно-правового регулювання, яка діє в Україні, залишилися сфери економічної діяльності, в яких існує нагальна необхідність вирішення проблеми неврегульованості бухгалтерського обліку. Перш за все це стосується некомерційного сектору, який в Україні набуває все більшого економічного та соціального впливу на суспільство. Так званий «третій сектор» або неприбуткові підприємства за роки незалежності набули в Україні значного поширення та швидко розвиваються. Діяльність неприбуткових підприємств охоплює широкий спектр громадського суспільства: економіку, політику, науку, культуру, освіту. Це благодійні фонди, молодіжні, професійні, дитячі, жіночі, ветеранські, релігійні організації, політичні партії, профспілки, недержавні пенсійні фонди, аналітичні центри.

Оцінка стану нормативно-правового забезпечення бухгалтерського обліку та складання фінансової звітності дозволяє констатувати, що в Україні відсутні нормативно-правові акти, які враховують специфіку діяльності некомерційних підприємств. Інформація про неприбуткові установи та правила їх діяльності має бути доступна державним органам, донорам, суспільству та кожному зацікавленому громадянину. Тому необхідність створення сприятливих умов для розвитку інститутів громадянського суспільства та подальшої їх інтеграції в міжнародні ринки шляхом збільшення транспарентності, підзвітності і підконтрольності обумовлює доцільність розробки спеціального методологічного, методичного та організаційного забезпечення бухгалтерського обліку та фінансової звітності некомерційних підприємств та організацій України.

Ще однією особливістю інституціонального середовища бухгалтерського обліку є обмеженість його дії. Так, застосування діючих національних стандартів розповсюджується на всіх юридичних осіб, створених відповідно до законодавства України, незалежно від їх організаційно-правових форм та форм власності, а також на представництва іноземних суб'єктів господарської діяльності, які зобов'язані вести бухгалтерський облік та подавати фінансову звітність згідно з законодавством. В Україні метою державного регулювання бухгалтерського обліку та фінансової звітності наголошується «створення єдиних правил ведення бухгалтерського обліку та складання фінансової звітності, які є обов'язковими для всіх підприємств». Створення таких правил має забезпечувати існування єдиної системи бухгалтерського обліку та фінансової звітності. Але об'єктивним результатом врахування специфіки діяльності суб'єктів господарювання в умовах ринкового господарства є фактичний розподіл єдиної системи на підсистеми.

Реально в Україні існує складна система нормативного регулювання бухгалтерського обліку, відповідно до якої порядок ведення бухгалтерського обліку та складання фінансової звітності встановлюється різними органами виконавчої влади, що забезпечують формування державної фінансової політики.

Проте така обмеженість є об'єктивною та забезпечує врахування специфіки економічної діяльності та правового регулювання бухгалтерського обліку у різних сферах економічної діяльності за умови відповідності нормативно-правовим актам вищої юридичної сили.

Проблемним аспектом нормативного регулювання бухгалтерського обліку є його спрямованість лише на затвердження нормативно-правових актів та невизначеність виконавців та органів, відповідальних за їх розробку.

Ловінська Л. Г. порушувала питання: «Хто повинен здійснювати реформування обліку шляхом розробки та ухвалення відповідних нормативних актів, хто має впроваджувати їх в повсякденну практику бухгалтера, хто повинен нести відповідальність за ефективність цього процесу?» [3].

Далі вона зазначала, що Закон № 996-XIV «не дає відповіді на питання, у чому зміст державного регулювання бухгалтерського обліку, хто є його суб'єктом, а що – об'єктом, які складові входять в національну систему обліку, який взаємозв'язок між ними є і яка їх підпорядкованість». Станом на 2019 рік ситуація мало у чому змінилася. Законом № 996-XI визначений орган, який затверджує національні положення (стандарти) бухгалтерського обліку – «центральний орган виконавчої влади, що забезпечує формування державної фінансової політики». До внесення змін до Закону України «Про бухгалтерський облік та фінансову звітність» регулювання питань методології бухгалтерського обліку та фінансової звітності покладалося безпосередньо на Міністерство фінансів України (ст. 6), при якому діяла як дорадчий орган, відповідальний за організацію розробки та розгляд проектів національних стандартів бухгалтерського обліку – Методологічна рада з бухгалтерського обліку (ст. 7). Згідно із Законом України «Про внесення змін до деяких законодавчих актів України щодо діяльності Міністерства фінансів України, Міністерства економічного розвитку і торгівлі України, інших центральних органів виконавчої влади, діяльність яких спрямовується та координується через відповідних міністрів» № 5463-VI від 16.10.2012 статтю 7 було виключено. Все це дозволяє стверджувати про непрозорість процесу розробки нормативної бази бухгалтерського обліку.

Висновки. Створення і функціонування неприбуткових організацій у всьому світі покликано вирішувати соціальні проблеми, які постають перед сучасним суспільством. Метою створення цих установ є досягнення соціальних, благодійних, культурних, освітніх, наукових цілей, захисту прав і законних інтересів громадян, а також їх здоров'я, розвитку фізкультури і спорту, задоволення духовних та інших нематеріальних потреб громадян та у інших цілях, які спрямовані на досягнення суспільних благ.

Усі неприбуткові установи України поділяються на бюджетні і небюджетні. Крім того, їх розрізняють за особливостями оподаткування та ознаками неприбутковості. Діяльність різних груп таких установ регламентується відповідними законами, проте існує багато невирішених питань у частині обліку, звітності та їх оподаткування, що призводить як до проблем у їх діяльності, так і до зловживань з їх боку.

Список літератури

1. Господарський кодекс України [Електронний ресурс] : Кодекс від 16.01.2003 р. № 436-IV.Режим доступу: http://zakon4.rada.gov.ua /laws/show/436-15
2. Класифікація видів економічної діяльності (КВЕД-2010) [Електронний ресурс]. Режим доступу: https://evrovektor.com › kved
3. Ловінська Л. Г. Вплив євроінтеграційних процесів на розвиток бухгалтерського обліку та звітності в Україні / Л. Г. Ловінська // Фінанси України. - 2014. - №9. -С. 21–30.
4. Податковий кодекс України № 2755-VI від 02.12.2012. [Електронний ресурс]. Режим доступу: http://sts.gov.ua/nk
5. Цивільний кодекс України [Електронний ресурс]: Кодекс від 16.03.2003 № 435 – IV. Режим доступу: http://zakon3.rada.gov.ua

УДК 657

К. Глинська, магістр гр. ОО-18/М-1,4
Центральноукраїнський національний технічний університет

ВПЛИВ ОСОБЛИВОСТЕЙ ДІЯЛЬНОСТІ БУДІВЕЛЬНИХ ПІДПРИЄМСТВ НА ПОБУДОВУ ОБЛІКУ ДІЯЛЬНОСТІ

Наявність розбіжностей між положеннями різних нормативно-правових документів, якими регламентовано облік будівельних підприємств, створює труднощі у частині розуміння сутності поняття «будівництво» як виду економічної діяльності. У статті досліджено сутність поняття «будівництво», розкрито значення будівництва в умовах сьогодення при формуванні облікової інформації. Проаналізовано проблемні питання щодо використання даного поняття у різних нормативно-правових документах, розглянуто можливі шляхи їх вирішення. Обґрунтовано необхідність узгодження положень досліджених у статті нормативних документів, якими визначається облік будівельних підприємств.
будівництво, облік, будівельне підприємство, методологія обліку, вид економічної діяльності, звітність, будівельна продукція

Наличие разногласий между нормами различных нормативно-правовых документов, которыми регламентируется учет на строительных предприятиях, создает трудности в части понимания сущности понятия «строительство» как вида экономической деятельности. В статье исследована сущность понятия «строительство», раскрыто значение строительства в сегодняшних условиях при формировании учетной информации. Проанализированы проблемные вопросы использовани данного понятия в различных нормативно-правовых документах, рассмотрены возможные пути их решения. Обоснована необходимость согласования положений исследованных в статье нормативных документов, которыми определяется учет строительных предприятий
строительство, учет, строительное предприятие, методология учета, вид экономической деятельности, отчетность, строительная продукция

Постановка проблеми. Будівництво, як вид підприємницької діяльності, в сучасних умовах – одна з найпоширеніших та прибуткових сфер діяльності. У той же час це дуже специфічний вид діяльності, який працює на віддалену перспективу, потребує значних первинних інвестицій, який тривалий час буде займати певну територію. На даному етапі розвитку нашої країни ринок будівництва є одним з таких ринків, що найдинамічніше розвивається. Як відомо, будівництво – це один з найтриваліших виробничих процесів, до якого відносяться ті об'єкти, суб'єкти або процеси, які тривалий час існують. При цьому під будівництвом розуміють як спорудження нового об'єкту, так і реставрацію, реконструкцію, розширення і добудову об'єктів, а також виконання монтажних робіт.

Водночас, будівництво базується на реальних інвестиціях, для здійснення яких необхідна достовірна та оперативна інформаційна база про фінансові результати суб'єктів господарювання, спрямована на задоволення потреб різних інвесторів як основних її користувачів. Саме системою бухгалтерського обліку створюється значний обсяг цієї інформації, з огляду на важливість якої, особливо що стосується фінансових результатів діяльності будівельних підприємств, зростає значення контрольних процедур, які здійснюються на всіх етапах будівництва. Базовими формуючими елементами фінансових результатів виступають показники доходів і витрат.

Аналіз останніх досліджень і публікацій. Вагомий внесок у дослідження питань обліку доходів і витрат у будівництві зробили такі фахівці як, Атамас П. Й., Бабіч В. В., Білуха М. Т., Бутинець Ф. Ф., Валуєв Б. І., Грузінов В. П., Захожай В. Б., Карпушенко М. О., Костюшко А. О., Крушельницька О. В., Мельник Л. Г., Осовська Г. В., Продіус Ю. І., Соколов Я. В., Сопко В. В., Тітов В. І., Чалий І. Г., Швець В. Г., Юшкевич О. О. та інші.

Проте, ряд проблем, пов'язаних з дослідженням впливу особливостей діяльності будівельних підприємств на постановку та ведення обліку, залишається недостатньо дослідженим.

Постановка завдання. Мета написання статті полягає в дослідженні особливостей здійснення будівельної діяльності на постановку та ведення бухгалтерського обліку.

Виклад основного матеріалу. Будівництво є галуззю матеріального виробництва, діяльність якої спрямована на зведення нових і реконструкцію старих будівель, споруд, об'єктів виробничого та невиробничого призначення на місці їх функціонування.

Сьогодні у Цивільному кодексі України, Кодексі законів про адміністративні правопорушення використовується поняття будівництва, а у Господарському кодексі – капітального будівництва. Відтак, існує неузгодженість у використанні термінології, що ускладнює розуміння сутності даних понять (табл. 1).

Таблиця 1 – Визначення сутності понять «капітальне будівництво» та «будівництво» у нормативно-правових джерелах

№	Поняття	Назва джерела	Визначення
1.	Капітальне будівництво	Порядок державного фінан-сування капітального будівництва № 1764 від 27 грудня 2001 р.	Процес створення нових, а також розширення, реконструкція, технічне переоснащення діючих підприємств, об'єктів виробничого і невиробничого призначення, пускових
2.	Будівництво	Закон України «Про архітек-турну діяльність» від № 687-XIV 20.05.1999 р.	Нове будівництво, реконструкція, реставрація, капітальний ремонт
3.		Закон України «Про регулю-вання містобудівної діяльності» від № 3038-VI від 17.02.2011 р.	Нове будівництво, реконструкція, реставрація, капітальний ремонт об'єктів будівництва
4.		Національний класифікатор України «Класифікація видів економічної діяльності ДК 009:2010»	Вид економічної діяльності (секція F, що містить у своєму складі 3 розділи, 9 груп і 22 класи)
5.		П(С)БО 18 «Будівельні контракти» № 205 від 28 квітня 2001 р.	Спорудження нового об'єкта, реконструкція, розширення, добудова, реставрація і ремонт об'єктів, виконання монтажних робіт
6.		Методичні рекомендації з формування собівартості будівельно-монтажних робіт № 573 від 31.12.2010 р.	Спорудження нових об'єктів, реконструкція, реставрація та ремонт об'єктів
7.		Правила визначення вартості будівництва «ДСТУ Б Д.1.1-1:2013» № 293 від 05.07.2013 р.	Нове будівництво, реконструкція, капітальний ремонт та технічне переосна-щення будинків, будівель та споруд будь-якого призначення, їх комплексів, лінійних об'єктів інженерно-транс-портної інфраструктури, а також рестав-рація пам'яток архітектури та містобудування
8.		Порядок розроблення проектної документації на будівництво об'єктів: наказ Міністерства	Нове будівництво, реконструкція, технічне переоснащення діючих підприємств, реставрація та капітальний

		регіонального розвитку, будів-ництва та житлово-комуналь-ного господарства України ДБН А.2.2-3-2014 № 45 від 16.05.2011 р.	ремонт об'єктів будівництва
9.		Склад та зміст проектної документації на будівництво: ДБН А.2.2-3-2014	Нове будівництво, реконструкція, капітальний ремонт та технічне переоснащення об'єктів будівництва

Отже, за даними табл. 1 можна зробити висновок, що в нормативних джерелах застосовується переважно поняття «будівництво», визначення сутності якого схожі, проте не однакові. Беручи за основу тлумачення будівництва в облікових нормативних документах, його визначення може бути представлено як спорудження нового об'єкта, реновація (реконструкція, розширення, добудова, реставрація, ремонт, технічне переоснащення об'єктів будівництва), виконання будівельних робіт.

Крім того, в основних документах, якими керуються при побудові обліку на будівельних підприємствах, визначення будівництва також відрізняються, зокрема, добудова, розширення й виконання монтажних робіт як складові будівництва заявлені лише в П(С)БО 18 «Будівельні контракти». Згідно з Правилами визначення вартості будівництва «ДСТУ Б Д.1.1-1:2013» № 293 від 05.07.2013 монтажні роботи є складовою будівельних робіт разом з ремонтно-будівельними, реставраційно-відновлювальними та пусконалагоджувальними роботами (п. 5.1.3). У Національному класифікаторі України «Класифікація видів економічної діяльності ДК 009:2010» від 11.10.2010 № 457 (зі змінами) в структурі секції F «Будівництво» монтажні роботи виокремлено як складову будівельних. У Методичних рекомендаціях з формування собівартості будівельно-монтажних робіт № 573 паралельно використовуються обидва поняття: «будівельні роботи» (розділ 7) та «будівельно-монтажні роботи» (розділ 1).

У формі статистичної звітності «Структурне обстеження підприємства» (№ 1-підприємництво (річна)), затвердженої наказом Державної служби статистики України 24.06.2016 р. № 97, будівельні підприємства зобов'язані відображати загальний обсяг будівельних робіт, що виконаний підрядником (розділ 5 «Інші показники», рядок 501 «Дохід від виконання будівельних робіт на умовах підряду (без ПДВ)». Така ж інформація має бути заявлена у Звіті про виконання будівельних робіт (№ 1-кб), затвердженому наказом Державної служби статистики України від 26.07.2016 р. № 129, де в розділі 2 «Обсяг реалізованих будівельних робіт» зазначається обсяг реалізованих будівельних робіт, (ряд. 02), у тому числі за договорами субпідряду (ряд. 021). Отже, наведення у статистичній звітності інформації про монтажні роботи будівельних підприємств не передбачено.

Зважаючи на викладене вище, під будівництвом пропонуємо розуміти спорудження нового об'єкта, реновацію (реконструкцію, розширення, добудову, реставрацію, ремонт, технічне переоснащення об'єктів будівництва), виконання будівельних робіт. Використання даного визначення дасть змогу уніфікувати розбіжності в законодавстві у частині тлумачення сутності будівництва. Воно лаконічне, змістовне і спрямоване на усунення відмінностей між законодавчими документами, якими керуються представники бухгалтерських служб при веденні бухгалтерського обліку будівельних підприємств.

Специфіка діяльності будівельних підприємств зумовлює й певні особливості організації та ведення обліку на будівельних підприємствах. Узагальнення підходів фахівців щодо особливостей організації бухгалтерського обліку будівельних підприємств наведено в табл. 2.

Таблиця 2 – Особливості організації бухгалтерського обліку будівельних підприємств

№	Особливості організації бухгалтерського обліку	Бутинець Ф.Ф.	Захожай В.Б.	Швець В.Г.	Сопко В.В.	Атамас П.Й.
1	Виробничий процес здійснюється на нерухомих об’єктах при рухомо-му характері роботи засобів праці	-	-	+	-	+
2	Велика тривалість виробничого циклу	+	+	+	+	+
3	Безцехова структура будівельних організацій	+	-	-	-	+
4	Покупець (замовник) часто здійснює періодичні платежі	-	+	-	+	+
5	Територіальна розгалуженість будівельних майданчиків	+	+	-	+	-
6	Об'єкти будівництва знаходяться на відкритій місцевості, вплив кліматичних умов	+	+	-	+	-
7	У будівництві існує велика залежність від суміжників	+	+	-	+	-
8	Собівартість будівельних послуг розраховується на основі технічної та кошторисної документації	-	-	+	+	-
9	Специфіка обліку тимчасових нетитульних споруд	-	-	+	-	+

На основі аналізу праць вітчизняних науковців щодо висвітлення сутності організаційно-технологічних особливостей будівництва проведено їх виокремлення у двох площинах: будівельного процесу (значна тривалість процесу будівництва; різноманітність учасників будівельного процесу; територіальна розгалуженість об’єктів будівництва; залежність від природних факторів) та будівельної продукції (особливий характер розрахунків за готову продукцію; особливості ціноутворення на будівельну продукцію; нерухомість будівельної продукції при постійному переміщенні засобів праці і робітників за об’єктами будівництва) і досліджено вплив перерахованих особливостей будівництва на облік та контроль доходів і витрат основної діяльності (рис. 1).

Узагальнення точок зору різних авторів дозволило виокремити визначальні особливості діяльності будівельних підприємств, що чинять вплив на організацію бухгалтерського обліку, є:

- виробничий процес здійснюється на нерухомих об’єктах (будівлях, спорудах) при рухомому характері роботи засобів праці (будівельних машин і механізмів);
- велика тривалість виробничого циклу – у будівництві спостерігаються значні обсяги незавершеного будівництва, об'єкти мають велику собівартість та вартість, період будівництва може тривати кілька звітних періодів. У завдання обліку входить організація постійного контролю за рівнем витрат у незавершеному будівництві, правильне визначення собівартості продукції, дотримання сум витрат, передбачених кошторисом;
- безцехова структура будівельних організацій, що зумовлює специфіку в організації обліку загальновиробничих витрат;
- покупець (замовник) часто здійснює періодичні платежі у межах загальної контрактної вартості як оплату процесу будівництва. У завдання обліку входить визначення оцінки ступеня завершеності будівництва за звітний період;

– територіальна розгалуженість будівельних майданчиків – об’єкт будівництва розробляють не за місцем розміщення виробника-виконавця, а на окремій дільниці, вказаній замовником; об’єкти виробництва знаходяться на значній відстані від апарату управління, що вимагає від бухгалтерської служби посилити контроль за збереженням матеріальних цінностей;

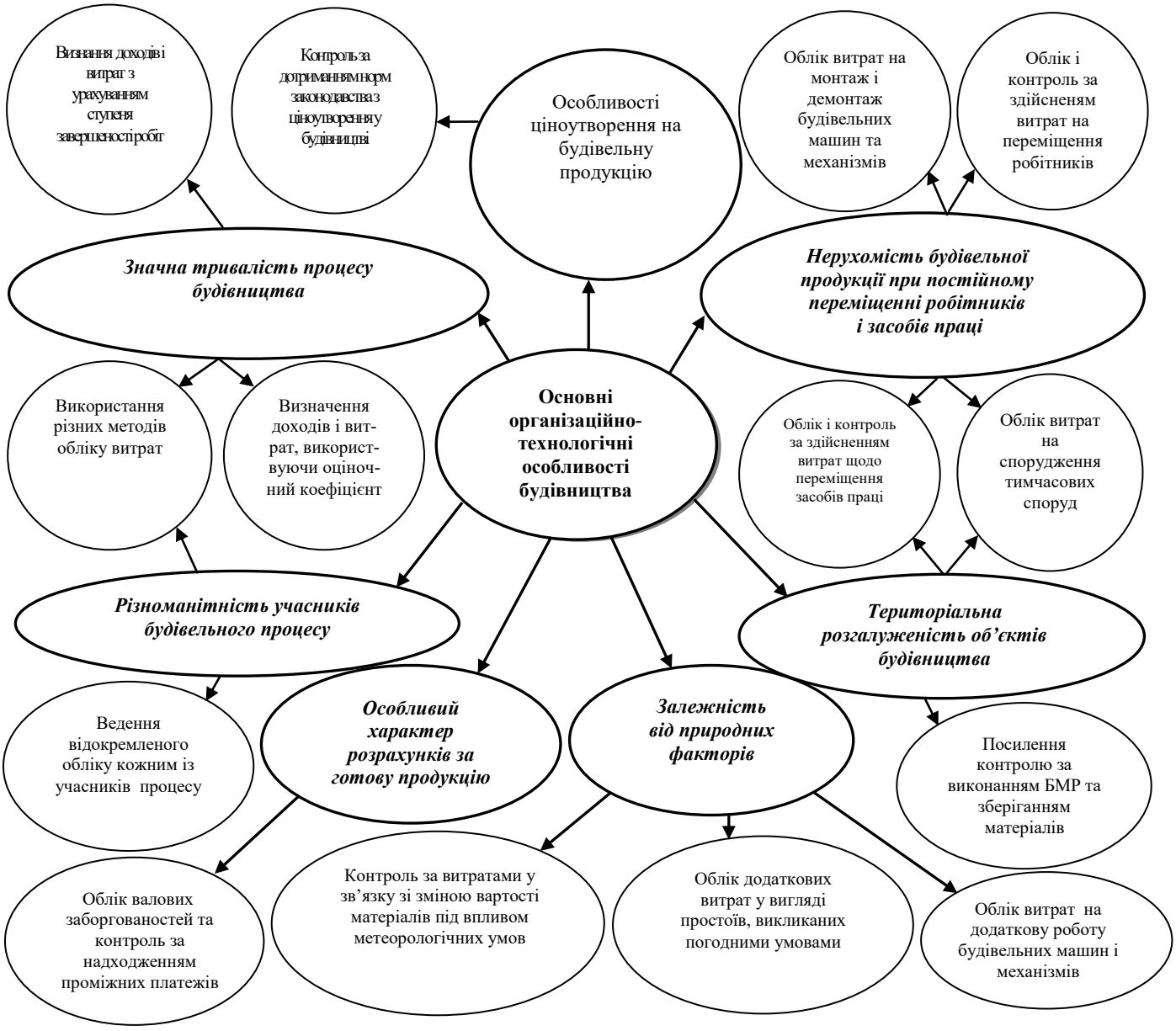


Рисунок 1 – Узагальнення визначальних особливостей діяльності будівельних підприємств, що чинять вплив на організацію бухгалтерського обліку

– об'єкти будівництва знаходяться на відкритій місцевості, спостерігається вплив кліматичних умов, що призводить до значних витрат. У бухгалтерському обліку потрібно проводити чітке розмежування природних втрат і втрат з вини матеріальних осіб;

– у будівництві існує велика залежність від суміжників, тому в завдання обліку входить контроль за дотриманням строків постачання матеріалів, виконання суміжних робіт;

– собівартість будівельних послуг, що надаються, розраховується на основі технічної та кошторисної документації;

– для забезпечення необхідних побутових умов належного рівня техніки безпеки на будівельних майданчиках часто зводять тимчасові будівлі, споруди, огорожі тощо, які обліковують як тимчасові (нетитульні) споруди на субрахунку 113 аналогічної назви.

Висновки та перспективи подальших досліджень. Взагалі, облік будівництва ґрунтується на тих самих принципах, що й облік виробництва промислової продукції. При цьому, слід зважати на особливості технології, організації та управління будівельним виробництвом, а також контролем за виробничими процесами та якістю будівництва, які й обумовлюють особливості ведення обліку таких підприємств.

Напрямками подальших досліджень можуть бути методичні напрацювання щодо розробки рекомендацій з обліку на підприємствах будівельної галузі різних обсягів діяльності.

Список літератури

1. Дерій М.В. Облік і контроль грошово-розрахункових операцій в житловому будівництві : дис. … к.е.н. : спец. 08.00.09 бухгалтерський облік, аналіз та аудит (за видами економічної діяльності) / М.В. Дерій. – Тернопіль : ТНЕУ, 2013. – 298 с.
2. Задорожний З.В. Внутрішньогосподарський облік у будівництві : монографія / З.В. Задорожний. – Тернопіль : Економічна думка, 2006. – 336 с.
3. Задорожний З.В. Облік у будівництві : підручник / Я.Д. Крупка, З.В. Задорожний, Р.О. Мельник. – Київ : Знання, 2008. – 631 с.
4. Національний класифікатор України «Класифікація видів економічної діяльності ДК 009:2010» : наказ : від 10.10.2010 : № 457 / Державний комітет України з питань технічного регулювання та споживчої політики України [Електронний ресурс]. – Режим доступу : http://zakon0.rada.gov.ua/rada/show/vb457609-10.
5. Про бухгалтерський облік та фінансову звітність в Україні : закон : від 16 липня 1999 : № 996-XIV / Верховна Рада України [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/996-14.

УДК 336.7

А. Головатий, магістр гр. ФС-18М(1,4)
Центральноукраїнський національний технічний університет

ТЕОРЕТИЧНІ ПІДХОДИ ДО ВИЗНАЧЕННЯ СУТНОСТІ РЕСУРСНОГО ПОТЕНЦІАЛУ БАНКУ

У статті досліджено сутність ресурсного потенціалу банку, визначено основні його складові. Автором узагальнено методику оцінки ресурсного потенціалу комерційного банку з виділенням системи аналітичних показників. Розглянуто найбільш важливі заходи управління комерційним банком, що можуть бути застосовані з метою нарощування його ресурсного потенціалу.

ресурсний потенціал банку, фінансові ресурси, нормативи фінансової стійкості, конкурентний аналіз

Постановка проблеми. На сучасному етапі функціонування вітчизняних комерційних банків однією зі стратегічних проблем є дефіцит фінансових ресурсів, скорочення їх обсягу, порушення оптимальної структури ресурсного потенціалу банків. Тому важливою умовою забезпечення конкурентоспроможності кожного комерційного банку є досягнення достатнього рівня його ресурсного потенціалу. Це обумовлює актуальність вивчення методичних аспектів оцінки ресурсного потенціалу комерційного банку та розробки заходів з його нарощування.

Аналіз останніх досліджень чи публікацій. Зважаючи на стратегічну роль ресурсного потенціалу для функціонування комерційного банку, в науковій літературі

неодноразово піднімалися питання його характеристики, розроблялися авторські методики визначення обсягу та достатності ресурсного потенціалу банку. Зокрема, проблемі визначення економічної сутності ресурсного потенціалу банку присвячено дослідження таких науковців як І. Барилюк, О. Васюренко, А. Єпіфанов, Г. Панасенко, М. Савлук, І. Федосік та ін. Методичним аспектам оцінки ресурсного потенціалу комерційних банків присвячені роботи таких дослідників як В. Коваленко, А. Плотніцький, Ж. Торяник, Д. Циганюк та ін. Незважаючи на численні економічні дослідження за вказаною тематикою, в наукових колах відсутні єдині підходи до розуміння сутності поняття «ресурсний потенціал банку», а також не запропоновано стандартні алгоритми оцінки ресурного потенціалу та його достатності для забезпечення роботи комерційного банку.

Формулювання цілей статті. Зважаючи на актуальність вказаних питань та беручи до уваги невисвітлені аспекти даної теми, основними завданнями статті стало узагальнення наукових підходів до розуміння економічної сутності ресурсного потенціалу банку, розробка комплексної методики оцінки його обсягу й достатності, а також формулювання пропозицій щодо оптимізації вартості та структури ресурного потенціалу комерційних банків.

Виклад основного матеріалу дослідження. В економічній літературі відсутній єдиний підхід до розуміння сутності ресурсного потенціалу комерційного банку. Зокрема, можна виділити два основних підходи:

1) за першим науковим підходом зміст досліджуваного терміну ототожнюється з поняттям «фінансові ресурси» комерційного банку. Так, наприклад, А. Єпіфанов під ресурсним потенціалом банку розуміє сукупність власних, залучених та позичкових коштів банку, що перебувають у безпосередньому його розпорядженні і використовуються на його розсуд для здійснення банківської діяльності [4, с. 89];

2) за другим науковим підходом поняття «ресурсний потенціал» та «фінансові ресурси» не є тотожними. При цьому враховується, що категорія потенціалу враховує перспективи досягнення певним результатів. Такого підходу дотримується, наприклад, М. Савлук, на думку якого ресурсний потенціал банку – це потенційні можливості його формувати свої ресурси [3, с. 13]. З певними можливостями банку пов'язаний також ресурсний потенціал у розумінні О. Васюренка та І. Федосік, за визначенням яких ресурсний потенціал комерційного банку – це сукупність усіх фінансових коштів банку, які знаходяться в безпосередньому його розпорядженні, і ресурсів, які можуть бути залучені банками внаслідок проведення ефективної повномасштабної банківської діяльності, прибутку або збитку внаслідок проведення активних операцій [2, с. 59-60].

Г. Панасенко, досліджуючи наукові підходи до розуміння сутності ресурсного потенціалу комерційного банку, виділяє три підходи до його сприйняття – ресурсний, результативний і змішаний [7, с. 296].

Ресурсний підхід – це вже розглянута нами наукова позиція, згідно якої основу ресурсного потенціалу банку складають його фінансові ресурси.

Змішаним підходом можна вважати вже наведену позицію О. Васюренка та І. Федосік, оскільки на їх думку потенціал комерційного банку складається з фінансових ресурсів, але пов'язаний також з результатами діяльності (прибуток, збиток), які створюють подальші перспективи його функціонування.

Згідно з результативним підходом потенціал комерційного банку пов'язаний, перш за все, з його результатами роботи у найближчому та віддаленому періодах.

Такого підходу значною мірою дотримується Г. Панасенко. Науковець зауважує, що «ресурсний потенціал» потрібно розглядати як максимально можливий обсяг продажу банківських продуктів і послуг за найбільш ефективного використання за часом і продуктивністю ресурсів, що є в наявності. Іншими словами, під ресурсним потенціалом банку варто розуміти граничні можливості установи в процесі формування свого потенціалу, тобто той максимум коштів, які банк може залучити на фінансовому ринку. Крім того, Г. Панасенко вважає, що основу сучасного синтезованого бачення потенціалу банківської установи повинно складати позиціонування його в системі координат «ресурси –

спроможності – компетенції», де ресурсна площина розкриває феномен перетворення можливостей на спроможності, а спроможності, водночас, через розкриття, закріплення й оновлення за допомогою навчання трансформуються в компетенції (базові і ключові). Реалізація комплексу таких можливостей відбувається за умови здійснення бізнес-процесів (як дій, спрямованих на кінцевий результат) і процесів самоорганізації (внаслідок яких частково формується колективне знання й організаційна культура) і сприяє створенню цінності для зацікавлених сторін [7, с. 295].

Практично в усіх наукових підходах домінуюче місце серед базових елементів ресурсного потенціалу банків відводиться фінансовому потенціалу, під яким розуміють потенціал власних, позичених та залучених фінансових ресурсів, що використовуються чи використовуватимуться у банківській діяльності, істотно впливаючи на обсяг та структуру усіх інших елементів ресурсного потенціалу [1, с. 17].

Загальний обсяг фінансових ресурсів комерційного банку складається із власного капіталу банку і зобов'язань. Капітал банку формується з внесків коштів його засновників (акціонерів, учасників) і прибутку. Зобов'язання банку виникають у процесі реалізації ним послуг (продукту). У загальному обсязі ресурсів, якими володіє комерційний банк, переважають зобов'язання банку. В економічній літературі зобов'язання заведено поділяти на залучені та запозичені кошти. Залучені кошти є найбільшою частиною зобов'язань банку. Це основне джерело формування ресурсів банку, які спрямовуються на проведення активних операцій. До залучених коштів банку належать залишки коштів на поточних, бюджетних рахунках клієнтів, депозитні вклади фізичних та юридичних осіб, вклади до запитання, залишки на пластикових платіжних картах, кредиторська заборгованість тощо.

В цілому, економічне значення ресурсного потенціалу банку проявляється у:

– забезпеченні банків необхідними для функціонування обсягом та структурою ресурсів;

– стимулюванні економічного зростання країни шляхом кредитування потреб суб’єктів економіки за рахунок акумульованих ресурсів;

– збереженні довгострокових конкурентних переваг банків шляхом виявлення перспективних методів формування ресурсів та напрямів їх ефективного використання, а також зростанні конкурентоспроможності банківської системи шляхом адаптації кращого іноземного досвіду організації банківської справи;

– інтеграції у світову фінансову систему шляхом виходу українських банків на міжнародні ринки капіталу та залучення іноземних інвестицій у вітчизняну банківську систему;

– інформаційно-аналітичному обґрунтуванні розроблення та реалізації стратегії формування ресурсного потенціалу;

– забезпеченні адаптації діяльності вітчизняних банків до змін ринкового середовища функціонування;

– визначенні напряму стратегічного розвитку банківської системи України шляхом реалізації банками відповідного виду ресурсної політики [1,с. 18].

Виходячи зі стратегічного значення ресурсного потенціалу, важливим завданням у процесі управління комерційним банком є оцінка обсягу та достатності ресурсного потенціалу.

На сьогодні в економічній літературі відсутній єдиний методологічний підхід до оцінки ресурсного потенціалу комерційного банку. Основні завдання оцінки ресурсного потенціалу банку можна сформулювати наступним чином:

– оцінка динаміки, складу і структури пасивів (фінансових ресурсів) банку;
– аналіз динаміки і структури капіталу банку, його достатності;
– оцінка динаміки, складу і структури зобов'язань банку;
– оцінка раціональності формування фінансових ресурсів банку та їх структури.

Тобто, в літературі звертається увага на необхідність аналізу його динаміки та структури, а також порівняння з економічними нормативами, встановленими Нацбанком.

Разом з тим, досить ефективним залишається метод оцінки ресурсного потенціалу банку на основі розрахунку інтегрального показника, який являє собою агреговану величину і допомагає визначити наявність проблем у ресурсному забезпеченні банку, його фінансову стійкість та ефективність ресурсної політики.

Так, наприклад, В. Коваленко та Ж. Торяник запропонували визначати інтегральний показник оцінки ресурсного потенціалу банку на основі наступних оціночних коефіцієнтів: норматив адекватності регулятивного капіталу; коефіцієнт ефективності використання власних коштів; коефіцієнт забезпечення зобов'язань власними коштами; коефіцієнт якості власного капіталу; коефіцієнт захищеності власного капіталу банку; коефіцієнт співвідношення зобов'язань до запитань із всіма зобов'язаннями; коефіцієнт автономності банку; коефіцієнт незалежності банку від зовнішніх джерел; коефіцієнт покриття залучених ресурсів; норматив поточної ліквідності; показник достатності ресурсного потенціалу банку [5, с. 131-132].

Схожих методичних принципів дотримуються А. Плотніцький та Д. Циганюк, які для розрахунку інтегрального показника оцінки ресурсного потенціалу комерційного банку рекомендують, поряд з деякими вищеназваними коефіцієнтами, використовувати також показник достатності ресурсного потенціалу; мультиплікатор капіталу та норматив поточної ліквідності [8, с. 94].

Вказані наукові розробки щодо оцінки ресурсного потенціалу комерційного банку є обґрунтованими і доцільними у застосуванні. Разом з тим, вони базуються виключно на ресурсному підході до розуміння сутності терміну «ресурсний потенціал банку».

Якщо ж враховувати результативний та змішаний підходи до трактування досліджуваного поняття, то в оцінку ресурсного потенціалу комерційного банку доцільно включити й стратегічний аналіз, в основі якого лежить визначення перспектив розвитку банку і потенційних можливостей досягнення ним певних результатів, зокрема і в порівнянні з найближчими конкурентами.

Результати такого аналізу дадуть можливість визначити найбільш проблемні аспекти щодо формування ресурсного потенціалу банку порівняно з найближчими конкурентами, а також намітити оптимальні шляхи стратегічного розвитку банківської установи.

Звичайно, на сучасному етапі розвитку вітчизняної економіки нарощування ресурсного потенціалу комерційних банків є досить важким завданням, адже довіра населення до банківської системи знаходиться за низькому рівні, іноземний капітал демонструє відтік з банківського сектору України. Тому важливим завданням банківського менеджменту в такій ситуації стає вчасне виявлення та вирішення проблем управління ресурсним потенціалом. З цією метою в літературі рекомендуються наступні заходи [6]:

1. Якісне удосконаленням уже існуючих видів послуг та пошук можливих варіантів їх модифікації з метою підвищення комфортності й задоволення потреб наявних клієнтів банку і залучення нових.
2. Використання інструментів Mystery Shopping, Mystery Call, як невід'ємної умови контролю за якістю послуг банку.
3. Пошук та розвиток принципово нових операцій та послуг.
4. Розробка стратегії депозитної політики згідно стратегії і тактики банку;
5. Підвищення рівня захисту (гарантування) вкладів громадян..
6. Активізація використання нецінових методів управління залученими коштами (реклама, рівень обслуговування, розширення спектру рахунків та послуг, комплексне обслуговування, додаткові види безкоштовних послуг, розташування філій у місцях, максимально наближених до клієнтів, пристосування графіку роботи до потреб клієнтів, надання клієнтам платіжних карток з кредитним лімітом, які дають їм право сплачувати комунальні платежі без додаткових комісій тощо).
7. Забезпечення оптимального співвідношення між зовнішніми та внутрішніми джерелами фінансових ресурсів банку;
8. Підвищення стандартів щодо подання звітності, рівня прозорості діяльності.

Дотримання цих рекомендацій – це загальні шляхи вдосконалення ресурсного потенціалу банків. Що ж до кожної окремо взятої банківської установи, то пошук перспектив нарощування ресурсного потенціалу повинен проводитися з урахуванням результатів конкурентного стратегічного аналізу.

Висновки. Таким чином, проведене дослідження показало відсутність в економічній літературі єдиного розуміння сутності ресурсного потенціалу банку. Серед найбільш популярних серед науковців підходів до трактування даного терміну можна виділити ресурсний, результативний та змішаний підхід. Найбільш адекватним є саме змішаний підхід, що передбачає врахування як наявних фінансових ресурсів банку, так і його перспектив у найближчому та віддаленому періодах.

З урахуванням такого змішаного підходу, оцінку ресурсного потенціалу банку слід проводити не лише за допомогою розрахунку ряду аналітичних показників, зокрема й нормативів фінансової стійкості банку, але й за допомогою стратегічного аналізу, зокрема конкурентного.

Такий аналіз дасть можливість визначити ті аспекти управління ресурсним потенціалом, що створюють перспективи стратегічного розвитку комерційного банку порівняно з його найближчими конкурентами.

Перспективи подальших розвідок у даному напрямку пов’язані з апробацією запропонованої методики оцінки ресурсного потенціалу комерційного банку на прикладі результатів діяльності вітчизняних банківських установ.

Список літератури

1. Барилюк І. Стратегічний підхід до формування структури ресурсного потенціалу банку / І. Барилюк // Формування ринкової економіки в Україні. - 2012. - Вип.26.Ч.1 - С.16-24.
2. Васюренко О. Ресурсний потенціал комерційного банку / О. Васюренко, І. Федосік // Банківська справа. - 2002. - № 1. - С. 58-64.
3. Вступ до банківської справи: навч. посіб. / ред. М. І. Савлука ; Українська фінансово-банківська школа. - К. : Лібра, 1998. - 344 с.
4. Єпіфанов, А.О. Операції комерційних банків: навч. посіб. / А. О. Єпіфанов, Н. Г. Маслак, І. В. Сало. - Суми: ВТД «Університетська книга», 2007. - 523 с.
5. Коваленко В. В. Забезпечення функціональної достатності ресурсного потенціалу банку як передумова стабільного функціонування банківської системи / В. В. Коваленко, Ж. І. Торяник // Проблеми і перспективи розвитку банківської системи України: зб. наукових праць / Державний вищий навчальний заклад "Українська академія банківської справи Національного банку України". - Суми, 2009. - Вип. 25 . - С. 124-134.
6. Міхеєва Ю.В., Завадська Д.В. Ресурсний потенціал банку: сутність та шляхи вдосконалення управління в українських банках [Електронний ресурс]. - Режим доступу: http://www.msmuka.com/Ш_DN_2012/Ecoшmics/1_Ш5577.doc.htm
7. Панасенко Г.О. Синтезоване бачення поняття «ресурсний потенціал банку» в контексті розвитку економічної теорії / Г.О. Панасенко // Науковий вісник НЛТУ України. - 2013. - Вип. 23.12. - С. 291 - 297.
8. Плотніцький А.В. Оцінка ресурсного потенціалу банківських установ / А.В. Плотніцький, Д.Л. Циганюк // Молодіжний науковий вісник УАБС НБУ, Серія: Економічні науки. - 2013. - №3. - С.92-99.

УДК: 658:330

К. Горова, магістр гр. УФЕБ-18М-1,4
Центральноукраїнський національній технічний університет

АНАЛІЗ ОСОБЛИВОСТЕЙ ОРГАНІЗАЦІЇ ЕКОНОМІЧНОЇ БЕЗПЕКИ: МІЖНАРОДНИЙ ДОСВІД

У статті розглянуто та удосконалено підходи до аналізу організації економічної безпеки. Висвітлено результати порівняльного аналізу організації економічної безпеки в деяких зарубіжних країнах. Розкрита сутність поняття «економічна безпека» та види служб безпеки, які притаманні певним країнам. Сформовано загальний висновок по забезпеченню та контролю економічної безпеки на територіях.
система безпеки, економічна безпека, служба охорони, відділ безпеки

Актуальність проблеми. Зарубіжний досвід показує, що забезпечення економічної безпеки (ЕБ) у масштабах національної економіки істотно впливає на міжнародний авторитет країни. У зв'язку з цим застосування позитивного досвіду зарубіжних країн щодо забезпечення ЕБ має стати одним з найважливіших напрямків у стратегії довгострокової перспективи розвитку національної економіки країни.

Аналіз останніх досліджень і публікацій.

Вагомий внесок у вирішення теоретичних та практичних питань економічної безпеки зробили: Отенко І. П. [1] у своєму посібнику «Економічна безпека підприємства» де розкрив основні проблеми економічної безпеки в цілому, Філіпенко А. С. [1] у праці «Світова економіка», Захаров О. І. [6] «Комплексність економічної безпеки підприємства та вплив зовнішнього середовища», Михасюк І. [6] «Державне регулювання економіки», а також Козаченко Г. В., Пономарьов В. П., Ляшенко О. М. [3] «Економічна безпека підприємства: сутність та механізм забезпечення», також праці вітчизняних науковців Єдинака В. Ю., Філіпенко А. С., Живко З. Б., Керницька М. Л., Франчук В. І. та інші.

Мета статті. Дослідити міжнародний досвід організації економічної безпеки та розробити рекомендації щодо впровадження деяких його елементів в сучасних умовах української економіки.

Виклад основного матеріалу. Економічна безпека суб'єкта господарювання є комплексним поняттям та пов'язана не лише з його внутрішнім станом, але й із взаємодією суб'єктів зовнішнього середовища, з якими господарюючий суб'єкт співпрацює. Також економічну безпеку суб'єкта господарювання можна розглядати як міру гармонізації в часі та просторі економічних інтересів цього суб'єкта з інтересами пов'язаних з ним суб'єктів зовнішнього середовища, що діють поза його межами. У процесі діяльності на суб'єкт господарювання впливають різні чинники, що можуть спричинити різного роду небезпеку та загрози його діяльності.

Республіка Білорусь. Законодавчо ЕБ відображається у Концепції національної безпеки Білорусі. До пріоритетних напрямків забезпечення ЕБ відносяться: розвиток системи економічних відносин, створення механізмів розв'язання наявних у суспільстві протиріч та анулювання передумов їх виникнення; розробка стратегії забезпечення реалізації життєво важливих економічних інтересів у країні; формування довгострокової програми економічних перетворень; забезпечення сталого соціально-економічного розвитку; використання неінфляційних методів фінансування дефіциту бюджету та ефективний перерозподіл фінансових ресурсів; удосконалення зовнішньоекономічної політики; створення сприятливих умов для підприємницької діяльності [2].

У Великобританії спеціальна законодавча база щодо забезпечення ЕБ відсутня. Окремі норми, які регламентують ЕБ, містяться у нормативно-правових актах у сфері оборонної політики. Вони ґрунтуються на оцінках національних інтересів і реалізуються через їх захист. Методи щодо забезпечення ЕБ пов'язані з прогнозуванням і запобіганням найбільш небезпечних зовнішніх і внутрішніх ризиків. При виробленні та реалізації рішень, що відносяться до забезпечення ЕБ, акцент робиться на спеціалізовані організації, що представляють інтереси промисловців і підприємців.

Німеччина. Державні установи, банки, концерни, промислові асоціації й приватні компанії Німеччини, поряд із використанням власних і самостійних детективно-охоронних агентств, активно використовують національні спеціальні служби для вирішення пріоритетних економічних проблем шляхом створення сучасних контррозвідувальних структур, що виконують функції підрозділів безпеки й охорони.

Виходячи з характерних рис у Німеччині виділяються дві великі групи служб охорони, безпеки й розшуку:

- агентства, що надають фірмам і підприємствам, банкам та держустановам комплекс детективно-охоронних послуг із забезпечення безпеки бізнесу, майна й фізичного захисту співробітників;

- служби й підрозділи власного (внутрішнього) захисту, створені приватними підприємствами й фірмами [4].

Протягом останніх років у Франції спостерігається стрімке нарощування діяльності служб безпеки в промислово-торговельних фірмах і фінансових інститутах. Створення приватних служб безпеки відображає потребу національних ділових кіл у зменшенні комерційних ризиків, особливо при роботі на слабко вивчених ринках, підвищенні безпеки підприємницької діяльності, а в останні роки й особистої безпеки бізнесменів. Попит на послуги приватних детективів і охоронних структур зростає з боку приватних осіб, керівників і високопоставлених співробітників комерційних банків, страхових компаній і адвокатських контор [8]. У зв'язку зі зростаючою економічною залежністю країни й посиленням інтеграції у Європу, в другій половині 1990-х років в країні виникла необхідність розробити ряд заходів по підвищенню економічної безпеки підприємств та країни в цілому. Внаслідок цього були розроблені три напрями забезпечення економічної безпеки, зокрема: захист матеріальних та нематеріальних активів підприємств; проведення постійного моніторингу національних та іноземних конкурентів та вплив на зони, в яких підприємства поступаються конкурентам; запобігання настанню економічної кризи силами держави та спеціалістами підприємств та подолання загроз, викликаних недостатньою та несвоєчасною інформацією [3].

Фінляндія, Норвегія, Швеція й Данія. Враховуючі географічне положення, традиції і звичаї, досить близькі мовні системи і норми законодавства в країнах північної Європи, відзначається багато загальних підходів до організації діяльності охоронних служб безпеки. В цих країнах бюро розшуку й охоронні бюро відносять до категорії приватних підприємств, при цьому мається на увазі, що їх реєстрація, фінансування, оподатковування, правовий стан й діяльність регламентуються загальними нормами чинного законодавства.

В Чехії, Болгарії, Угорщині, Польщі та Словаччини спеціальна законодавча база щодо забезпечення ЕБ відсутня. Забезпечення ЕБ орієнтується на відповідні нормативно-правові акти ЄС. При виборі методів забезпечення ЕБ країни враховують геополітичну ситуацію, вектор і стратегію розвитку економіки відповідно до тенденцій регіонального та світового еволюційного процесу, напрямок економічних реформ [7].

Російська Федерація. У практиці російських підприємств та наукових дослідженнях крім терміну «служба безпеки» зустрічаються такі назви підрозділів підприємства, діяльність яких безпосередньо пов'язана із забезпеченням економічної безпеки підприємства (економічної безпеки): служба охорони, відділ безпеки, служба економічної безпеки підприємства тощо. Сьогоднішні темпи розвитку бізнесу у Росії доводять, що технологічно оснащена система економічної безпеки – це інструмент для виживання. В процес ведення господарської діяльності дуже сильно увійшли інформаційні технології. З’явилось дуже багато джерел інформації, що впливають на систему безпеки [6].

В сучасному світі у сфері безпеки великого значення набувають цифрові технології. Тому, управління фінансовою безпекою підприємства в умовах цифрової економіки має передбачати, передусім, визначення об’єктів, на які впливає той чи інший вид ризику. Важливо мати чітку інформацію про те, який об’єкт обтяжений ризиком (інформація, технологія, персонал, керівництво підприємства тощо). Слід зазначити, що власні

співробітники, особливо на підприємствах, де відсутній контроль за наданням прав доступу високого рівня, а також відсутні розмежування з прав доступу до інформаційних ресурсів, є суттєвим джерелом загроз фінансовій безпеці [9].

Висновки. Таким чином, у кожній країні сформовано власне уявлення про економічну безпеку і відповідно про методи її забезпечення, які можуть бути спрямовані на досягнення національних, суспільних інтересів або на стійкість економічного розвитку, або на незалежність національної економіки від зовнішнього ринку. На сьогоднішній день забезпечення економічної безпеки повинно стати одним з основних напрямів зовнішньої політики України. При використанні зарубіжного досвіду необхідно враховувати схожість завдань, цілей, пріоритетів національних стратегій, а також рівень економічного розвитку, рівень розвитку інститутів управління, забезпечення контролю за ЕБ.

Список літератури

1. Світова економіка: підручник / А.С. Філіпенко та ін. – К.: Либідь, 2007. – 640 с.
2. Михасюк І., Державне регулювання економіки / А. Мельник, М. Крупка, З. Залога; за ред. д-ра екон. наук, проф., акад. АН вищої школи України І. Михасюка. – ЛНУ ім. І. Франка. – К.:Атіка, Ельга-Н, 2000. – 592 с.
3. Г.В. Козаченко, В.П. Пономарьов, О.М. Ляшенко. Економічна безпека підприемства: сутність та механізм забезпечення: Монографія. – К.:Лібра, 2003. – 280 с.
4. Дерепуца, А.С. Анализ опыта стран Европейского союза в сфере обеспечения национальной экономической безопасности [Електронний ресурс] / Портал : Global international scientific analytical project. – Режим доступу \www/ URL: http://gisap.eu/ru/node/172. – Заголовок з екрану, доступ умовно-вільний.
5. Живко З.Б. Соціально-економічна безпека: практикум / З.Б. Живко, М.Л. Керницька, В.І. Франчук. – Львів: Ліга-Прес, 2009. – 136 с.
6. Захаров О.І. Комплексність економічної безпеки підприємства та впливи зовнішнього середовища / О.І. Захаров // Ефективність управління в процесі реформування: макро- та мікроекономічний аспекти: колективна монографія /за наук. ред. проф. І.Ф. Радіонової. – К.: ВНЗ «Університет економіки та права «КРОК», 2012. – 364 с.
7. Концепция национальной безопасности Республики Беларусь [Електронний ресурс] /Портал : Национальный правовой интернет-портал Республика Беларусь. – Режим доступу\www/ URL: http://www.pravo.by/main.aspx?guid=3871&p0=P31000575&p2={NRPA} – Заголовокз екрану, доступ вільний.
8. Отенко І. П. Економічна безпека підприємства: навчальний посібник / укл. І. П. Отенко, Г. А. Іващенко, Д. К. Воронков. – Х.: Вид. ХНЕУ, 2012. – 252 с.
9. Сторожук О. В. Фінансова безпека підприємства в умовах цифрової економіки / О. В. Сторожук, О.В. Заярнюк // Фінансово-кредитний механізм розвитку економіки та соціальної сфери: Матеріали ІІ Міжнародної науково-практичної інтернет конференції, 24-25 жовтня 2019 р., м. Кропивницький. – К.: «Ексклюзив-Синтез», 2019. – 216 с.

УДК 351

А. Городнянська, магістр гр. АДМ-18-МЗ
Центральноукраїнський національний технічний університет

ОСОБЛИВОСТІ СТРАТЕГІЧНОГО УПРАВЛІННЯ АГРОПРОМИСЛОВИМ РОЗВИТКОМ РЕГІОНУ

У статті досліджено сутність стратегії управління агропромисловим розвитком на регіональному рівні. Визначено характерні особливості стратегічного управління у сучасних умовах, наведено основні принципи розробки стратегії управління агропромисловим розвитком регіону. Запропоновано напрями вдосконалення стратегічного управління шляхом створення інноваційно-інтегрованих структур, які дозволять підвищити результативність та ефективність усіх учасників.
стратегія, стратегічне управління, агропромисловий розвиток, ефективність

Головними нормативними документами, що визначають цілі і завдання розвитку регіонів, їх районів, міст і галузей, є стратегії розвитку. Теорія і методологія розробки стратегій соціально-економічного-розвитку територій здійснюється за визначеними алгоритмами з використанням принципів і методів, пропонованих вченими, провідними фахівцями, експертами-аналітиками, державними діячами і активними громадянами. Постійно удосконалюється і механізм управління процесами розвитку. Сьогодні регіони, міста і господарюючі суб'єкти мають довгострокові й середньострокові стратегії розвитку на період від 3 до 5, 10 та 15 років [1].

Саме по собі стратегічне управління представляє собою інститут розвитку, визначаючий широкий спектр правил, втілення яких створює можливості та обумовлює повноваження регіонального довгострокового менеджменту, а також економічних гравців та територіального соціуму. Одночасно умовою якісного довгострокового територіального менеджменту є система інститутів, що діє в регіоні й слугує для ефективної реалізації стратегічних рішень [2].

Загальна концепція стратегічного управління охоплює такі істотні характерні особливості [3]:

– поєднує теорії менеджменту;
– враховує умови, у яких функціонує об'єкт управління;
– інтерпретує стратегічну інформацію;
– прогнозує наслідки прийнятих рішень;
– застосовує певні інструменти і методи розвитку об'єкта управління;
– створює передумови для функціонування в стратегічному режимі.

Стратегія управління агропромисловим розвитком регіону – це розроблення на основі системи наукових знань на довгостроковий період напрямів економічного розвитку агропромислового виробництва регіону (галузей, виробничо-господарських структур) з обґрунтуванням соціально-економічних і техніко-технологічних прогнозних показників отримання кількісних та якісних параметрів кінцевих результатів господарської діяльності [4].

Толстова А. В., Косенко Н. С. розглядають забезпечення ефективного функціонування підприємств АПК з точки зору комплексного розвитку економіки, формування інтеграційних взаємозв'язків між всіма елементами національної економіки [5].

Основним стратегічним напрямом розвитку регіону слід вважати максимальне забезпечення його потреб власним виробництвом у широкому асортименті високоякісних харчових продуктів з урахуванням сезонного збільшення потоків контингенту прибулих на відпочинок і лікування людей. Тому для визначення концептуальних положень стратегії розвитку сільськогосподарського виробництва необхідно обґрунтувати пріоритетність розвитку та територіального розміщення галузей аграрного сектору економіки і переробної промисловості, які мають забезпечити потребу в постачанні споживачам основних видів сільськогосподарської продукції та випуску переробною промисловістю широкого асортименту готових до споживання якісних харчових продуктів. До таких пріоритетних галузей сільськогосподарського виробництва належать ті, які мають постачати найбільший

річний обсяг продукції для споживання у свіжому та переробленому вигляді і які характеризуються нетривалим зберіганням та обмеженими якостями при їх транспортуванні [4].

До основних принципів розробки стратегії управління агропромисловим розвитком регіону належать наступні (рис. 1.5).

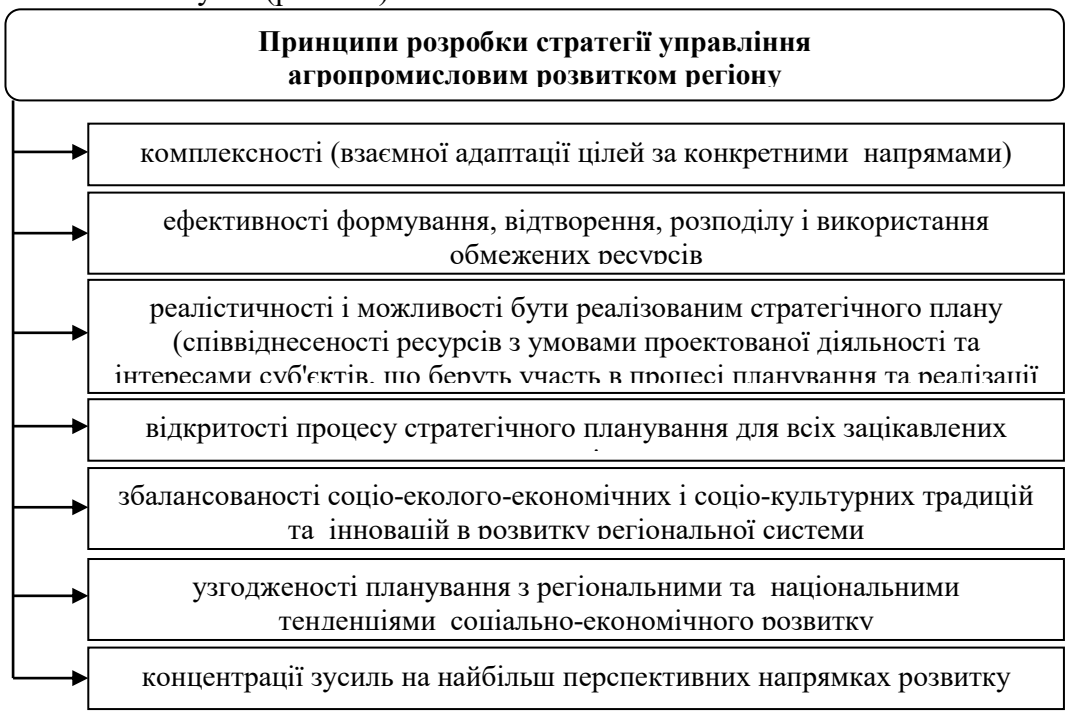


Рисунок 1 – Принципи розробки стратегії управління агропромисловим розвитком регіону

Джерело: складено на основі [6]

Стратегічне планування в органах публічного управління на місцевому рівні соціально-економічного розвитку – це, в першу чергу, документ, за допомогою якого місцеве співтовариство та місцева адміністрація діють за чітко налагодженою програмою задля вирішення існуючих проблем. Реалізація програми має складатися з експертних та планових рішень адаптування території до нових обставин, які можуть створювати переваги чи загрози послаблення конкурентних позицій. Тому стратегія розглядається як модель, яка об’єднує в єдине ціле основні цілі, політику та дії, концентруючи головні зусилля в потрібний час у потрібному місці [7].

Досліджуючи загальні підходи до стратегічного планування можна стверджувати, що воно виступає в якості процесу, за яким відбувається обґрунтування, прийняття та затвердження найважливіших завдань щодо перспективного розвитку об’єкту планування. Основою виступає стратегічна модель, сформована на сукупності принципів, визначенні ефективних механізмів використання усіх видів ресурсів, спрямованих на досягнення цілей із урахуванням зовнішніх обмежень [8].

Таким чином, особливості стратегічного управління агропромисловим розвитком регіону полягають у забезпеченні комплексного підходу до регуляторного впливу, необхідності впровадження інноваційного менеджменту на всіх рівнях, доцільності стимулювання розвитку інноваційно-інтегрованих структур різних типів, що дозволить забезпечити досягнення синергетичного ефекту в процесі функціонування підприємств аграрної сфери, виробників сільськогосподарської сировини та інших учасників об’єднань.

Список літератури

1. Морозов Р.В., Морозова О.Г. Концептуальний підхід до розроблення стратегії управління розвитком рисівництва в Україні. Бізнес-навігатор. 2019. Вип. 3-1. С. 48-52.
2. Чекан І.В. Інституційне середовище стратегічного управління регіональним розвитком як система. Науковий вісник Ужгородського університету. Серія: Економіка. 2019. Вип. 2. С. 79-84.
3. Ярута М.Ю. Удосконалення сучасного сільськогосподарського управління та методологія стратегічного управління земельними ресурсами. Вісник ХНАУ. Серія: Економічні науки. 2019. №1. С. 237-247.
4. Плеханов Д.О. Визначення стратегічних напрямів розвитку агропромислового виробництва регіону. Державне управління: удосконалення та розвиток. 2011. №2. URL: http://nbuv.gov.ua/UJRN/Duur_2011_2_11 (дата звернення: 23.09.2019).
5. Толстова А.В., Косенко Н.С. Формування інтегрованого агропромислового кластеру: стратегічний напрям розвитку підприємств сільського господарства харківського регіону. Вісник економіки транспорту і промисловості. 2014. Вип. 48. С. 158-164.
6. Богуславська С.І., Овсюк Н.В. Стратегія ресурсного забезпечення сталого розвитку регіону. Вчені записки Таврійського національного університету імені В.І. Вернадського. Серія: Економіка і управління. 2019. Т. 30(69), №5(1). С. 154-158.
7. Прилепа Н.В., Гуц В.В. Стратегічне планування в органах публічного управління на місцевому рівні. Вісник Хмельницького національного університету. Економічні науки. 2019. №5. С. 180-183.
8. Дишкантюк О.В. Методологічні підходи стратегічного планування у системі державного управління розвитком індустрії гостинності. Економічні інновації. 2016. Вип. 62. С. 398-407.

УДК 334.73

А. Гулецька, магістр гр. ОКД-18-1,4
Центральноукраїнський національний технічний університет

НАПРЯМИ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ФУНКЦІОНУВАННЯ СІЛЬСЬКОГОСПОДАРСЬКИХ ОБСЛУГОВУЮЧИХ КООПЕРАТИВІВ

У статті досліджено сутність сільськогосподарських обслуговуючих кооперативів та їх роль у забезпеченні розвитку агропромислового комплексу. Визначено, що залежно від виду діяльності сільськогосподарські обслуговуючі кооперативи поділяються на переробні, заготівельно-збутові, постачальницькі та інші. Запропоновано напрями підвищення ефективності функціонування сільськогосподарських обслуговуючих кооперативів.
кооперація, управління, ефективність, сільське господарство, оцінка

Сучасний стан аграрного сектору характеризується дисбалансом концентрації земель між агрохолдингами та іншими організаційно-правовими формами господарювання, і, як наслідок, вирощування високорентабельних олійних та зернових культур, призводить до дефіциту деяких сільськогосподарських культур, плодоовочевої та м'ясо-молочної продукції. Управління розвитком сільськогосподарських обслуговуючих кооперативів є одним із механізмів поліпшення соціально-економічного стану жителів сільської місцевості та забезпечення продовольчої безпеки України [1].

Розвиток сільськогосподарської обслуговуючої кооперації виступає одним із пріоритетів аграрної політики та інструментом досягнення економічного зростання в аграрному секторі, становлення сільського розвитку та зміцнення дрібних товаровиробників, їх конкурентоспроможності на продовольчому ринку, більш надійний захист від впливу монополізованих структур в агробізнесі [2].

Сільськогосподарський обслуговуючий кооператив – сільськогосподарський кооператив, що утворюється шляхом об'єднання фізичних та/або юридичних осіб – виробників сільськогосподарської продукції для організації обслуговування, спрямованого на зменшення витрат та/або збільшення доходів членів цього кооперативу під час

провадження ними сільськогосподарської діяльності та на захист їхніх економічних інтересів [6].

Залежно від виду діяльності сільськогосподарські обслуговуючі кооперативи поділяються на переробні, заготівельно-збутові, постачальницькі та інші (табл.1).

Об'єднуючись в обслуговуючі кооперативи, сільськогосподарські виробники отримують можливість ефективніше працювати за умови взаємної допомоги один одному. При цьому великого значення набуває державна підтримка сільськогосподарських обслуговуючих кооперативів, яка збільшує їхні фінансові можливості для діяльності. У процесі державного фінансового сприяння розвитку обслуговуючих кооперативів частково відшкодовується вартість техніки, що зумовлює зниження витрат і зростання доходів їхніх членів. Це має велике значення для розвитку учасників сільськогосподарської обслуговуючої кооперації [3].

Світовий досвід переконує, що об'єднання дрібних товаровиробників у обслуговуючі сільськогосподарські кооперативи дає можливість на рівних конкурувати з великими підприємствами. Адже це реальний шлях до піднесення добробуту кожного сільського домогосподарства, стабілізації і урізноманітнення джерел їхніх доходів, збереження наявних і створення нових робочих місць, поповнення місцевого бюджету, підтримання в належному стані сільських територій [4].

Таблиця 1 – Види сільськогосподарських обслуговуючих кооперативів

Вид	**Характеристика**
Переробні	До переробних сільськогосподарських обслуговуючих кооперативів належать кооперативи, які здійснюють переробку сільськогосподарської сировини, що виробляється членами таких кооперативів (виробництво хлібобулочних, макаронних виробів, овочевих, плодово-ягідних, м'ясних, молочних, рибних продуктів, виробів і напівфабрикатів з льону, луб'яних культур, лісо- і пиломатеріалів тощо).
Заготівельно-збутові	Заготівельно-збутові сільськогосподарські обслуговуючі кооперативи здійснюють, зокрема, заготівлю, зберігання, передпродажну обробку та продаж продукції, виробленої членами таких кооперативів, надають їм маркетингові послуги.
Постачальницькі	Постачальницькі сільськогосподарські обслуговуючі кооперативи утворюються з метою закупівлі та постачання членам таких кооперативів засобів виробництва, матеріально-технічних ресурсів, необхідних для виробництва сільськогосподарської продукції та продуктів її переробки, виготовлення сировини, матеріалів та постачання їх членам кооперативу.
Інші	У разі поєднання кількох видів діяльності утворюються багатофункціональні кооперативи.

Джерело: складено на основі [6]

За сучасних умов значні переваги мають саме багатофункціональні обслуговуючі кооперативи. Такий кооператив повинен мати декілька напрямів діяльності, кожен з яких має власні функції (рис. 1).

Рисунок 1 – Напрями діяльності багатофункціональних обслуговуючих кооперативів

Джерело: побудовано на основі [7]

У всьому світі кооперація є однією із складових частин економічної системи, де вона заповнює нішу з обслуговування різних верств населення, яким не під силу це зробити без взаємодії з іншими носіями аналогічних потреб. У нашій країні вона поступово починає набирати популярності, виступаючи об'єднуючою силою, передусім у сферах сільського господарства та соціально-економічного розвитку сільських територій. Недостатній рівень зайнятості, неналежний стан житлово-комунальної та соціально-побутової інфраструктури призводить до відтоку працездатного населення. Вирішення вказаних проблем можливе за умови співпраці органів публічної влади з громадськістю щодо розвитку обслуговуючої кооперації, діяльність якої спрямована на покращення наявної ситуації [5].

Отже, маючи значний потенціал розвитку агропромислового комплексу, Україна потребує вирішення на державному та регіональному рівні різноманітних аспектів стимулювання аграріїв до підвищення ефективності їх діяльності. Однією з актуальних форм максимізації результативності діяльності сільськогосподарських товаровиробників є їх об'єднання у рамках обслуговуючих кооперативів. Напрямами підвищення ефективності функціонування сільськогосподарських обслуговуючих кооперативів є удосконалення законодавчої бази їх діяльності, інформаційно-консультативна та організаційна підтримка, сприяння у диверсифікації джерел фінансових ресурсів та підвищення інвестиційної привабливості.

Список літератури

1. Зоргач А.М. Управління розвитком сільськогосподарських обслуговуючих кооперативів в Україні. Науковий вісник Національного університету біоресурсів і природокористування України. Серія: Економіка, аграрний менеджмент, бізнес. 2016. Вип. 249. С. 183-191.
2. Макушок О.В., Невлад В.Ф., Панкратова Л.А. Особливості бізнес-планування в діяльності сільськогосподарських обслуговуючих кооперативів: практичний аспект. Вісник ХНАУ. Серія: Економічні науки. 2018. №2. С. 249-256.
3. Галайко А.М. Фінансова підтримка розвитку сільськогосподарських обслуговуючих кооперативів. Інтелект XXI. 2018. №5. С. 28-31.
4. Демидаш Л.С. Підтримка розвитку кооперації, передбачена програмою розвитку обслуговуючих сільськогосподарських кооперативів/ Вісник Хмельницького національного університету. Економічні науки. 2015. №6. С. 193-195.

5. Приліпко С.М. Особливості діяльності сільськогосподарських обслуговуючих кооперативів у сфері житлово-комунального господарства. Ефективність державного управління. 2018. Вип. 1. С. 260-267.
6. Про сільськогосподарську кооперацію: Закон України від 17.07.1997 р. №469/97-ВР, зі змінами та доповненнями: Офіційний сайт Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/469/97-%D0%B2%D1%80 (дата звернення: 07.10.2019).
7. Коваль О.А. Багатофункціональний сільськогосподарський обслуговуючий кооператив як можливість підвищення власного фінансового забезпечення підприємства. Бізнес Інформ. 2016. №3. С. 149-154.

УДК 336.763

І. Долгіх, магістр гр.УФЕ(Б)-18М
Центральноукраїнський національний технічний університет

СУТНІСТЬ ТА ОСНОВНІ ПОЛОЖЕННЯ ФІНАНСОВО-ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

У статті розглянуто сутність фінансово-економічної безпеки з позиції економічної безпеки. Визначено механізм забезпечення економічної безпеки та розглянуто методичні положен- ня в процесі розробки комплексної системи забезпечення економічної безпеки підприємництва.

Рассмотрена сущность финансово-экономической безопасности с позиции экономической безопасности. Определен механизм обеспечения экономической безопасности и рассмотрены методические положения в процессе разработки комплексной системы обеспечения экономической безопасности предпринимательства.

фінансово-економічна безпека, комплексна система, політика, завдання та принципи формування системи економічної безпеки підприємства, концепція, методичні положення

Останні роки фінансово-економічна безпека викликає зацікавленість все більшої кількості підприємств у процесі реалізації нових підходів до управління. Під час розгляду фінансово-економічної безпеки будь-якої економічної системи будь-якого рівня необхідно виходити з її здатності протистояти небезпекам і загрозам для досягнення поставлених цілей. Взагалі – це неможливо без формування відповідної системи фінансово-економічної безпеки. Тому дана стаття розглядає дослідження сутності та складових системи фінансово-економічної безпеки підприємства.

Об'єктом дослідження є система фінансово-економічної безпеки підприємства в умовах зовнішнього середовища.

Предметом дослідження є функціональні складові фінансово-економічної безпеки підприємства.

Метою статті є дослідження функціональних складових для формування комплексної системи фінансово-економічної безпеки підприємства у сучасних умовах функціонування.

Управління підприємством в сучасних умовах, коли набирають інтенсивності рейдерські захоплення та поглинання, корпоративні конфлікти, конкурентна боротьба, фіктивне підприємництво та інші правопорушення у сфері підприємницької діяльності, вимагає формування в системі менеджменту такої складової, яка може адекватно реагувати на виклики зовнішнього середовища та протидіяти загрозам нормального функціонування підприємства. Саме така ситуація є передумовою створення системи фінансово-економічної безпеки підприємства.

Дослідження наукових результатів багатьох вчених показують, що навіть саме поняття фінансово-економічної безпеки немає однозначного тлумачення. При дослідженні сутності економічної безпеки застосовують декілька підходів та розглядають їх на різних рівнях: на національному, регіональному та галузевому рівнях, на рівні підприємств.

Перший підхід визначає економічну безпеку як складову національної безпеки; другий – як стан економіки; третій – як сполучення або сукупність умов і факторів, що забезпечують певний необхідний рівень економічного розвитку країни; четвертий – як якісний стан сукупності основних факторів суспільного виробництва в сполученні зі здатністю держави забезпечити їх ефективне захищене використання в національних інтересах і здійснювати економічну стратегію, адекватну викликам його мінливого економічного простору, з метою досягнення стабільного, стійкого розвитку та самовдосконалення всього суспільства [2]. Саме фінансово-економічна безпека на рівні підприємства і є об'єктом даного дослідження. Окрім зазначених підходів до трактування змісту поняття економічної безпеки, на думку вчених, варто застосовувати й багатокритеріальні виміри [2, 3, 8].

Огляд основних підходів до формулювання сутності фінансової безпеки (табл.) дозволив виявити певні властивості, які відповідають стану фінансової безпеки на підприємстві:

1. Здатність забезпечити фінансову рівновагу, стабільність, платоспроможність і ліквідність підприємства в довгостроковому періоді.
2. Задоволення потреб підприємства у фінансових ресурсах для стійкого розширеного відтворення підприємства.
3. Забезпечення високого рівня фінансової незалежності суб'єкта господарювання.
4. Здатність протистояти наявним і потенційним небезпекам та загрозам, що можуть завдати фінансової шкоди підприємству, або небезпечно змінити структуру капіталу, або примусово ліквідувати підприємство.
5. Забезпечення достатньої гнучкості при прийнятті фінансових рішень.
6. Забезпечення захищеності фінансових інтересів власників підприємства.

Щодо фінансової безпеки, то більшістю дослідників її сутність визначається як складова економічної безпеки на всіх рівнях, в тому числі і на рівні підприємства. Як відомо, між економічною і фінансовою діяльністю господарюючих суб'єктів, існує тісний взаємозв'язок: деякі категорії , з одного боку, є економічними за своєю суттю, а з іншого – фінансовими. Так прибуток є прямим результатом економічної діяльності підприємства, і водночас – він є фінансовим результатом, фінансовим ресурсом підприємства, який підприємство може свідомо витрачати на свій розвиток, на розвиток та мотивацію персоналу, на створення комфортних умов для праці та відпочинку, на розширення бізнесу та його диверсифікацію.

Таблиця 1.1. Поняття фінансово-економічної безпеки

№	Автор	Визначення поняття «фінансово-економічна безпека підприємства»
1	Столбов В.Ф., Шаповал Г.М.	Під фінансово-економічною безпекою підприємства слід розуміти стан захищеності його ресурсів та інтелектуального потенціалу, який характеризується високими фінансовими показниками діяльності та перспективою економічного розвитку в майбутньому [9].
2	Варналій З.С., Іващенко О.В., Четвєріков П.М.	Фінансово-економічна безпека – це результат комплексу складових, орієнтованих на усунення фінансово-економічних загроз функціонування та розвитку підприємства і забезпечення його фінансової стійкості й незалежності, високої конкурентоспроможності технологічного потенціалу, правового захисту діяльності, захисту інформаційного середовища, комерційної таємниці, безпеки персоналу, капіталу, майна та комерційних інтересів [3]
3	Єпіфанов А.О.,	Фінансово-економічна безпека це стан підприємства, що: 1)

	Пластун О.Л.	дозволяє забезпечити фінансову рівновагу, стабільність, платоспроможність і ліквідність у довгостроковому періоді; 2) забезпечує достатню фінансову незалежність; задовольняє потреби підприємства у фінансових ресурсах для стійкого розширеного відтворення; 3) здатний протистояти існуючим і виникаючим небезпекам, що прагнуть завдати фінансової шкоди підприємству або змінити всупереч бажанню структуру власного капіталу, або примусово ліквідувати підприємство. [4]
4	Кириченко О.А.	Фінансово-економічна безпека це стан найбільш ефективного використання корпоративних ресурсів підприємства, виражений у найкращих значеннях фінансових показників прибутковості і рентабельності бізнесу, якості управління, використання основних і оборотних засобів підприємства, структури його капіталу, норми дивідендних виплат по цінних паперах підприємства, а також курсової вартості його цінних паперів. [5]
5	Бондаренко О.О., Сухецький В.А.	Фінансово-економічна безпека є поняттям складним і комплексним і її визначають: сукупність робіт, які забезпечують платоспроможність підприємства та ліквідність його оборотних активів; організація контролю усіх видів діяльності підприємства з метою підвищення його ефективності; кваліфікація, компетентність та активність менеджерів; ефективність використання усіх видів ресурсів; процес попередження можливих збитків через внутрішні та зовнішні загрози тощо [1].
6	Васильців Т.Г., Волошин В.І. та ін.	Фінансово-економічна безпека це складна система, яка включає певний набір внутрішніх характеристик, спрямованих на забезпечення ефективності використання корпоративних ресурсів за кожним напрямом діяльності[2].
7	Трухан О.Л., Кокнаєва М.О.	Фінансово-економічна безпека підприємства трактується одночасно з двох позицій – статичної (як результат діяльності підприємства на певну дату) та динамічної (розвиток підприємства в умовах фінансово-економічної безпеки у короткостроковій та довгостроковій перспективі) [6, 10].
8	Мойсеєнко І.П., Марченко О.М.	Поняття фінансово-економічної безпеки підприємства визначають як такий його фінансово-економічний стан, який забезпечує захищеність його фінансово-економічних інтересів від внутрішніх і зовнішніх загроз та створює необхідні фінансово-економічні передумови для стійкого розвитку в поточному та довгостроковому періодах [7].
9	Подольчак Н.Ю., Карковська В.Я.	Захищеність потенціалу підприємства у різних сферах діяльності від негативної дії зовнішніх і внутрішніх чинників, прямих або непрямих загроз, а також здатність суб´єкта до відтворення [8]

Тому, до наукового обігу увійшло поняття фінансово-економічної безпеки підприємства, що очевидно підкреслює взаємозалежність економічної та фінансової діяльності підприємства та визначальну роль фінансів у економічній сфері будь-якого суб’єкта господарювання.

Але, як зазначають автори, поняття «фінансово-економічної безпеки» є складним і потребує комплексного, системного підходу до розуміння своєї сутності та створення системи управління фінансово-економічною безпекою підприємства [8].

Існує багато наукових поглядів на сутність поняття «фінансово-економічна безпека», але його варто досліджувати з метою формування оптимальної системи та механізму управління фінансово-економічною безпекою.

Під фінансово-економічною безпекою підприємства розуміють захищеність потенціалу підприємства у різних сферах діяльності від негативної дії зовнішніх і внутрішніх чинників, прямих або непрямих загроз, а також здатність суб'єкта до відтворення [8]. Ці ж автори пишуть, що фінансово-економічна безпека – це стан і здатність фінансово-економічної системи протистояти небезпеці руйнування її організаційної структури і статусу, а також перешкодам у досягненні цілей розвитку .

Отже, у результаті аналізу підходів до визначення дефініцій «фінансова безпека» та «фінансово-економічна безпека» виявлено, що в економічній науці існує два основних погляди на сутність цих понять:

1) фінансова безпека – самостійний об'єкт в системі управління загальною безпекою суб'єкта господарювання;

2) фінансова безпека – складова економічної безпеки.

Поєднання, частини і цілого в одному терміні може свідчити про додатковий наголос на фінансовій складовій системи економічної безпеки. Саме в цьому аспекті вживання терміну «фінансово-економічна безпека» і є, на думку О. С. Пархоменко, доречним, бо в тільки такому випадку можна уникнути плутанини, яка виникає під час частого неправомірного використання понять економічної безпеки, фінансової безпеки та фінансово-економічної безпеки як синонімів підприємства [7].

Враховуючи науковий досвід досліджень у сфері фінансово-економічної безпеки, слід зазначити, що фінансово-економічна безпека підприємства є поняттям складним і комплексним і її визначають: сукупність робіт, які забезпечують платоспроможність підприємства та ліквідність його оборотних активів; організація контролю усіх видів діяльності підприємства з метою підвищення його ефективності; кваліфікація, компетентність та активність менеджерів; ефективність використання усіх видів ресурсів; процес попередження можливих збитків через внутрішні та зовнішні загрози тощо.

Список літератури

1. Бондаренко О.О. Фінансово-економічна безпека підприємства: теоретичний та практичний аспекти [Електронний ресурс] / О.О. Бондаренко, В.А. Сухецький // Ефективна економіка. – 2014. – №10. – Режим доступу: http://www.economy.nayka.com.ua/ ?op=1&z=3580
2. Василенко А. В. Менеджмент устойчивого развития предприятий: Монография. – К.: Центр учебной литературы, 2005. – 648 с.
3. Економічна безпека: навч. посіб. / За ред. З.С. Варналія. - К.: Знання, 2009. - 647с.
4. Єпіфанов А.О. Фінансова безпека підприємств і банківських установ: моногр. / А.О. Єпіфанов, О.Л. Пластун. – Суми: ДВНЗ «УАБС НБУ». - 2009. – 295 с.
5. Кириченко О. А. Вдосконалення управління фінансовою безпекою підприємств в умовах кризи / О. А. Кириченко, І. В. Кудря // Інвестиції: практика та досвід. – 2009. – № 10. – С. 22–26.
6. Кокнаєва М.О. Концептульні основи управління фінансово-економічною безпекою підприємств торгівлі [Електронний ресурс] / М.О.Кокнаєва. - Режим доступу: www.pdaa.edu.ua/sites/default/files/ nppdaa/2011/ v2i3/319
7. Пархоменко О. С. «Фінансова безпека» та «фінансово-економічна безпека»: сутність та особливості понять [Електронний ресурс] /О.С. Пархоменко //Ефективна економіка. – 2015. – №5. – Режим доступу: http://www.economy.nayka.com.ua/ ?op=1&z=4270
8. Подольчак Н.Ю. Організація та управління системою фінансово-економічної безпеки: навч. посібник / Н.Ю.Подольчак, В.Я.Карковська .-Львів: Видавництво Львівської політехніки, 2014. - 268с.
9. Столбов В.Ф. Особливості управління системою фінансово-економічної безпеки будівельних підприємств / В.Ф.Столбов, Г.М.Шаповал // Комунальне господарство міст. Науково-технічний збірник. - 2013.- №111. - С. 103-108.

10. Трухан О.Л. Наукова інтерпретація функцій стратегічного управління підприємствами/ О.Л. Трухан // Вісник Хмельницького національного університету / Економічні науки. – 2010. – № 1. – Т. 2. – С. 29–35.

УДК 631. 37

Д. Доцяк, магістр гр. АТ-18МЗ
Центральноукраїнський національний технічний університет

ПОКРАЩЕННЯ ЕКОЛОГІЧНОСТІ АВТОМОБІЛІВ

Розглянуті основні напрями зменшення викидів шкідливих речовин ДВЗ. Найбільш ефективним в сучасних умовах є застосування альтернативних видів палива, одним із яких є біопаливо. Переведення автомобіля на біодизельне паливо допоможе знизити його експлуатаційні витрати за рахунок меншої вартості біодизеля та покращити екологічні показники
автомобіль, екологічні показники, альтернативні види палива, біопаливо

Економія паливно-енергетичних ресурсів та зниження рівня забруднення навколишнього середовища відносяться, безумовно, до актуальних досліджень, що спрямовані на покращення екологічних та економічних показників дизельних автомобілів. Відомо, що автомобіль є значним джерелом забруднення навколишнього середовища, перш за все, через викиди шкідливих речовин з відпрацьованими газами двигунів внутрішнього згоряння (ДВЗ). При спалюванні вуглеводневого палива в атмосферу викидаються продукти згоряння, які містять близько 400 хімічних речовин, у тому числі токсичних та канцерогенних. Забруднення атмосфери цими речовинами викликає екологічні проблеми [1, 2].

Основними екологічними проблемами, які пов’язані з використанням у ДВЗ нафтових палив є [3]:

- проблема потепління клімату планети внаслідок «парникового ефекту;
- теплове забруднення навколишнього середовища;
- проблема кислотних дощів, що містять сірчану та азотну кислоти;
- фотохімічний смог, пов’язаний з реакціями, що протікають під впливом ультрафіолетового випромінювання;
- забруднення морів і річок нафтою та нафтопродуктами внаслідок витоків при видобуванні та транспортуванні;
- шум, вібрація та інш.

На сьогодні існують багато шляхів покращення екологічних показників автомобілів, але більшість дослідників [4, 5 та інш.] розглядають наступні основні напрями:

- удосконалення конструкції та робочого процесу двигуна;
- очищення відпрацьованих газів у системі випуску.
- використання альтернативних палив.

Напрям покращення екологічних показників за рахунок удосконалення конструкції ДВЗ не можна застосовувати для двигунів, що знаходяться в експлуатації. Нейтралізатори відпрацьованих газів можна застосовувати для всіх типів ДВЗ, в тому числі й на автомобілях, випущених у попередні роки, двигуни яких не відповідають вимогам стандартів [5].

Одним із найбільш ефективних шляхів покращення екологічності автомобілів є застосування альтернативних видів палива. Інтерес до альтернативних джерел енергії, зокрема, до альтернативних видів палива, підвищується з кожним витком росту цін на нафту і нафтопродукти.

Альтернативні види палива можна класифікувати за наступними ознаками:

- за складом: вуглевоводнево-кислотні (спирти), ефіри, водневі палива з добавками;
- за агрегатним станом: рідкі, газоподібні, тверді;

- за об'ємом використання: цілком, як добавки;

- за джерелам сировини: з вугілля, торфу, сланців, біомаси, горючого газу, електроенергії та інш.

У роботі [6] проаналізовані недоліки та переваги кожного з видів палива (рис.1).

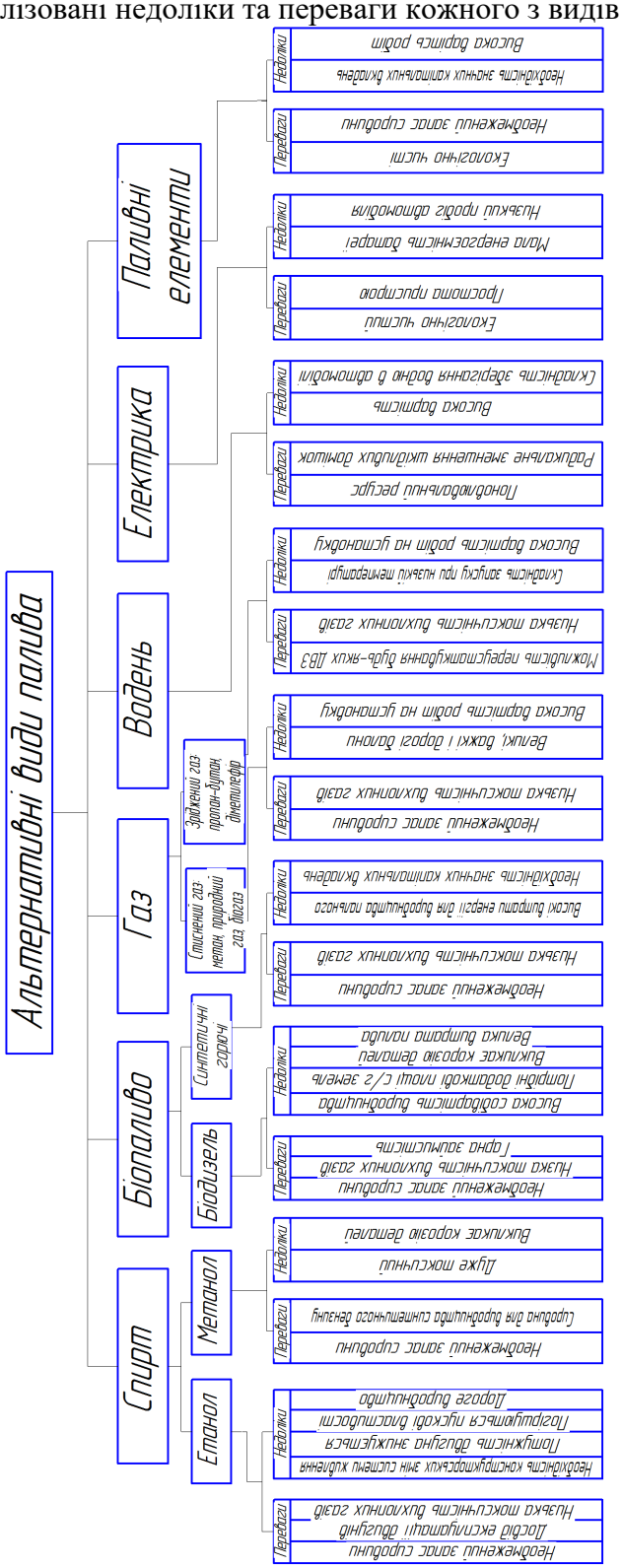


Рисунок 1 – Аналіз альтернативних видів палив [6]

На даному етапі розвитку вітчизняної альтернативної енергетики більш раціональним є використання в ДВЗ палив рослинного походження, які можна ефективно використовувати в двигунах без зміни конструкції, або незначної її модифікації [7].

Виробництво біопалива в умовах Кіровоградської області має досить серйозні перспективи [6]. Якщо випуск біодизельного палива буде відбуватися в значних обсягах,

Україна зможе значно зменшити імпорт енергоресурсів, а отже й економічну й політичну залежність від постачальників нафти. Сільськогосподарський потенціал області й наявність в нашому регіоні переробних виробництв дозволить експортувати ріпак і біодизельне паливо. Переведення автомобіля на біодизельне паливо допоможе знизити його експлуатаційні витрати за рахунок меншої вартості біодизеля та покращити екологічні показники.

Список літератури

1. Атамась А.І. Підвищення екологічних показників дизельного автомобіля під час використання біодизельного палива / А.І. Атамась, В.Ф. Шапко, С.В. Шапко // Вісник Кременчуцького національного університету імені Михайла Остроградського. – Кременчук : КрНУ ім. М. Остроградського, 2012. – Вип. 3/2012 (74). – С. 128–132.
2. Кабанов О.М. Екологія автомобільного транспорту. Конспект лекцій. – Харків: Видавництво ХНАДУ, 2011. – 142 с.
3. Звонов В.А. Образование загрязнений в процессе сгорания / В.А. Звонов. – Луганск: Издательство Восточноукраинского государственного университета, 1998. – 126 с.
4. Поляков А.П. Поліпшення економічних та екологічних показників автомобіля з дизельним двигуном, переведеним на біодизельне паливо / А.П. Поляков, Д.О. Галущак, О.В. Вдовиченко, Б.С. Маріянко // Матеріали VI міжнародної науково-практичної конференції «Сучасні технології та перспективи розвитку автомобільного транспорту»: 21-23 жовтня 2013 р. – Вінниця: ВНТУ, 2013.
5. Шапко В.Ф. Методика досліджень екологічних показників дизельних автомобілів / В.Ф. Шапко, С.В. Шапко, А.І. Атамась // «Екологічна безпека»: Науковий журнал.– Кременчук : КНУ ім. М.Остроградського, 2011– Вип.1/2011 (11) – С. 81–84.
6. Кропівний В.М. Перспективи використання альтернативних видів палива для автомобілів/ В.М. Кропівний, І.В. Шепеленко, М.В. Красота, І.Ф. Василенко// Техніка в сільськогосподарському виробництві, галузеве машинобудування, автоматизація. – Кіровоград: КНТУ, 2008. – Вип.20. – С.110-116.
7. Ковбасенко С.В. Перспективи виробництва і використання біодизельного палива в Україні / С.В. Ковбасенко, В.В. Сімоненко // Вісник національного транспортного університету: в 2-х частинах: Ч. 2. – К: НТУ, 2007. – Випуск 15. – С.28 – 31.

УДК 007.658

О. Жебко, магістр гр. ОКД -18 -МЗ (1,4)
Центральноукраїнський національний технічний університет

КОМЕРЦІЙНА ДІЯЛЬНІСТЬ ЯК ОБ'ЄКТ УПРАВЛІННЯ НА ПІДПРИЄМСТВІ

У статті визначене сучасне розуміння сутності «комерційна діяльність», як частини підприємницької діяльності, дана загальна характеристика сутності управління комерційною діяльністю. Запропонована модель управління комерційною діяльністю, яка побудована на засадах системного та функціонального підходів, сформований механізм управління комерційною діяльністю, як функціональна складова загальної системи менеджменту підприємства.
підприємство, комерційна діяльність, управління комерційною діяльністю, механізм управління комерційною діяльністю

В статье определено современное понимание сущности «коммерческая деятельность», как части предпринимательской деятельности, дана общая характеристика сущности управления коммерческой деятельностью. Предложенная модель управления коммерческой деятельностью, которая построена на основе системного и функционального подходов, сформирован механизм управления коммерческой деятельностью, как функциональная составляющая общей системы менеджмента предприятия.
предприятие, коммерческая деятельность, управление коммерческой деятельностью, механизм управления коммерческой деятельностью

Комерційна діяльність є основною для будь-якого господарюючого суб'єкта – учасника ринкових відносин. Це зумовлює необхідність управління комерційною діяльністю. Проведені дослідження свідчать про значний інтерес до управління комерційною діяльністю та значний обсяг наукових досліджень, що представлені у працях як вітчизняних, так і зарубіжних науковців зокрема з проблем управління комерційною діяльністю – М. Арістархової, В. Вовк, Ю. Дайновського, С. Ілляшенка, М. Калиниченка, Є. Крикавського, О. Ляшенка, Я. Матковської, Б. Мізюка, Ф. Панкратова, П. Перерви, В. Соловйова, С. Філиппової, М. Халікова, Н. Чухрай. Незважаючи на наявні розробки, відзначимо доцільність подальших досліджень у цьому напрямі, зокрема визначення сучасного розуміння суті комерційної діяльності, та управління нею, обґрунтування комплексної моделі управління комерційною діяльністю підприємства. Отже, тема дослідження є безумовно актуальною і своєчасною.

Метою дослідження є розроблення теоретичних засад і практичних рекомендацій щодо побудови моделі управління комерційною діяльністю та механізму управління комерційною діяльністю, як функціональної складової загальної системи менеджменту підприємства.

Для досягнення поставленої мети у дослідженні вирішено такі завдання: - досліджено сутність і теоретичні засади комерційної діяльності та управління комерційною діяльністю; - розробити модель управління комерційною діяльністю, яка побудована на засадах системного та функціонального підходів; - запропонувати механізм управління комерційною діяльністю, який формується як функціональна складова загальної системи менеджменту суб'єкта господарювання і включає цілі, об'єкти, суб'єкти, методи та засоби управління.

Об'єктом дослідження є процес управління комерційною діяльністю підприємства, як функціональної складової загальної системи менеджменту підприємства.

Щодо сутності комерційної діяльності слід відзначити, що сам термін «комерція» походить від латинського «comercium», що в перекладі означає «торгівля». З огляду на це логічними виглядають твердження, подані в працях [1; 12; 4], згідно з якими комерційна діяльність є ознакою діяльності суб'єктів торговельної галузі.

Зокрема З. С. Варналій розглядає комерційну діяльність як один із видів підприємницької діяльності, ототожнюючи комерційну діяльність із діяльністю у сфері обігу [1, с. 4]. Так Ф. П. Половцева, даючи визначення терміна «комерційна діяльність» говорить, що це є комплексом операцій, що є торгівлею в широкому значенні слова [11, с. 39], а Ф. Г. Панкратов та Т. К. Серьогіна пов'язують комерцію з реалізацією товарів та відзначають, що це особливий вид діяльності, від якої безпосередньо залежать кінцеві результати торгового підприємства [9, с. 39]. Згідно з іншим підходом комерційною вважається будь-яка діяльність, метою якої є отримання прибутку. Так, за Господарського кодексу України господарська діяльність представлена двома видами – комерційною та некомерційною діяльностями [3]. За визначеннями, наданими у статтях 42 та 52 Господарського кодексу України, метою комерційної діяльності є досягнення економічних і соціальних результатів та одержання прибутку, некомерційної – досягнення економічних, соціальних та інших результатів без мети одержання прибутку. Як бачимо в цьому випадку комерційна діяльність ототожнюється з підприємництвом загалом.

За результатами порівняльного аналізу та критичної оцінки визначень комерційної діяльності, наведених у науковій літературі, виділено три напрями трактування цього поняття.

Представники першого напряму ототожнюють комерційну діяльність із підприємництвом загалом, другого – виключно з торговельним підприємництвом, третього – сприймають як частину підприємницької діяльності суб'єктів господарювання будь-якого виду економічної діяльності

Ми поділяємо позиції представників останнього напряму та вважаємо, що комерційна діяльність є складовою підприємницької діяльності та провідною в забезпеченні функціонування та розвитку господарюючого суб'єкта будь-якого виду економічної

діяльності. Загалом, узагальнюючи погляди вчених різних шкіл і формацій на сутність комерційної діяльності і її роль в у сучасних умовах, ми пропонуємо таке більш повне визначення сутності КД: сукупність взаємопов'язаних процесів (управлінських, основних, допоміжних і обслуговуючих), які суб'єкт господарювання здійснює в сферах обміну, виробництва, розподілу та обігу, що базуються на урахуванні всіх факторів і виконанні всіх функцій, належному задоволенні споживачів та отриманні прибутку.

Для визначення сутнісних характеристик управління комерційною діяльністю ми виходили зі загальних підходів до управління підприємством, а також існуючих розробок щодо формування моделі управління комерційною діяльністю, поданих у літературі. Погоджуючись з доцільністю дотримання стратегічного підходу в управлінні комерційною діяльністю відзначимо, що стратегічні рішення – це лише один з рівнів управління. Для нормального функціонування підприємства та реалізації комерційних цілей його розвитку необхідне поєднання та узгодження підсистем стратегічного та оперативного управління. За результатами теоретичного узагальнення та аналізу літературних джерел ми пропонуємо розроблену модель управління комерційною діяльністю, яка побудована на засадах системного та функціонального підходів (рис. 1).

Згідно з системним підходом комерційна діяльність подана як сукупність відповідних елементів, згідно з процесним – як циклічний процес реалізації загальних управлінських функцій (планування, організація реалізації, контроль) [5]. Як основні елементи системи управління комерційною діяльністю на підприємстві виділено такі: суб'єкт, об'єкт, критерії та методи управління. З позиції функціонального підходу управління комерційною діяльністю представлено загальними функціями, що об'єднані у такі блоки як планування, організація реалізації та контроль за здійсненням комерційних процесів та операцій на підприємстві.

Під час формування моделі управління комерційною діяльністю підприємства ураховано обидва компоненти – суб'єкт та об'єкт. Щодо суб'єктного складу, то в ефективній комерційній діяльності підприємства зацікавлені всі основні учасники економічних відносин, а саме власники і працівники підприємства, контрагенти, фінансові установи, представники місцевих органів державного управління та ін.

Відзначимо, що, з огляду на сутність комерційної діяльності, під час її формування об'єктивним є дослідження ринків покупців та постачальників, а також моніторинг конкурентного середовища. Водночас, попри вплив усіх названих учасників на діяльність торговельного підприємства, вважаємо за доцільне під час формування комплексної моделі управління комерційними операціями як основні відзначити внутрішніх суб'єктів такого впливу, а саме осіб, які безпосередньо приймають рішення комерційного характеру, − менеджерів різних ланок, як на рівні функціональних та територіальних підрозділів, так і торговельного підприємства загалом. За результатами дослідження зроблено висновок, що під час подання моделей управління комерційною діяльністю науковці здебільшого акцентують увагу на суб'єктах управління та питаннях інформаційно-методичного забезпечення реалізації цього процесу. Водночас такий чинник управління як характер управлінського рішення залишається поза уваги дослідників. Вважаємо це невірним і пропонуємо урахувати сучасні тенденції в управлінні підприємством та розглядати комерційну діяльність підприємства як комплекс взаємопов'язаних процесів стратегічного та оперативного управління. З точки зору стратегічного управління рішення у сфері комерційної діяльності стосуються розвитку підприємства у довгостроковій перспективі, посилення його конкурентоспроможності, здатності своєчасно реагувати на запити ринку та зміни у зовнішньому середовищі. Оперативне управління комерційною діяльністю підприємства пов'язане з ресурсним забезпеченням і прибутковістю комерційних операцій у просторі та часі.

Рисунок 1 - Структурна модель системи управління комерційною діяльністю підприємства

Джерело: розроблено автором

Для управління комерційною діяльністю використовують відповідні економічні, адміністративні та соціально-психологічні методи. Управління комерційною діяльністю реалізується за умови використання відповідних засобів, які в загальному вигляді подані сукупністю методів планування та прогнозування комерційної діяльності (експертних оцінок, нечітких множин), мотивації діяльності, аналізу (факторного, кореляційного, функціонально-вартісного) та оцінки (експрес- та поглибленої) результатів комерційної діяльності. Застосування відповідних засобів та інструментів управління залежить від характеру управлінських рішень, функції, об'єкта (ресурси, результати, ефективність діяльності, ціннісні характеристики підприємства) та інформаційного забезпечення процесу управління.

Проведений аналіз та узагальнення наукових підходів до управління комерційною діяльністю дали змогу визначити та обґрунтувати доцільність дотримання в управлінні комерційною діяльністю підприємства системно-функціонального підходу. Дотримання цього підходу а також урахування ключових характеристик комерційної діяльності підприємства дозволили визначити суть управління комерційною діяльністю підприємства, яке трактується наступним чином. Управління комерційною діяльністю на підприємстві – це цілеспрямована діяльність, яка ґрунтується на засадах стратегічного та оперативного управління, здійснюється з використанням відповідних методів та способів планування, організації й контролю комерційних процесів та операцій із закупівлі та реалізації партій товарів, з дотриманням ціннісних орієнтирів та забезпечення прибутку як у поточному періоді так і довгостроковій перспективі.

В свою чергу, механізм управління комерційною діяльністю формується як функціональна складова загальної системи менеджменту суб'єкта господарювання. Цей механізм включає цілі, об'єкти, суб'єкти, методи та засоби управління (табл. 1).

Таблиця 1 – Механізм управління комерційною діяльністю

Складові механізму	Характеристика

Цілі управління	- за значимістю; - за рівнем формування; - за часом дії; - за системою оцінки; - за сферою застосування
Об'єкти управління	- структурні підрозділи підприємства; - основні управлінські процеси комерційної діяльності; - міжособистісні відносини, які виникають при виконанні комерційних процесів
Суб'єкти управління	- керівник підприємства, керівник комерційної служби, керівники структурних ланок
Методи управління	- стратегічне планування та прогнозування; - комерційний розрахунок; - система заохочень з боку держави; - економічна та соціальна мотивація комерційних працівників
Засоби управління	- системний аналіз, інформаційне забезпечення, адміністративно-правове управління; - імітаційне моделювання

Джерело: розроблено автором

В якості найважливіших засад управління комерційною діяльністю підприємства дослідниками виділяються: - системний розгляд комерційної діяльності як сукупності взаємопов'язаних операцій; - управління комерційними операціями на основі логістичного та маркетингового підходів; - створення технології реалізації окремих комерційних операцій в залежності від зовнішніх та внутрішніх факторів; - розробка моделі управління комерційною діяльністю.

За результатами проведених досліджень уточнено термінологічний апарат предметної галузі, зокрема уточнено поняття «комерційна діяльність», яка визначена частиною підприємницької діяльності, що включає в себе операції підприємства по здійсненню торговельних угод з метою отримання доходу; сукупність взаємопов'язаних процесів (управлінських, основних, допоміжних і обслуговуючих), які суб'єкт господарювання здійснює в сферах обміну, виробництва, розподілу та обігу, що базуються на урахуванні всіх факторів і виконанні всіх функцій, належному задоволенні споживачів та отриманні прибутку. Досліджено сутність поняття «управління комерційною діяльністю», яка визначена як цілеспрямована діяльність, яка ґрунтується на засадах стратегічного та оперативного управління, здійснюється з використанням відповідних методів та способів планування, організації й контролю комерційних процесів та операцій із закупівлі та реалізації партій товарів, з дотриманням ціннісних орієнтирів та забезпечення прибутку як у поточному періоді так і довгостроковій перспективі. У зв'язку з сучасними умовами господарювання і трансформації як самих ринкових відносин, так і підходів до комерційної діяльності, відбувається ускладнення управління нею та її основними процесами, тому нами було поглиблено підходи до управління комерційною діяльністю на підприємствах, що включає модель управління комерційною діяльністю, яка побудована на засадах системного та функціонального підходів та сформований механізм управління комерційною діяльністю, як функціональна складова загальної системи менеджменту підприємства. Це забезпечить підвищення ефективності управління комерційною діяльністю підприємства в конкурентній сфері.

Список літератури

1. Варналій З.С. Основи підприємництва : навч. посібник / З.С. Варналій. – К. : Знання-Прес, 2002. – 239 с.

2. Германчук А.М. Управління комерційною діяльністю підприємств на основі маркетингу : автореф. дис. канд. екон. наук : 08.06.02 / А.М. Германчук. – Донецьк., 2000. – 21с.
3. Господарський кодекс України // Відомості Верховної Ради України.—2003.—№ 18, № 19–20, № 21–22.—Ст. 144
4. Кисельов А.П. Основи бізнесу : підручник / П.П. Кисельов. – К. : Вища школа, 1997. – 191 с
5. Лисак Г.Г. Системно-функціональний підхід до управління комерційною діяльністю на підприємстві оптової торгівлі / Г.Г. Лисак : матеріали міжнар. наук.-практ. конф. [«Інноваційні підходи і 157 сучасна наука»], (Київ, 30 квіт. 2015 р.). – К. : Центр наукових публікацій, 2015. − С. 89−91.
6. Марченко И.С. Системный подход к управлению коммерческой деятельностью организации / И.С. Марченко // Вестник МГТУ. – 2010. – Т. 1. – С. 27-30.
7. Меженська В.В. Механізм управління комерційною діяльністю торговельного підприємства / В.В. Меженська // БізнесІнформ. – 2012. – № 4. – С. 144-146.
8. Мізюк Б.М. Сучасні концепції управління комерційною функцією в роздрібних торговельних мережах / Б.М. Мізюк, М. Д. Гонський // Вісник Львівської комерційної академії. Серія економічна. – Львів : ЛКА, 2014. – Вип. 45. – С. 91-95.
9. Панкратов Ф.Г. Коммерческая деятельность. / Ф.Г. Панкратов, Т.К. Серёгина. – М. : ИВЦ Маркетинг, 2000. – 340 с.
10. Панчук А.С. Концептуальна модель стратегічного маркетингового управління комерційною діяльністю підприємств [Електронний ресурс] / А.С. Панчук.
11. Половцева Ф.П. Коммерческая деятельность / Ф.В. Половцева. – М. : ИНФРА-М, 2009. – 248 с.
12. Сидоров В.П. Коммерческая деятельность : уч. пособие / В.П. Сидоров. – Владивосток : Изд-во ВГУЭС, 2014. – 248 с.

УДК 332.334

С. Жук, магістр гр. АДМ-18М-1,4
Ю. Малаховський, канд. екон. наук, доц.
Центральноукраїнський національний технічний університет

ОСОБЛИВОСТІ УПРАВЛІННЯ МУНІЦИПАЛЬНИМИ ЗЕМЕЛЬНИМИ РЕСУРСАМИ

До основних організаційних дій з управління земельними ресурсами належать:

1) планування, тобто визначення і постановка цілей, завдань і методів ухвалення рішення для досягнення найбільш ефективного і раціонального землекористування;

2) організація управлінської структури з визначенням ролі і завдань кожного підрозділу;

3) мотивація, тобто створення внутрішнього спонукання управлінських структур до необхідних дій;

4) контроль, тобто процес забезпечення досягнення цілей управління [1; 3; 4].

Ухвалення рішення пов’язане з великим числом можливих комбінацій потенційних управлінських дій. Основними етапами ухвалення рішення з управління земельними ресурсами є такі: постановка завдання; пошук інформації; визначення умов існування об’єкта управління і пов’язаних з ним структур; визначення кола користувачів; визначення запитів землекористувачів; дослідження поводження споживачів передбачуваного управлінського рішення і дії; нагромадження, систематизація й аналіз даних про об’єкт керування; розрахунок можливої ефективності; здійснення пілот-проекту; розрахунок фактичної ефективності або її моделювання; вибір варіанта й ухвалення управлінського рішення [2; 6].

Визначальним етапом є постановка завдання й ухвалення управлінського рішення. Прийняття управлінських рішень допускає визначення критерію і виявлення умов об’єкта управління.

При постановці завдання управління велике значення мають: аналіз і врахування умов управління; визначення критерію ухвалення рішення; вибір методів аналізу умов існування об'єктів управління і моделювання процесів управління.

Разом з тим, на умови управління земельними ресурсами мають вплив такі фактори: економічна стабільність у суспільстві й регіоні; загальний стан законодавчої бази; інформаційне забезпечення; період часу ухвалення рішення; мажорні/форс-мажорні обставини і т. д. [7; 8; 10].

Суто до управлінських умов слід віднести: відповідність завдань управління законодавству; формування системи взаємодії виконавчих і законодавчих органів влади; забезпечення укомплектованості кадрами; підвищення ступеня навчання фахівців (керівників і виконавців); забезпечення картографічними матеріалами необхідного масштабу; проведення повсюдної інвентаризації земель, землеустрою, земельного кадастру, моніторингу земель, їхньої охорони; автоматизація процесу управління і ведення державного земельного кадастру; можливість адаптації вхідних геоінформаційних систем (ГІС) до умов об'єкта управління; інші умови [14; 16; 17].

Разом з тим, реалізація законів і принципів управління може здійснюватися тільки із застосуванням відповідних методів управління.

Метод управління – це сукупність прийомів і способів впливу на керований об'єкт для досягнення поставлених цілей.

Слово "метод" (від грец. *methodos*) у перекладі означає спосіб досягнення будь-якої мети. Через методи управління реалізується основний зміст управлінської діяльності.

Характеризуючи методи управління, необхідно розкрити їхню спрямованість, зміст і організаційну форму.

Спрямованість методів управління виражає їх орієнтованість на конкретну систему (об'єкт) керування.

Зміст – специфіка прийомів і способів впливу.

Організаційна форма – специфічний вплив на реально сформовану ситуацію. Це може бути прямий (безпосереднє) або непрямий (постановка завдання і створення стимулюючих умов) вплив.

У практиці управління, як правило, одночасно застосовують різні методи та їхнє поєднання (комбінації), що органічно доповнюють один одного, знаходяться в стані динамічної рівноваги.

Можна виділити такі методи управління: соціальні і соціально-психологічні, які застосовуються з метою підвищення соціальної активності людей; економічні, зумовлені економічними стимулами; правові, які включають норми і правила, що визначаються, у першу чергу, земельним законодавством і обов'язкові для виконання; землевпорядні як комбінація правових, соціальних, економічних та інших методів, шляхом яких встановлюються обмеження у використанні земель, землеохоронні регламенти; організаційно-адміністративні, засновані на прямих директивних вказівках [6; 9].

У більш загальному вигляді всі методи управління можна розділити на дві групи: основні і комплексні.

До основних належать такі, у яких чітко виділяється змістовний аспект за ознакою відповідності методів управління вимогам тих чи інших об'єктивних законів (наприклад, соціальних, економічних, організаційно-технічних та ін.).

Складними, або комплексними, методами управління є комбінації основних методів.

За змістом методи управління відображають вимоги різних об'єктивних законів соціально-економічного розвитку: економічних, організаційно-технічних, соціологічних і т. д [5; 9; 11-13; 15].

Соціальні методи управління пов'язані зі способами досягнення соціальних цілей суспільства не тільки економічними, організаційно-адміністративними способами мотивації людської поведінки, а й безпосередньо: через визначення соціальних цілей, підвищення якості життя. Будучи основними, соціальні методи виступають і як комплексні, але в цьому

комплексі відповідно до вимог об'єктивних закономірностей (зростання ролі соціального фактора) вони багато в чому визначають змістовний аспект управління і задають вектор розвитку всім іншим методам впливу. Наприклад, поряд з економічним стимулюванням сьогодні широко використовується стимулювання якістю соціального впливу, почуттям соціальної причетності до справ тощо.

Соціальні методи включають широкий спектр методів соціального формування, соціального регулювання, морального стимулювання та ін. Методи соціального нормування дають змогу упорядкувати соціальні відносини між соціальними групами, колективами й окремими працівниками шляхом уведення різних соціальних норм у соціальному управлінні, конкретним методом соціального нормування є регламентування розмірів приватної власності на землю. Методи соціального регулювання використовуються для упорядкування соціальних відносин шляхом виявлення і регулювання інтересів і цілей різних колективів, груп та індивідуумів.

Економічні методи управління являють собою способи досягнення економічних цілей управління (засобу) на основі реалізації вимог економічних законів. Іншими словами, під економічними методами в сучасному значенні розуміється економічний розрахунок, заснований на свідомому використанні всієї системи економічних законів і категорій ринкової економіки.

Серед різноманіття економічних методів управління можна виділити, наприклад, методи економічного стимулювання. Економічне стимулювання – метод управління, що спирається на економічні інтереси землекористувачів, і становить основу формування ефектів від раціоналізації землекористування. Система економічного стимулювання є сукупністю розроблювальних і здійснюваних заходів, спрямованих на посилення зацікавленості землекористувачів в одержанні можливо високого прибутку. Економічне стимулювання базується на таких основних принципах: взаємозв'язок і погодженість цілей економічного стимулювання з цілями розвитку вигод і раціоналізації землекористування; диференціація економічного стимулювання спрямована на реалізацію необхідних змін у структурі землекористування; поєднання економічного стимулювання з іншими методами мотивації; поєднання економічного стимулювання з економічними санкціями, які передбачають матеріальну відповідальність землекористувачів.

Організаційно-адміністративні методи базуються на владі, дисципліні і відповідальності. Організаційно-адміністративний вплив здійснюється в таких основних видах: пряма адміністративна вказівка, що має обов'язковий характер, адресується конкретним керованим об'єктам або особам і впливає на конкретно сформовану ситуацію; встановлення правил, що регулюють землекористування (нормативне регулювання), вироблення стандартних процедур адміністративного впливу; розробка і впровадження рекомендацій з організації й удосконалювання тих або інших процесів, що піддаються організаційно-адміністративному впливові; контроль за використанням і охороною земель.

Основною формою реалізації і застосування організаційно-адміністративних методів управління є розпорядження й оперативне втручання у процес управління з метою координації зусиль його учасників для виконання поставлених перед ними завдань.

У цілому об'єктивною основою використання організаційно-адміністративних методів управління виступають організаційні відносини, що складають частину механізму управління. Оскільки через їхнє посередництво реалізується одна з найважливіших функцій управління – функція організації, завдання організаційно-адміністративної діяльності полягає в координації дій підлеглих. Нерідко, і справедливо, критикують спроби абсолютизації адміністративного управління, однак варто мати на увазі, що ніякі економічні методи не зможуть існувати без організаційно-адміністративного впливу, що забезпечує чіткість, дисциплінованість і порядок роботи. Важливо визначити оптимальне поєднання, раціональне співвідношення організаційно-адміністративних, економічних, соціальних і землевпорядних методів.

Підхід, відповідно до якого сфера впливу економічних методів розширюється тільки за рахунок витиснення організаційно-адміністративних методів управління, не можна визнати правомірним ні з наукової, ні з практичної точок зору. Організаційно-адміністративні методи в основному спираються на владу керівника, його права, властиву організації (установі, підприємству) дисципліну і відповідальність. Однак адміністративні методи не слід ототожнювати з вольовими і суб'єктивними методами керівництва, тобто адмініструванням.

Організаційно-адміністративні методи впливають на керований об'єкт через стандарти, норми, оперативні вказівки, що віддаються письмово або через рішення, проекти та програми землеустрою, контроль за їх виконанням, систему адміністративних засобів підтримки технологічної дисципліни і т. д.

Вони покликані забезпечити організаційну чіткість і дисципліну технології виробництва. Ці методи регламентуються правовими актами земельного, природоохоронного і господарського законодавства, соціального регулювання.

У рамках організаційної системи управління можливі такі форми прояву організаційно-адміністративних методів: обов'язкове розпорядження (наказ, заборона і т. п.); єднальні заходи (консультації, компроміси); рекомендації, побажання (порада, роз'яснення, пропозиція, спілкування і т. п.).

Організаційно-адміністративні методи відрізняє від інших чітка адресність директив, обов'язковість виконання розпоряджень і вказівок: їх невиконання розглядається як пряме порушення виконавської дисципліни і спричиняє визначені стягнення. Це переважно примусові методи, що зберігають свою силу доти, поки праця не перетворюється на першу життєву необхідність.

Методи управління земельними ресурсами можна поділити на: методи вивчення об'єктів управління, методи розробки управлінських рішень та методи реалізації управлінських рішень.

Реалізація управлінських рішень, особливо при безпосередньому управлінні здійснюється за допомогою організаційно-адміністративного чи економічного методу.

Організаційно-адміністративний метод пов'язаний з прийняттям і реалізацією безпосередніх управлінських рішень-директив. Цей метод заснований на реалізації державою своїх функцій з управління, відображених у законодавстві. Це акти прямої дії: вилучення чи надання земель, зонування земель, заходи щодо вивчення земель і їх реалізація. Правовий метод виявляється при опосередкованому управлінні, коли створюване законодавство і нормативи використання земель змушують суб'єктів земельних відносин приймати потрібні державні рішення. Економічний метод допускає створення економічних стимулів і показників, що забезпечують реалізацію державної політики в галузі землекористування.

Усі методи повинні застосовуватися при здійсненні системи управління земельними ресурсами. При виробленні цілей і критеріїв оцінки ефективності управління необхідно з достатньою точністю визначити методи реалізації кожної функції для формування економічно ефективної системи управління земельними ресурсами.

Список літератури

1. Акімова Т. А. Теорія організації: навчальний посібник для вузів / Т. Акімова. – М.: ЮНИТИ-ДАНА, 2003. – 367 с.
2. Методи і моделі інформаційного менеджменту: Навчальний посібник / Д.В. Александров, А.В. Костров, Р.І. Макаров, Є.Р. Хорошева – К.: Всеувито 2007. – 336 с.
3. Андреєва В.М. Маркетинг і поведінка споживача на ринку комунальних послуг: Навчальний посібник для студентів спеціальності "Менеджмент організацій" / В.М. Андреєва, Є.М. Кайлюк, Д.О. Шаповаленко. – Харків: ХНАМГ, 2007. – 150 с.
4. Васильев А.А. Муниципальное управление [Электронный ресурс] / А. Васильев. – Режим доступа: http://vasilievaa.narod.ru/mu/stat_rab/books/ MU_konsp_lekts_Vasiliev/L5.Osn_napr_mun_pol.htm.
5. Воронкова В.Г. Муніципальний менеджмент: Навчальний посібник / В. Воронкова. – К. : Професіонал, 2004. – 256 с.

6. Гурне Б. Державне управління / Б. Гурне. – К.: Основи, 1994. – 165 с.
7. Гуськова І. Особливості управління комунальною власністю як специфічною формою групової власності [Електронний ресурс] / І. Гуськова // Публічне управління : теорія та практика. – № 4(12). – 2012. – Режим доступу : http://www.kbuapa.kharkov.ua/e-book/putp/2012-4/doc/3/08.pdf.
8. Державне управління регіональним розвитком України: Монографія / за заг. ред. В.Є. Воротіна, Я.А. Жаліла. – К.: НІСД, 2010. – 288 с.
9. Круш П.В. Національна економіка: регіональний та муніципальний рівень: Підручник] / П.В. Круш, О.О. Кожемяченко. – К.: Центр учбової літератури, 2011. – 320 с.
10. Макаренко М. В. Система цілей та завдань управління регіональним розвитком [Електронний ресурс] / М.В. Макаренко // Теоретичні і практичні аспекти економіки та інтелектуальної власності = Theoretical and Practical Aspects of Economics and Intellectual Property : збірник наукових праць: у 3-х т. / ПДТУ. – Маріуполь, 2011. – Т.1. – Режим доступу: http://eir.pstu.edu/bitstream/handle/123456789/442/54.1.pdf?sequence=1.
11. Мельник А.Ф. Муніципальний менеджмент: Навчальний посібник / А.Ф. Мельник, Г.Л. Монастирський, О.П. Дудкіна; За ред. А. Ф. Мельник. – К.: Знання, 2006. – 420 с.
12. Мельник А.Ф. Державне управління: Підручник / А.Ф. Мельник – К.: Знання, 2009. – 582 с.
13. Мельник А.Ф. Управління розвитком муніципальних утворень: теорія, методологія, практика: Монографія / А.Ф. Мельник, Г.Л. Монастирський. – Т.: Екон. думка, 2007. – 476 с.
14. Монастирський Г. Становлення та розвиток територіальних спільнот низового рівня в Україні, Польщі та Швеції: уроки для України / Г. Монастирський // Рада. – 2002. – № 2. – С. 78–83.
15. Пашкевич М.С. Наукові засади регулювання регіональної економіки: Монографія / М.С. Пашкевич. – Д. : Національний гірничий університет, 2012. – 790 с.
16. Посібник з моніторингу та оцінювання програм регіонального розвитку / Б. Винницький, М. Лендьел, Ю. Ратейчак, І. Санжаровський; За ред. І. Санжаровського, Ю. Полянського. – К.: К.І.С., 2007. – 80 с.
17. Системи управління якістю при наданні муніципальних послуг у відповідності до вимог ISO 9001:2008: існуючі практики та напрями удосконалення. Аналітичне дослідження, виконане в рамках Проекту ПРООН “Муніципальна програма врядування та сталого розвитку” [Електронний ресурс]. – Режим доступу: http://www.minregion.gov.ua/attachments/content- attachments/1395/System_quality_PROON2012.pdf.

УДК 005.934:330.1

В. Затока, магістр гр. УФЕБ-18М
Центральноукраїнський національний технічний університет

ОСОБЛИВОСТІ УПРАВЛІННЯ ФІНАНСОВО-ЕКОНОМІЧНОЮ БЕЗПЕКОЮ ДЕРЖАВНИХ ПІДПРИЄМСТВ

Стаття присвячена питанням управління державними підприємствами. Визначено роль та необхідність стабільного розвитку державних підприємств. Розглянуто зарубіжний досвід управління вказаними підприємствами, а також визначено вітчизняні недоліки державного управління. Обґрунтовано доцільність та необхідність забезпечення фінансово-економічної безпеки державних підприємств.

державне підприємство, держава, фінансово-економічна безпека, державна влада, зарубіжний досвід, управління державним підприємством

Постановка проблеми. Українська економіка зіткнулась із рядом загроз. Серед внутрішніх загроз корупційні схеми в бізнесі, відкати; боротьба олігархічних кланів за сфери впливу; фінансова нестабільність; відтік робочої сили; втрата вітчизняними виробниками ринків збуту тощо. Зовнішні загрози представляють собою глобальну експансію транснаціонального капіталу; велику боргову залежність держави перед МВФ; корупцію вітчизняних чиновників, які співпрацюють з міжнародними і транснаціональними корпораціями; критична залежність України від імпорту; слабкий валютний та зовнішньоторговельний контроль тощо. Всі ці загрози створюють фінансово-економічну нестабільність економіки держави.

Власний досвід та досвід розвинених зарубіжних країн доводить необхідність державного втручання в економіку. Посилення ролі держави в регулюванні економіки вимагає створення гнучкої і економічно обґрунтованої системи державного підприємництва, яка б повною мірою відповідала світовому досвіду побудови ефективних ринкових відносин [1].

У зв'язку зі складною соціально-економічною ситуацією в країні та врахуванням перелічених вище загроз функціонування економіки, державним підприємствам та критично не вистачає фінансових ресурсів, які б дали змогу своєчасно оновлювати виробничий капітал, поступово його розширювати та створювати нові потужності тощо. Також проблемою можна вважати відсутність автономії у вирішення господарських питань. Це спонукає державні підприємства звертатися за кредитуванням до іноземного капіталу. Адже з боку держави відсутній ефективний фінансовий механізм, надання вітчизняним підприємствам фінансових ресурсів з нульовою ставкою за кредитом або хоча б зі ставкою, порівнянною з пропозиціями іноземних контрагентів [2, с. 27]. Така ситуація є неприпустимою, адже в подальшому може загрожувати національним інтересам України, зокрема її фінансово-економічній безпеці та незалежності. В цьому ключі актуальності набуває питання щодо розроблення механізмів достатнього забезпечення та управління фінансовими ресурсами державних підприємств.

Аналіз останніх досліджень і публікацій. Теоретичні основи розробки механізмів управління економічною безпекою підприємства відображені в роботах вітчизняних та зарубіжних авторів, таких як: Т. Васильців, О. Барановський, І. Бланк, К. Горячева, Т. Гладченко, О. Грунін, М. Єрмошенко, Р. Кириченко, Т. Клебанова, Г. Клейнер, Г. Козаченко, А. Ляшенко, А. Могильний, Є. Олейников, В. Ортинський, Р. Руденський, В. Тамбовцев, А. Шеремет, В. Шлемко, В. Шликов та ін. Однак, залишаються дискусійними питання вибору методів управління цим економічним явищем та розроблення загального механізму управління.

Питаннями, що стосуються вдосконалення механізмів насичення фінансовими ресурсами економіки країни та управління фінансами в державних підприємствах, приділено достатньо уваги в науковій літературі. Зокрема в працях О. Власюка, Л. Губська, Т. Дідух, А. Іменинник, М. Коваленко, Н. Коваль, Л. Лондар, В. Міщенко, Л. Шемаєва, М. Шестак тощо.

Проте, незважаючи на досить вагомі напрацювання науковців за вказаним напрямками, залишається відкритим і потребує подальшого дослідження питання щодо фінансово-економічної безпеки та стабільності самого державного підприємства, яке розглядалося б не як посередник у вирішенні держаних питань, а як господарська одиниця зі своїми внутрішніми проблемами.

Цілі статті. Метою роботи є визначення шляхів вирішення проблем фінансово-економічної безпеки державних підприємств, а також проаналізувати ефективність управління ними.

Виклад основного матеріалу. Роль та необхідність функціонування державних підприємств обговорюється науковцями тривалий час.

По-перше, навряд чи можна піддавати сумніву положення про те, що державне підприємство є визначальною складовою країн з ринковою економікою та поширене передусім у галузях, які мають важливе значення для всієї економіки, або в галузях, що потребують великих капіталовкладень і де приватні чи колективні підприємства не можуть забезпечити достатньої норми прибутку для розширеного відтворення.

Фактично в сучасних умовах саме державні підприємства покликані захищати національні інтереси, забезпечувати захист, правопорядок, благоустрій, культурний та історичний розвиток та збагачення. З огляду на значущість цих сфер діяльності, а також реалізації зазначених функцій, подальший розвиток та ефективне використання потенціалу державних підприємств становить одну з базисних цілей будь-якої країни, яка намагається отримати максимальний соціальний ефект від своєї економіки в умовах стрімкого розвитку ринків та їх коливань [3, с. 87].

По-друге, варто нагадати, що сучасні економісти часто пов'язують функціонування та розвиток державних підприємств з об'єктивними недоліками ринків, тобто з наявністю в ринковій економіці таких сфер, галузей та виробництв, до результатів діяльності яких критерій максимізації прибутку об'єктивно не застосовується [4, 66–81]. У цьому плані в умовах ринкової економіки слід говорити не про поступове «відмирання економічної функції держави», а про те, що сама держава стає важливим виробником цілого ряду товарів та послуг, якими вона має забезпечити громадян і без яких неможливий нормальний суспільний розвиток [5, с. 94].

У зв'язку з цим стабільне та безпечне функціонування державних підприємств є стратегічним напрямком розвитку економіки.

Сьогодні в Україні функціонують державні підприємства, які існують на основі державної власності, разом із приватними підприємствами. Одним із чинників визначення ефективності державного підприємництва є їхня правова база.

Державне підприємництво виконує багато важливих функцій у ринковій економіці. Виступаючи альтернативою приватному, воно здійснює такі призначення, які або не можуть бути забезпечені приватною ініціативою, або задовольняються нею на умовах вищих суспільних витрат.

Найчастіше серед цілей державного підприємництва називають забезпечення населення суспільними товарами (благами). На відміну від індивідуальних товарів, виробництво яких у своїй основі є прерогативою приватного бізнесу, суспільні товари знаходяться у сфері громадських інтересів.

Ці товари характеризуються двома ознаками:

1) неконкурентність, що означає загальнодоступність блага, можливість його безоплатного споживання;

2) невинятковість, означає, що ніхто не може бути дискримінований під час його споживання [1, с. 258].

Одна із функцій державного підприємництва полягає у тому, що воно виступає ініціатором (провайдером) щодо приватного сектору. Воно започатковує процеси, спрямовані на реконструкцію та розвиток економічного потенціалу суспільства, зростання сукупного капіталу. Саме державні виробничі об'єкти можна трактувати і як своєрідну матеріальну базу, і як інструмент для здійснення урядової економічної політики. Ще однією із функцій державного підприємництва є реалізація соціальних цілей. На сучасну державу покладається обов'язок вирішення соціальних проблем, розвиток соціальної інфраструктури. Досягнення соціальної рівноваги у суспільстві є важливим чинником державного підприємництва [6].

Аналіз результатів ринкових перетворень в Україні показує, що ефективному використанню державної власності через інститути державного підприємництва перешкоджають багато проблем:

- відсутні науково обґрунтовані критерії оптимізації обсягу і структури державного сектору економіки;
- потреба в удосконаленні механізму державного регулювання і контролю на підприємствах з державною формою власності;
- відсутня стратегія розвитку підприємств державного сектору економіки;
- низький професійний рівень менеджменту підприємницької діяльності.

Чинники, що сприяють поширенню державного підприємництва, є дезорганізація, нестійкість або порушення функціонування ризиків, слабкість національного приватного капіталу, військово-стратегічні і політичні мотиви. Політика фінансового забезпечення підприємств держави здійснюється за допомогою галузевих програм розвитку народного господарства, які розробляються для реалізації державного регулювання їх розвитку та вирішення важливих проблем галузі [1].

Сьогодні в Україні залишаються невирішеними проблеми, пов'язані з утворенням дійового механізму державної влади в цілому та управління державними підприємствами зокрема. Неодноразові спроби скорочення чисельності апарату управління, перебудови відомств не зробили дії органів виконавчої влади ефективнішими.

Не вдалося також усунути суб'єктивізм у визначенні функцій та владних повноважень центральних і місцевих органів. Як і раніше, дублюються функції органів виконавчої влади, їхня діяльність характеризується слабкою виконавчою дисципліною. Крім того наявність величезної кількості нормативних актів та розпоряджень і їх ігнорування органами виконавчої влади свідчать про зростання авторитарної бюрократизації вищих управлінських рівнів.

Зниження ролі державного управління, дезорганізація у здійсненні важливих функцій виконавчої влади багато в чому є наслідком хибного підходу до економічних реформ, в основі якого була переконаність у безмежних можливостях самоорганізації ринку та необхідності усунути державу від управління економікою. Доцільно звернутись до зарубіжного досвіду управління державними підприємствами.

Правовий статус державних підприємств у різних країнах відзначається великою різноманітністю. При цьому в жодній країні, як правило, немає єдиного законодавчого акта, який би регулював діяльність усіх державних підприємств. Практично кожне підприємство створюється і діє на основі спеціальної постанови державних установ, які регламентують методи контролю та управління з боку держави, а також регулюють фінансові і майнові відносини з державою та ринком.

Так, за допомогою системи законів про державні підприємства та компанії, у Великобританії повністю побудоване поводження всього державного сектора національної економіки, причому змодельовано виходячи з особливостей кожного підприємства. Один закон про державне підприємство поширюється на державний авіаційний концерн і державну взуттєву фабрику, а також всю національну залізничну систему. Зрозумілою в британській системі є роль галузевих міністерств, які створені не для того, щоб давати державним підприємствам вказівки, а з метою контролю за виконанням чинного законодавства [7, с. 219].

У Франції на державному підприємстві діє урядовий комісар; як правило, він є представником міністерства, під юрисдикцією якого перебуває дане підприємство, бере участь у засіданнях правління. Програму капіталовкладень розробляє фонд економічного і соціального розвитку. Рахункова палата кожні 2 роки готує доповідь про управління і фінансові результати державних підприємств. На кожному з них працює призначений судовим органом бухгалтер-ревізор, котрий здійснює аудит оформлення бухгалтерської звітності. Найвище право контролю за діяльністю державних підприємств надано парламенту. Але управління ними не зводиться тільки до контролю.

У Польщі становище державних підприємств затверджено відповідним законом від 1981 р., до якого вже кілька разів вносилися поправки. Закон постулює, що державне підприємство – незалежний суб'єкт, створений державним органом, що перший його

директор призначається органом-засновником, окремі зміни мають відбуватися за погодженням з органом-засновником, а бухгалтерська звітність проводиться за звичайними стандартами.

Так, зарубіжний досвід управління державними підприємствами показує, що саме держава має створити сприятливі умови для їх розвитку, і перш за все шляхом фінансової підтримки, збільшення статутного капіталу, надання дотацій, субсидій тощо.

Висновки. Таким чином, дослідивши поняття, функції державних підприємств та поглибившись у досвід зарубіжних країн в даній сфері, можна зробити висновок про їх необхідність, доцільність та вагомість існування в сучасних ринкових умовах. Це пояснюється тим, що держава має бути гарантом стабільності, недоторканності та правопорядку, а державні підприємства є засобом досягнення цього, оскільки саме вони спроможні протистояти стихійним силам ринку та діяти там, де приватний власник є неефективний. Водночас, варто наголосити, що основним призначенням державних підприємств, крім надання товарів, послуг і благ, є досягнення економічного та соціального ефекту в країні, що є запорукою захисту держави, її загальнонаціональних інтересів, цілісності, правопорядку і безпеки. Наявність великої кількості загроз вимагає розробки та реалізації дієвих заходів із забезпечення фінансово-економічної безпеки державних підприємств.

Список літератури

1. Фурдичко Л. Є. Проблеми функціонування і фінансування державних підприємств в Україні / Л. Є. Фурдичко // Вісник Національного університету "Львівська політехніка". – 2011. – № 720 : Менеджмент та підприємництво в Україні: етапи становлення і проблеми розвитку. – С. 257–261.
2. Зюзь Д. В. Внутрішнє фінансування як чинник підвищення ефективності діяльності державних підприємств / Д. В. Зюзь // Вісник Національної академії державного управління при Президентові України. Серія : Державне управління. - 2018. - № 2. - С. 27-33. - URL: http://nbuv.gov.ua/UJRN/vnaddy_2018_2_6
3. Шестак М. Л. Проблеми функціонування державних підприємств у ринковій економіці: теоретичний аспект / М. Л. Шестак // Наукові праці МАУП. Сер. : Економічні науки. Психологічні науки. - 2013. - Вип. 2. - С. 87-91. - Режим доступу: http://nbuv.gov.ua/UJRN/Npmaupe_2013_2_17.
4. Самуэльсон П. А. Экономика / П. А. Самуэльсон, В. Д. Нордхаус; пер. с англ. — М.: БИНОМКНОРУС, 1997. — 800 с.
5. Макконелл К. Р. Экономика: принципы, проблемы, политика / К. Р. Макконелл, С. Л. Брю; пер. с англ. — В 2-х т.: Т. 1. — М.: Республика, 1992. — 399 с
6. Аніловська Г.Я. Місце та роль державного підприємництва у ринковій трансформації // Науковий вісник. – 2007. – Вип. 17.1 - С.173-179.
7. Мельник Л. Ю. Держава і власність / Л. Ю. Мельник, М. Х. Корецький. — Дніпропетровськ: Січ, 2002. — 411 с.

УДК 338:47:338:49

Б. Ігнатенко, магістр гр. АДМ-18М
Т. Грінка, доц, канд. екон. наук
Центральноукраїнський національний технічний університет

УДОСКОНАЛЕННЯ МЕХАНІЗМУ УПРАВЛІННЯ ТРАНСПОРТНОЇ СИСТЕМИ МІСТА

В статті розглянуто економічна сутність та особливості формування механізму управління транспортної системи міста а також напрями його вдосконалення. Обгрунтовано концептуальні підходи щодо ввпровадження організаційно-економічного механізму регулювання транспортної системи міста, що дозволить забезпечити баланс інтересів місцевих органів влади, нселення. приватного капіталу.

Транспорт є однією з головних складових територіального поділу праці та засобом забезпечення територіальних взаємозв'язків, сполучною ланкою між виробництвом і споживанням. Разом з іншими галузями транспортний комплекс міст є заставою ефективного розвитку усіх сфер його життєдіяльності, а також індикатором якості життя населення. Роль транспорту невпинно зростає, а особливо в період втілення в життя масштабних інтернаціональних інтеграційних планів.

Проблема та її зв'язок із важливими науковими чи практичними завданнями. На сьогодні міський пасажирський транспорт у багатьох містах України функціонує неефективно в економічному та соціальному аспектах. Перевезення пасажирів є збитковими, якість транспортного обслуговування населення не відповідає сучасним вимогам, негативний вплив громадського транспорту на здоров'я людини зростає. Для забезпечення подолання наявних проблем та підвищення ефективності функціонування громадського транспорту в містах країни вирішальним є удосконалення сталого механізму управління його розвитком, що зумовлює актуальність даного дослідження.

Аналіз досліджень і публікацій останніх років. Економічні проблеми розвитку транспортної інфраструктури досліджували у своїх роботах такі зарубіжні та вітчизняні вчені, як А. І. Воркут, Б. Л. Геронімус, П. Н. Розенштейн-Родан, Є. Симоніс, Є. Шотлер, Д. Р. Рей, Є. А. Жуков, В. Н. Іванов, В. Є. Канарчук, Л. В. Канторович, Є. Л. Логінов, А. М. Ткаченко, А. А. Багдаєв, О. П. Голіков, В. Г. Шинкаренко, А. І. Абрамов, А. В. Вельможин. Функціонування транспортної інфраструктури та її значення для економіки вивчали такі вітчизняні та зарубіжні науковці, як Р. А. Кожевніков, В. Є. Виноградов, А. Н. Перцев, Г. П. Андрєєв, П. Друкер, У. Ростоу, Дж. Бастіа. Таким чином, дослідженню інфраструктури у сучасній економіці приділяється достатньо уваги в науковій літературі, проте неповною мірою висвітленими залишаються проблеми виявлення місця та ролі транспортної інфраструктури в транспортній системі та в процесі реалізації національних економічних інтересів держави, що зумовило інтерес до дослідження зазначених питань.

Невирішені частини загальної проблеми. За сучасних умов ринкової економіки потреба надання транспортних послуг належного рівня в містах України зростає. Стан транспортної галузі та рівень її розвитку у Кропивницькому на даному етапі не можна вважати задовільними. Збільшилась кількість відмов у роботі об'єктів інфраструктури у зв'язку з технічним та моральним зносом, що призводить до економічної кризи транспортної інфраструктури.

Ціллі статті Метою статті є дослідження та розробка деяких питань удосконалення механізму управління транспортною системою міста.

Виклад основного матеріалу дослідження з новим обґрунтуванням отриманих наукових результатів. За результатами попередніх досліджень можна стверджувати, що для стабільної роботи транспортних підприємств та задоволення вимог пасажирів важливим є забезпечення соціально-економічного розвитку міського-пасажирського транспорту.

Тому до формування механізму управління розвитком транспортної системи міста необхідно підходити комплексно та враховувати, що результатом його реалізації має бути досягнення бажаного економічного та соціального ефекту. Механізм, з точки зору управління, є певною керуючою системою (методів, принципів, цілей, функцій тощо), дія якої перетворює іншу (керовану) систему, тобто змінює її стан, досягаючи при цьому поставлену мету. Механізм є єдиною системою, яка складається із взаємопов'язаних елементів, дія якого забезпечує процес управління іншою системою. Процесом є зміна станів системи, а механізм є рушійною силою, що спонукає цей процес. Під механізмом управління стратегічним розвитком транспортної системи міста можна розуміти сукупність методів, інструментів та важелів впливу на процеси досягнення стратегічних цілей, об'єднаних у систему, яка функціонує за певними принципами та забезпечує сталий розвиток міського пасажирського транспорту. Формування механізму управління стратегічним розвитком міського пасажирського транспорту передбачає послідовне визначення його структури,

принципів та функцій, а реалізація цього механізму вимагає чіткого визначення принципів, методів, важелів, інструментів.

Головними принципами формування механізму управління стратегічним розвитком транспортної системи міста є:

Системності: механізм управління стратегічним розвитком муніципальної транспортної системи повинен являти собою єдину систему, елементи якої пов'язані між собою і формують ієрархічну структуру та яка взаємодіє із зовнішнім середовищем;

Адаптивності: механізм повинен швидко реагувати на зміни зовнішніх та внутрішніх умов і забезпечувати стабільний розвиток системи міського пасажирського транспорту в нових умовах її функціонування;

Збалансованості інтересів: при формуванні механізму повинні бути враховані інтереси всіх учасників перевізного процесу;

Альтернативності: механізм повинен передбачати різні варіанти (альтернативи, сценарії) розвитку та відповідно до них – стратегічні напрями розвитку міського пасажирського транспорту.

Функціонування механізму управління стратегічним розвитком транспортної системи міста повинно відбуватися відповідно до таких принципів:

Ефективності: механізм повинен бути ефективним, тобто забезпечувати досягнення поставленої мети, а саме: реалізацію стратегії розвитку муніципальної транспортної системи, спрямовану на підвищення економічної, соціальної та екологічної ефективності її функціонування;

Інтегративності: всі складові механізму повинні бути направлені на досягнення єдиної мети, функціонувати взаємоузгоджено та спільно;

Ідентифікації та розподілу завдань: визначення та закріплення за кожною структурною одиницею механізму чітко визначених завдань, виконання яких забезпечить реалізацію стратегії розвитку транспортної системи міста;

Обґрунтованості методів управління: методи управління розвитком муніципальної транспортної системи повинні бути науково-обґрунтованими та доцільними для застосування.

Основними функціями механізму управління стратегічним розвитком транспортної системи міста є:

1) Планування – передбачає визначення стратегічних напрямів розвитку муніципальної транспортної системи та відповідно до них комплексу заходів, направлених на досягнення стратегічних цілей;

2) Організація – забезпечує організацію перевізного процесу і координування діяльності міського громадського транспорту та її матеріально-технічного, кадрового, інвестиційного забезпечення;

3) Регулювання – функція, спрямована на оперативне управління діяльністю міського пасажирського транспорту, забезпечення її ефективності при зміні зовнішніх та внутрішніх умов, внесення оперативних коригувань у стратегічні плани розвитку муніципальної транспортної системи;

4) Мотивація – функція, що передбачає стимулювання трудових колективів до ефективного виконання запланованих стратегічних завдань та зростання їх зацікавленості у результатах роботи міського пасажирського транспорту;

5) Контроль – функція, що забезпечує постійне спостереження та оцінку діяльності транспортної системи міста з метою виявлення резервів підвищення її ефективності.

Головною метою функціонування наведеного механізму є забезпечення сталого розвитку міського пасажирського транспорту.

За статистичними даними станом на 01.12.2017 р., чисельність населення міста Кропивницького складає 240,0 тис. осіб, для задоволення потреб якого в пасажирських перевезеннях створена мережа міських маршрутів загальною протяжністю 835,6 км, яка сформована з 44 автобусних та 4 тролейбусних маршрутів. На вказаних маршрутах

транспортні засоби працюють у звичайному режимі руху та режимі маршрутного таксі і здійснюють перевезення пільгових категорій пасажирів.

Щоденний обсяг перевезень автомобільним транспортом загального користування у м. Кропивницькому складає 144 тис. пасажирів.

Для обслуговування маршрутної мережі використовуються в середньому 470 автобусів: 20 – великої місткості, 25 – середньої місткості та 415 мікроавтобусів. Для перевезення осіб з обмеженими фізичними можливостями задіяно 51 одиницю транспортних засобів.

З жовтня 2017 року відновлено обслуговування маршрутів автобусами великої та середньої пасажиромісткості, а саме наступних мікрорайонів: Стара і Нова Балашівка, Лелеківка, Новоолексіївка, Кущівка, Катранівка, Арнаутово, Никанорівка, Новомиколаївка, Ковалівка, Озерна Балка, Завадівка, район Телецентру, смт. Нове, сел. Молодіжне, Гірниче.

Головним завданням на 2020-2022 роки є також запровадження роботи маршрутів звичайного режиму руху автобусами середньої пасажиромісткості та забезпечення стабільного транспортного сполучення мікрорайонів міста.

Основними пріоритетними напрямками на 2020-2022 роки мають бути наступні заходи:

запровадження на маршрути транспортних засобів великої та середньої місткості;

обладнання пристроями GPS – навігації та підключення всіх автобусів до диспетчерської служби для забезпечення ефективного контролю за роботою громадського транспорту;

сприяння перевізникам та створення умов для оновлення міських автобусів, у тому числі їхньої заміни на автобуси більшої місткості;

активізація роботи з Управлінням патрульної поліції у м. Кропивницькому щодо заборони стоянок на зупинках громадського транспорту та у місцях обмеженої пропускної спроможності центральних вулиць міста, зокрема вулиць Великої Перспективної, Преображенської, Шевченка, Шульгиних, Декабристів, В'ячеслава Чорновола;

придбання нового рухомого складу на КП «Електротранс» Міської ради міста Кропивницького».

Механізм управління розвитком міського пасажирського транспорту являє собою складну систему, яка включає: організаційно-інституційну, техніко-технологічну, інноваційно-інвестиційну та інформаційну складову.

Висновки. Однією із невід'ємних складових сталого розвитку сучасного міста є надійна, ефективно функціонуюча муніципальна транспортна система. Управління цією системою потребує вдосконалення шляхом впровадження дієвого механізму управління, який би ґрунтувався на засадах сталого розвитку та забезпечував збалансованість економічного, соціального та екологічного зростання. Функціонування механізму управління розвитком транспортної системи міста має бути направлене на досягнення:

1) Економічного ефекту: подолання збитковості перевізниками та інвестиційне забезпечення подальшого розвитку міського пасажирського транспорту;

2) Соціального ефекту: підвищення якості транспортних послуг та повне задоволення потреб населення у перевезеннях.

Список літератури

1. Біліченко В.В. Управління розвитком виробничої системи міських пасажирських перевезень / В.В. Біліченко, С.В. Цимбал, С.О. Романюк // Вісник ЖДТУ. – № 2 (53). – 2010. – С.11-19.
2. Бутко М.П. Транспортна компонента виробничої інфраструктури регіону: монографія / М.П. Бутко, Н.В. Іванова – Ніжин: ТОВ «Видавництво «Аспект-поліграф», 2010 – 312 с.
3. Вдовиченко В.О. Ефективність функціонування міської пасажирської транспортної системи: автореф. дис…канд.техн.наук: 05.22.01/ В.О. Вдовиченко.– К., 2004. – 20 с.
4. Величко В.В. Економіко-організаційне забезпечення міського пасажирського транспорту як функції міста: автореф. дис…канд.екон.наук: 08.10.01 / В.В. Величко. – Х., 2000. – 24 с.

УДК 338.65: 658.8

М. Кадет, магістр гр. УФЕБ-18М
Центральноукраїнський національний технічний університет

ЕКОНОМІЧНА БЕЗПЕКА ТОРГОВЕЛЬНОГО ПІДПРИЄМСТВА: ОСОБЛИВОСТІ ТА МЕХАНІЗМ ЗАБЕЗПЕЧЕННЯ

Стаття присвячена питанням розвитку підприємств торгівлі за рахунок забезпечення економічної безпеки. Визначено теоретичні основи економічної безпеки підприємства, зокрема етимологію даного поняття, об'єкти, суб'єкти, мета та завдання. Окремо розглянуто механізм забезпечення економічної безпеки торговельного підприємства через призму системного та комплексного підходів.
економічна безпека, торгівля, торговельне підприємство, механізм, система економічної безпеки, механізм економічної безпеки, об'єкт, суб'єкт, завдання

Постановка проблеми. Останніми роками в Україні спостерігаються кризові явища окремих секторів економіки, причому торгівля є одним із них. При цьому, торговельна діяльність в Україні на сьогодні вважається однією з найпоширеніших форм підприємництва.

Торговельні підприємства є чутливими до дестабілізуючих факторів впливу як із зовні, так із середини. Нестабільні умови зовнішнього та внутрішнього середовища вимагають від підприємств торгівлі постійного підтримання необхідного рівня економічної безпеки. В іншому випадку не може йти мова про розвиток та ефективність їх функціонування. Торгівля як посередницька ланка залежить як від виробництва, так і споживання товарів зумовлює особливості у функціональних складниках та індикаторах, сукупності загроз і ризиків, підходах до гарантування безпеки.

Економічну безпеку можна представити як динамічну систему, яка забезпечує стійке функціонування і розвиток підприємства за допомогою найбільш раціонального використання фінансових, трудових, технічних, інформаційних та інших ресурсів підприємства.

Аналіз останніх досліджень і публікацій. Питанням вивчення економічної безпеки підприємств сьогодні присвячується багато наукових досліджень, автормаи яких є Л. П. Артеменко, О. Р. Бойкевич, О. О. Бородіна, О. В. Орлик, Т. Г. Логутова, Д. І. Нагаєвський, О. О. Хворост, О. С. Шуміло, Т. Г. Васильців, В. І. Волошин, В. В. Каркавчук, С. В. Васильчак, О. Р. Жидяк, К. С. Тимощенко, Ф. І. Євдокимов, О. В. Мізіна, Ю. О. Ярова, О. Д. Тімченко, та багато інших. У переважній більшості публікацій проаналізована економічна безпека підприємства через її складові елементи, структуру, методи забезпечення, принципів та механізму її дії, а також представлено способи її оцінювання.

Питання розвитку торгівлі, стали об'єктом уваги таких учених як П. Й. Атамас, А. М. Виноградської, П. Авсєєв, М. Афанасьєв, О. Галушкіна, І. Лазебна, А. Мазаракі, Л. Осипова та ін.

Разом з тим, потребують більш детального вивчення питання, які стосуються аналізу економічної безпеки саме підприємств торгівлі, їх внутрішніх та зовнішніх загроз, а також системи її забезпечення.

Цілі статті. Метою статті є формування науково обґрунтованої системи економічної безпеки на торговельному підприємстві, що потребує розробки методологічних засад управління економічною безпекою підприємств торгівлі.

Виклад основного матеріалу. Економічна безпека підприємства являє собою складну систему, що поєднує в собі комплекс показників, факторів впливу та зв'язків між ними. Дослідимо етимологію даного показника.

На думку Приходько В. П. економічна безпека суб'єкта підприємницької діяльності досягається як забезпеченням його конкурентоспроможності протягом тривалого періоду, так і шляхом створення системи захисту від неефективно функціонуючої держави власних економічних інтересів [1].

Ярова Ю. А [2] економічну безпеку підприємства характеризує через сукупність якісних та кількісних показників, що залежать від спроможності керівництва підприємства та спеціалістів ефективно уникнути можливих загроз і ліквідувати шкідливі наслідки негативних складових зовнішнього і внутрішнього середовища підприємства.

Думка Груніна О. А. стосовно економічної безпеки підприємства заключається в тому, що він дане поняття визначає як стан господарчого суб'єкта, у якому він при найбільш ефективному використанні корпоративних ресурсів досягає послаблення, запобігання або захисту від існуючих небезпек та загроз або непередбачених обставин і в основному забезпечує досягнення цілей бізнесу в умовах конкуренції та господарчого ризику [3]. Олейніков Є. А. – «Стан найбільш ефективного використання ресурсів для подолання загроз і забезпечення стабільного функціонування підприємства сьогодні і в майбутньому» [4].

Більшість авторів розглядають економічну безпеку підприємства через призму системного підходу. Розглянемо найбільш репрезентативні з них.

Так, Реверчук Н. Й. економічну безпеку підприємства визначає як систему активного захисту від можливих матеріальних, людських і фінансових втрат, за якої реальні чи можливі збитки будуть меншими від встановлених норм [5]. На думку Кашина А. В., система економічної безпеки підприємства – це сукупність поглядів ідей, цільових установок, що направлені на забезпечення стабільного функціонування підприємства. Вона включає заходи, шляхи, напрямки досягання поставлених завдань та забезпечення умов для досягнення цілей бізнесу в умовах невизначеності та заходи запобігання діям внутрішніх і зовнішніх загроз [6]

Переважно під системою економічної безпеки підприємства розуміють комплекс організаційно-управлінських, режимних, технічних, профілактичних і пропагандистських заходів, спрямованих на якісну реалізацію захисту пріоритетних інтересів підприємства від зовнішніх та внутрішніх загроз [7]. Досить актуальним є підхід до визначення економічної безпеки як стану розвитку економічної системи, що забезпечує її ефективне функціонування засобами належного використання внутрішніх і зовнішніх чинників з урахуванням інтересів майбутніх поколінь, а також здатність до відтворення та результативного протистояння внутрішнім і зовнішнім впливам [8].

Елементами комплексної системи економічної безпеки підприємства, зокрема торговельного, є об'єкт та суб'єкт, мета та механізм її забезпечення.

Об'єкт і суб'єкт системи забезпечення економічної безпеки підприємства тісно взаємозв'язані. Об'єктом системи в цілому виступають цілі та інтереси підприємства в поточному і перспективному періоді.

Суб'єкт системи забезпечення економічної безпеки торговельного підприємства, як правило, носить складніший характер, оскільки його діяльність обумовлюється не тільки особливостями і характеристиками об'єкту, але і специфічними умовами зовнішнього середовища, яке оточує підприємство.

Виходячи з цього, можна виділити дві групи суб'єктів, що забезпечують економічну безпеку підприємства: зовнішні суб'єкти і внутрішні. До зовнішніх суб'єктів відносяться органи законодавчої, виконавчої і судової влади, покликані забезпечувати безпеку всіх без винятку законослухняних учасників господарських відносин. Ці органи формують законодавчу основу функціонування і захисту господарської діяльності в різних її аспектах і забезпечують її виконання. До внутрішніх суб'єктів відносяться особи, що безпосередньо здійснюють діяльність по захисту економічної безпеки даного конкретного суб'єкта господарської діяльності. Такими суб'єктами можуть виступати: працівники власної служби

безпеки підприємства; залучені працівники фірм, що надають послуги із захисту діяльності підприємства. Внутрішні суб'єкти, що забезпечують економічну безпеку підприємства, здійснюють свою діяльність на основі певної стратегії і тактики [9].

Метою забезпечення економічної безпеки торговельного підприємства є запобігання можливому нанесенню збитків його діяльності; захист прав підприємства; захист співробітників і власності від джерел зовнішніх і внутрішніх загроз; збереження і ефективне використання фінансових, матеріальних і інформаційних ресурсів; своєчасне виявлення і припинення різних правопорушень, запобігання причинам і умовам, що їх породжують; а також недопущення надзвичайних ситуацій або мінімізація їх негативних наслідків [10, с. 377].

Виходячи з необхідності досягнення мети забезпечення економічної безпеки підприємницької діяльності, можна визначити перелік основних завдань, які вирішуються системою економічної безпеки:

- оцінка надійності і ступеня захищеності торговельного підприємства від внутрішніх і зовнішніх загроз;
- своєчасне виявлення зазіхань на ресурси торговельного підприємства і ефективне припинення загроз керівництву і персоналу на основі комплексного підходу до безпеки;
- виявлення причин і умов, що сприяють нанесенню фінансового, матеріального і морального збитку інтересам торговельного підприємства, порушенню його нормального функціонування і розвитку;
- добування необхідної інформації для вироблення оптимальних управлінських рішень з питань стратегії і тактики стійкої економічної діяльності;
- вивчення партнерів, клієнтів і конкурентів, забезпечення безпеки зовнішньої діяльності торговельного підприємства;
- створення умов для відшкодування матеріального і морального збитку, що наноситься неправомірними діями юридичних і фізичних осіб, ослаблення негативних наслідків, що виникли через порушення економічної безпеки;
- виявлення відповідного впливу на формування у партнерів і клієнтури сприятливої думки про торговельне підприємство ;
- збір, аналіз, оцінка і прогнозування відомостей, що характеризують стан всього комплексу системи безпеки торговельного підприємства, контроль за ефективністю її функціонування [11, с. 42].

Механізм забезпечення економічної безпеки торговельного підприємства, направлений на створення і реалізацію умов, які б забезпечили ефективний захист його інтересів. Будь-який механізм, в тому числі і механізм забезпечення економічної безпеки торговельного підприємства, повинен ґрунтуватися на наступних принципах :

- законність, який передбачає, що будь-які заходи щодо забезпечення економічної безпеки повинні прийматися в рамках чинного законодавства і не суперечити йому;
- поєднання превентивних і реактивних заходів;
- координація і взаємодія, щоб зусилля всіх підрозділів підприємства та окремих виконавців, які забезпечують економічну безпеку, були належним чином спрямовані і скоординовані;
- поєднання гласності з конспірацією;
- компетентність, тобто питаннями забезпечення безпеки підприємства повинні займатися професіонали, які володіють необхідними знаннями та навичками, вміють своєчасно оцінити ситуацію і приймати правильні рішення;
- безперервність, який передбачає, що функціонування комплексної системи забезпечення економічної безпеки підприємства повинно здійснюватися постійно на плановій основі;

- плановість, тобто ефективне забезпечення економічної безпеки підприємства можливе за умов, коли вибір і застосування сил, засобів та охоронних заходів здійснюється на основі детально продуманої концепції;
- диференціація заходів передбачає вибір заходів щодо подолання виниклих загроз залежно від характеру загрози і ступеня тяжкості наслідків її реалізації;
- підконтрольність системи забезпечення економічної безпеки керівництву підприємства, щоб система безпеки не перетворилася на замкнуте утворення, орієнтоване на вирішення вузьких завдань без урахування інтересів підприємства в цілому, і для оцінки ефективності діяльності системи і її можливого вдосконалення;
- економічна доцільність передбачає, що витрати на організацію системи безпеки не повинні перевищувати рівня, при якому втрачається економічний зміст їх застосування [9].

Висновки. Таким чином, забезпечення економічної безпеки не є спонтанним процесом, а являє собою заздалегідь продуманий механізм, який ґрунтується на системному підході. Такий підхід передбачає глибоке дослідження явищ і процесів, а також включає дослідження внутрішнього та зовнішнього середовища та взаємозв'язків між ними.

Дослідження виявило, що структура економічної безпеки підприємства виражається забезпеченістю підприємства якісними ресурсами, їх оптимальними запасами з урахуванням можливих ризиків господарської діяльності. При цьому всі ресурси повинні бути ефективно задіяні в рентабельне виробництво для забезпечення отримання прибутку та підтримки ліквідності підприємства. Це дозволить витримати цільові установки розвитку підприємства з точки зору економічної безпеки.

Надійна економічна безпека торговельного підприємства вимагає також комплексного підходу, що дозволяє забезпечити стратегічний розвиток підприємства, розробити тактичні та оперативні дії для мінімізації наслідків кризи та негативного впливу загроз.

Список літератури

1. Приходько В. П. Управління економічною безпекою підприємства / В. П. Приходько // Економіка та держава. - 2013. - № 10. - С. 10-12. - Режим доступу: http://nbuv.gov.ua/UJRN/ecde_2013_10_4.
2. Ярова Ю. О. Структура економічної безпеки підприємства в умовах кризи / Ю. О. Ярова, Л. П. Артеменко // Економічний вісник Національного технічного університету України "Київський політехнічний інститут". - 2016. - № 13. - С. 257-263. - Режим доступу: http://nbuv.gov.ua/UJRN/evntukpi_2016_13_39
3. Грунин О. А., Грунин С. О. Экономическая безопасность организации. – СПб.: Питер, 2002. – 160 с.
4. Олейников Е. А. Основы экономической безопасности. – М. – 1997. – 233 с
5. Реверчук Н.Й. Управління економічною безпекою підприємницьких структур: монографія / Н. Й. Реверчук; Нац. Банк України. Львівський банк. Інститут. – Львів: ЛБІ НБУ, 2004. – 196 с.
6. Кашин А.В. Экономическая безопасность предприятия: управление решения: автореф. дис. на соиск. уч. степени канд. екон. наук: спец: 08.00.05 «Экономика и управление народным хозяйством» (экономическая безопасность) / А.В. Кашин. – М., 2008. – С. 21.
7. Пухальська Г.В. Економічна безпека підприємства: суть та її складові / Г.В. Пухальська, Г.О. Христич // Вісник Хмельн. нац. ун-ту. ек. наук. – 2008. – № 6. – Т. 1. – С. 198-200.
8. Гончарук Я.А. Диференціація підходів до аналізу категорії «економічна безпека держави» / Я.А. Гончарук, М.І. Флейчук // Збірник наукових праць Львівського державного університету внутрішніх справ. Серія економічна. – 2009. – № 2. – С. 15-30.
9. Хомів О.В. Аналіз впливу внутрішніх загроз на економічну безпеку торговельних підприємств / О.В. Хомів, А.В. Сибірний // Вісник Донецького національного університету. Серія В. Економіка і право. – 2015. – № 11. – С. 404-408.
10. Бланк И.А. Управление финансовой безопасностью предприятия. – К. : Изд-во «Эльга», «Ника-Центр», 2004. – 784 с.
11. Коробчинський О.Л. Методика формування системи економічної безпеки підприємства / О.Л. Коробчинський // Актуальні проблеми економіки. – 2009. – № 4 . – С. 41- 45.

УДК 336.77

А. Капшученко, магістр гр. ПД-201 МЗ
Національний авіаційний університет, м. Київ

ТЕОРЕТИКО-МЕТОДИЧНІ ЗАСАДИ УПРАВЛІННЯ ПІДПРИЄМНИЦЬКИМИ РИЗИКАМИ

Стаття присвячена дослідженню теоретико-методичних засад управління підприємницькими ризиками у сучасних умовах. Визначено сутність підприємницьких ризиків як економічної категорії, яка полягає у ймовірності настання певних подій, зумовлених змінами й невизначеністю у зовнішньому і внутрішньому середовищі підприємства, які можуть спричинити відхилення отриманих результатів господарської діяльності від очікуваних як у негативному, так і в позитивному напрямі. Досліджено підходи до проведення класифікації підприємницьких ризиків шляхом комплексного розгляду різноманітності видів ризиків за різними класифікаційними ознаками. Визначено складові механізму управління підприємницькими ризиками шляхом виокремлення його етапів, стратегій управління ризиком в залежності від його рівня та методів управління ризиками.

ризик, підприємництво, управління, ризик-менеджмент, невизначеність, аналіз

Сучасний етап розвитку національної економіки, який супроводжується загостренням фінансово-економічної, політичної та соціальної криз розвитку суспільства, призвів до посилення впливу підприємницьких ризиків на діяльність суб'єктів господарювання. Підприємницька діяльність вітчизняних підприємств, установ та організацій стає все більш ризиковою, а ризики супроводжують таку діяльність на всіх етапах життєвого циклу підприємства. Як результат, керівники і фахівці підприємств повинні опановувати сучасні методи, засоби та інструменти ідентифікації ризиків, їх аналізу та комплексного оцінювання, мінімізації їх негативного впливу та ефективного управління ними.

Питанням вивчення теоретико-методичних та практичних аспектів управління підприємницькими ризиками за сучасних умов присвячені наукові пошуки таких вітчизняних дослідників, як: Аранчій В. І., Бовкун О. А., Бугай В. З., Бурбело Н. О., Вербицька К. С., Вільчинська О. М., Вишневська О. А., Грубяк С. В., Дергалюк Б. В., Доценко І. О., Євдокименко В. М., Захарчук Л. Р., Ігнатенко М. М., Клочкова Н. В., Комеліна О. В., Кравченко Н. В., Латкіна С. А., Лугінін О. Є., Мацюк О. В., Мєшкова-Хрущ Н. А., Михальчук А. В., Нестеренко М. Є., Оксенюк К. І., Проценко О. О., Чайкіна А. О., Чирва Г. М. та ін.

Грубяк С. В. під підприємницьким ризиком необхідно розуміє економічну категорію, що кількісно і якісно виражається в невизначеності результату наміченої підприємницької діяльності, що відображає ступінь успіху або невдачі діяльності підприємця (фірми) в порівнянні із заздалегідь запланованими результатами [1].

Оксенюк К. І. під підприємницьким ризиком пропонує розуміти ймовірність настання несприятливих подій у процесі виробничої, збутової чи фінансової діяльності, в результаті яких суб'єкти господарювання можуть зазнати збитків, витрат, недоотримати доходи [2].

Аранчій В. І., Ігнатенко М. М. під ризиком у підприємницькій діяльності розуміють ймовірність (загрозу) настання події, що може викликати втрати чи зменшення прибутку за рахунок недоотримання доходів або появи додаткових витрат [3].

Бурбело Н. О. зазначає, що підприємницький ризик характеризується як небезпека потенційно можливої, ймовірної втрати ресурсів чи недоодержання доходів у порівнянні з варіантом, розрахованим на раціональне використання ресурсів у певному виді підприємницької діяльності [4].

Аналіз наведених визначень дозволяє дійти висновку, що єдиного погляду на сутність підприємницьких ризиків у наукових колах на даний час не існує. Більшість дослідників

акцентують увагу саме на негативних аспектах ризику, пов'язуючи його з імовірністю збитків, недоотриманням запланованих результатів, зменшенням розміру прибутку, втратою ресурсів, настанням негативних подій в умовах невизначеності тощо.

Підприємницький ризик, на нашу думку, є економічною категорією, сутність якої полягає у ймовірності настання певних подій, зумовлених змінами й невизначеністю у зовнішньому і внутрішньому середовищі підприємства, які можуть спричинити відхилення отриманих результатів господарської діяльності від очікуваних. Таке відхилення має певну ймовірність відбуватися як у негативному напрямі (поява збитків, недоотримання прибутку, втрата ресурсів тощо), так і в позитивному напрямі (отримання підприємством результатів діяльності, які певною мірою перевищують їх очікуваний розмір, унаслідок використання ситуації невизначеності на власну користь та вмілого керування ризиками).

Безпосередньо процес ризик-менеджменту може бути схематично відображений наступним чином (рис. 1): ідентифікація, оцінка, вибір стратегії, зниження ступеню ризику, контроль.

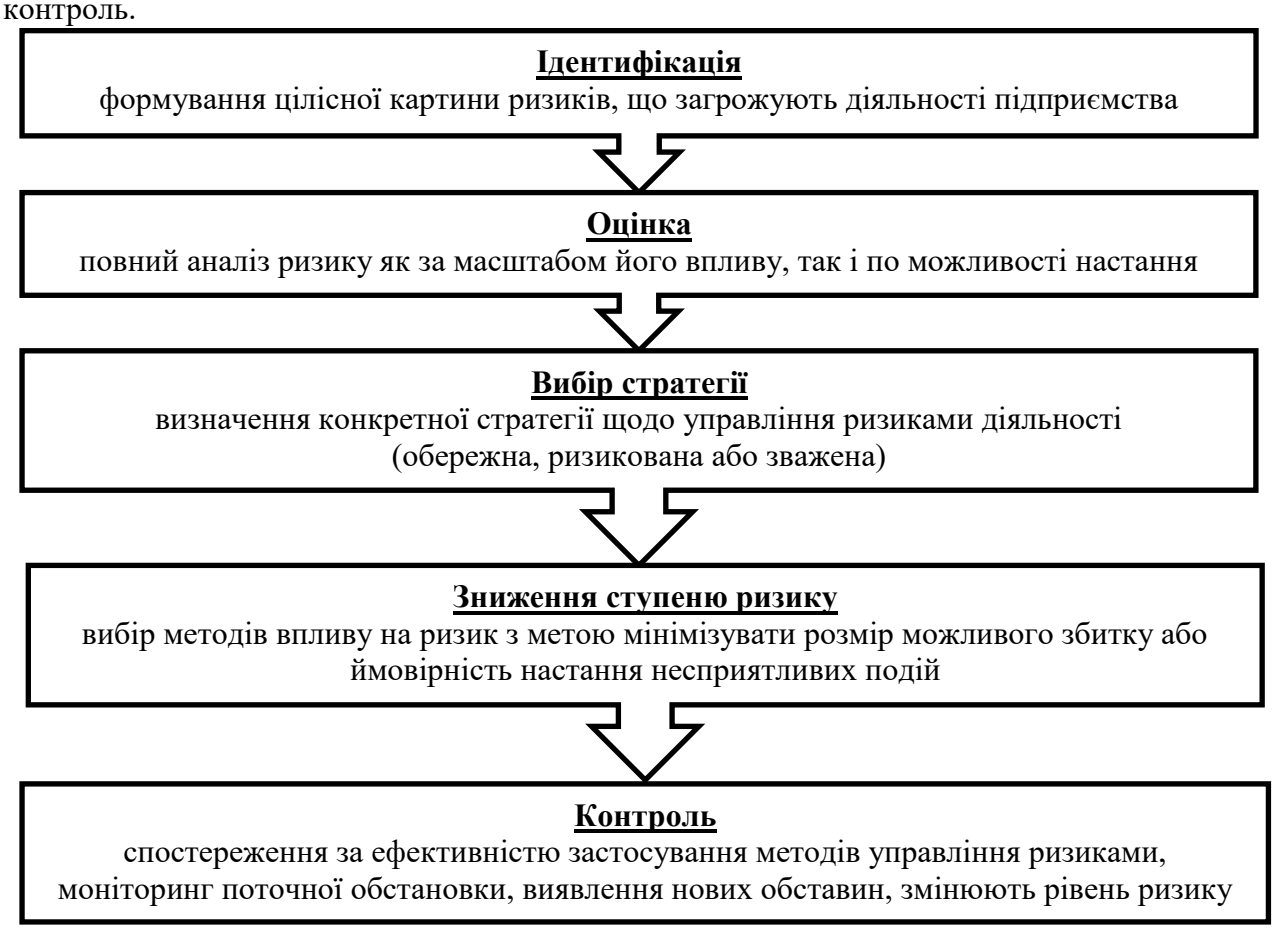


Рисунок 1 – Характеристика основних компонент ризик-менеджменту

Джерело: складено на основі [5]

Класифікація ризиків за видами діяльності підприємства включає: ризики, пов'язані зі збутовою діяльністю підприємства; ризики, пов'язані із інвестиційною та операційною діяльністю підприємства; ризики, пов'язані з фінансовою діяльністю підприємства. Залежно від можливості страхування підприємницькі ризики поділяються на ті, що страхують і ті, що не страхують. Залежно від можливості диверсифікації підприємницькі ризики поділяються на систематичні і несистематичні. Також, підприємницькі ризики можуть бути класифіковані за низкою інших ознак: за мірою впливу на діяльність підприємства, за джерелами виникнення, за тривалістю в часі, за можливістю прогнозування, за масштабом впливу, за типами, за рівнем втрат, за часом дії тощо.

Функціонування механізму управління підприємницькими ризиками передбачає послідовне виконання ряду етапів (ідентифікація, оцінка, вибір стратегії, зниження ступеню ризику, контроль), вибір відповідних стратегій управління ризиком в залежності від його рівня (низький, допустимий, високий, руйнівний), застосування конкретних підходів до управління ризиками (активний, адаптивний, консервативний) та методів управління ризиками (страхування, диверсифікацію, лімітування, резервування, прогнозування, розподіл ризиків, хеджування тощо).

Основні етапи аналізу ризиків підприємницької діяльності наведені на рис. 2.

Рисунок 2 – Основні етапи процесу аналізу ризиків підприємницької діяльності

Джерело: складено на основі [6]

Вважаємо, що причини виникнення ситуацій ризику на підприємстві найбільш доцільно класифікувати на внутрішні і зовнішні. Зовнішні причини, тобто ті, які не залежать від дій керівництва та персоналу конкретного підприємства, пов'язані з нестабільністю у військово-політичній, законодавчій, соціально-демографічній, фінансово-економічній, податковій, валютній ситуації в державі, а також з діями конкурентів, постачальників, споживачів, органів контролю, інших суб'єктів впливу.

Внутрішні причини виникнення ризиків на підприємстві, які безпосередньо залежать від існуючої системи керівництва та діяльності працівників суб'єкта господарювання, полягають у наявності недоліків чи прорахунків у виробничій, організаційній, інформаційній, маркетинговій, фінансовій, економічній, зовнішньоекономічній, інвестиційній, інноваційній, кадровій діяльності підприємства.

Кількісне оцінювання ризиків, з точки зору Лугініна О.Є., може бути здійснено за допомогою: аналітичних підходів, заснованих на використанні аналітичних економіко-математичних методів і моделей; застосування статичних критеріїв за умови повної

невизначеності; здійснення евристичного підходу на основі експертного обговорення ризикових проблем; упровадження імітаційного моделювання; використання спеціальних математичних моделей за теорією оптимального управління; побудови економіко-математичних моделей за теоріями ігор і корисності [7].

Вишневська О.А. розрізняє наступні методи оцінки ризику:

1. Експертний метод – застосовується при відсутності потрібних статистичних даних або за швидкої зміни умов діяльності. Він передбачає орієнтацію на висновки залучених висококваліфікованих фахівців.

2. Розрахунково-аналітичний метод – ґрунтується на теоретичній моделі розвитку підприємства. Вимагає значних матеріальних витрат, а також широкого діапазону знань і кваліфікації розробників. Допустимий лише для великих підприємств, проте є найбільш достовірним і точним.

3. Статистичний метод – переважно використовується при стабільних обставинах, якщо потенційні втрати оцінюють за попередніми даними [8].

Для оцінки фінансових ризиків поширеною практикою є визначення відносних показників, тобто коефіцієнтів (оцінки фінансової стійкості, оцінки ліквідності та платоспроможності підприємства, оборотності активів, рентабельності підприємства). Також застосовують такі методи аналізу ризиків, як: SWOT-аналіз, PEST-аналіз, бенчмаркінг, факторний аналіз відхилень, аналіз точки беззбитковості, вартісний аналіз, прогнозування ймовірності банкрутства підприємства, АВС-аналіз, портфельний аналіз, галузевий аналіз.

Список літератури

1. Грубяк С.В. Підприємницькі ризики: поняття, сутність, види. Інфраструктура ринку. 2016. Вип. 2. С. 136-139.
2. Оксенюк К.І. Систематизація класифікаційних ознак підприємницького ризику. Молодий вчений. 2019. №8(2). С. 328-330.
3. Аранчій В.І., Ігнатенко М.М. Сутність ризиків підприємницької діяльності та їх оцінка з метою нівелювання й уникнення в управлінні ефективністю й конкурентоспроможністю розвитку. Економічний вісник університету. 2018. Вип. 39. С. 52-58.
4. Бурбело Н.О. Аналіз і класифікація ризиків підприємницької діяльності. Економіка. Менеджмент. Бізнес. 2015. №1. С. 160-166.
5. Євдокименко В.М., Дергалюк Б.В. Ризики підприємницької діяльності: розробка механізму управління. Науковий вісник Херсонського державного університету. Сер.: Економічні науки. 2014. Вип. 5(2). С. 74-77.
6. Бугай В.З., Мацюк О.В. Обґрунтування методичного підходу до аналізу ризиків підприємницької діяльності. Вісник Запорізького національного університету. Економічні науки. 2017. №2. С. 7-13.
7. Лугінін О.Є. Оцінка підприємницьких ризиків під час управління проектами за теорією ігор. Бізнес-навігатор. 2018. Вип. 5. С. 86-89.
8. Вишневська О.А. Фактори та методи оцінки підприємницького ризику в Україні. Інфраструктура ринку. 2016. Вип. 2. С. 122-125.

УДК 338.439

В. Кладченко, магістр гр. АДМ-18-1,4
Центральноукраїнський національний технічний університет

СТАН ТА ТЕНДЕНЦІЇ РОЗВИТКУ ХАРЧОВОЇ ПРОМИСЛОВОСТІ КІРОВОГРАДСЬКОЇ ОБЛАСТІ

Стаття присвячена дослідженню сучасного стану та тенденцій функціонування галузі харчової промисловості Кіровоградської області. Наведено засоби регулювання інноваційної діяльності підприємств харчової промисловості. Проведено аналіз обсягів виробництва за найбільш вагомими для регіону видами продукції: виробів ковбасних, олії соняшникової, борошна, хліба та виробів хлібобулочних. Визначено, що розвиток харчової промисловості Кіровоградської області упродовж останніх п'яти років мав переважно негативні тенденції, які полягають у значному зменшенні обсягів виробництва. Відзначено доцільність формування інноваційних кластерів за участі підприємств харчової промисловості.

харчова промисловість, регіон, регулювання, управління, розвиток

Харчова промисловість відіграє визначну структуро-формуючу функцію держави і являє собою одну з провідних та найбільш перспективних галузей країни. Подальший розвиток харчової промисловості є запорукою сталого розвитку національної економіки, тому необхідним є обґрунтування пріоритетних заходів її державного регулювання задля підвищення ефективності й конкурентоспроможності підприємств харчової промисловості [2]. Важливим аспектом є також врахування регіональних особливостей розвитку харчової промисловості.

До найважливіших засобів державного регулювання інноваційної діяльності в харчовій промисловості належать:

1. Нормативно-правові акти.
2. Обсяги і джерела інвестування інновацій в харчову промисловість.
3. Норми і нормативи.
4. Ціноутворення в харчовій промисловості.
5. Ставки податків і пільги з оподаткування.
6. Відсотки за кредит і державні гарантії.
7. Державні замовлення і закупівлі.
8. Стандартизація та сертифікація.
9. Ліцензії і квоти.
10. Підтримка інфраструктурних утворень [4].

Проаналізуємо стан харчової промисловості за даними Головного управління статистики у Кіровоградській області. Індекси виробництва продукції промисловості представлені в табл.1.

Як бачимо, хоча індекси продукції промисловості в цілому у регіоні демонструють незначну тенденцію до зростання, у галузі харчової промисловості, навпаки, відбулося зниження у 2018 році – до 95,9% по відношенню до 2017 року. Індекси виробництва харчових продуктів, напоїв та тютюнових виробів були позитивними у 2016 році (125,5%) та 2017 році (112,1%). Найбільш суттєве зниження впродовж п'яти останніх років мало місце у 2015 році – 65,2%.

Проаналізуємо більш детально обсяги виробництва за найбільш вагомими для регіону видами продукції. На рис. 1 відображено динаміку обсягів виробництва виробів ковбасних.

Таблиця 1 – Індекси промислової продукції Кіровоградської області за 2014-2018 роки, % до попереднього року

Показник	2014	2015	2016	2017	2018	2018/ 2014
Промисловість	100,8	82,9	120,3	105,5	102,2	+1,4
Переробнапромисловість	107,5	78,4	122,7	104,1	97,4	-10,1

Виробництвохарчовихпродуктів, напоїв та тютюновихвиробів	115,8	65,2	125,5	112,1	95,9	-19,9

Джерело: складено за даними Головного управління статистики у Кіровоградській області [1]

Дана динаміка свідчить, що починаючи з 2015 року, виробництво даного виду продукції харчової промисловості мало тенденцію до зменшення. Так, якщо у 2014 році було виготовлено 20,4 тис. тон виробів ковбасних, то у 2018 році – лише 14,8 тис. тон.

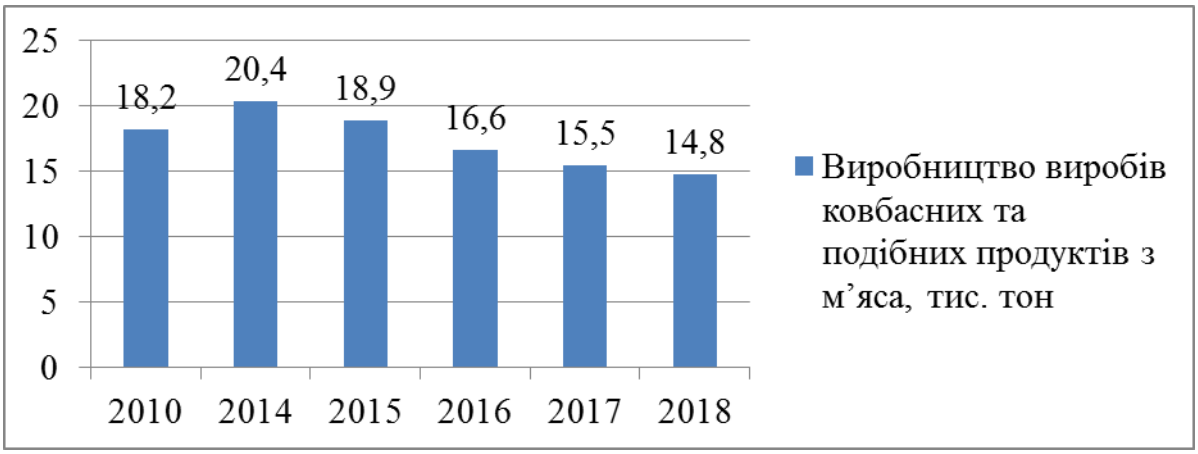


Рисунок 1 – Динаміка виробництва виробів ковбасних у Кіровоградській області за 2010-2018 року

Джерело: складено за даними Головного управління статистики у Кіровоградській області [1]

На рис. 2 відображено динаміку обсягів виробництва олії соняшникової. Максимальний обсяг виробництва олії соняшникової у Кіровоградській області мав місце у 2017 році – 825,9 тис. тон, мінімальний – у 2015 році (446,6 тис. тон). У 2018 році відбулося зниження порівняно з 2017 роком і обсяг виробництва олії складав 746,6 тис. тон.

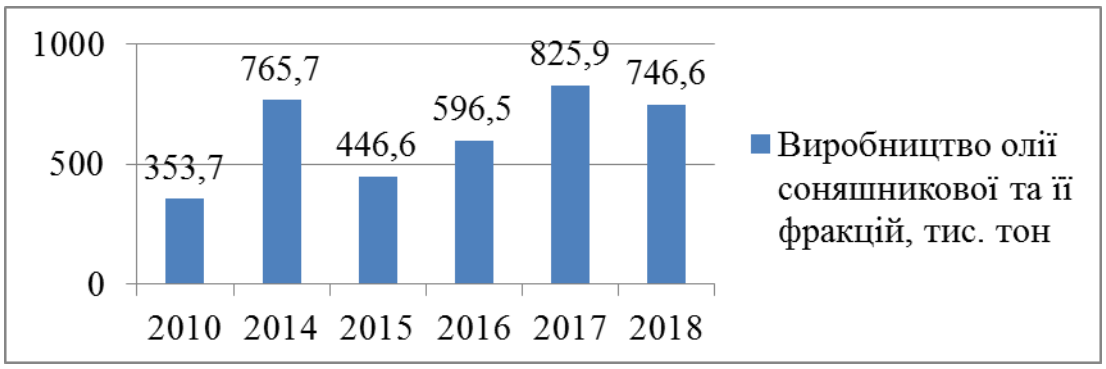


Рисунок 2 – Динаміка виробництва олії соняшникової у Кіровоградській області за 2010-2018 року

Джерело: складено за даними Головного управління статистики у Кіровоградській області [1]

Щодо обсягів виробництва борошна (рис. 3), то тут показники також мають значну тенденцію до зниження, починаючи з 2015 року. Мінімальний обсяг виробництва мав місце у 2017 році – лише 29,8 тис. тон. У 2018 році спостерігаємо певне зростання – до 37,7 тис. тон.

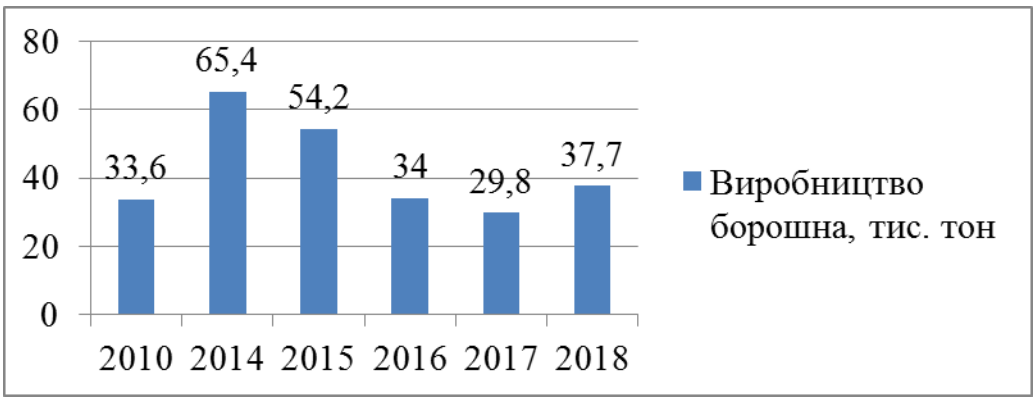


Рисунок 3 – Динаміка виробництва борошна у Кіровоградській області за 2010-2018 року

Джерело: складено за даними Головного управління статистики у Кіровоградській області [1]

Стосовно обсягів виробництва хліба та виробів хлібобулочних (рис. 4) можна відзначити також стійку негативну динаміку: якщо в 2014 році було виготовлено 20,7 тис. тон даного виду продукції, то в 2015 році – 14,2 тис. тон, в 2016 році – 12,6 тис. тон, в 2017 році – 11,3 тис. тон та в 2018 році – 10,9 тис. тон.

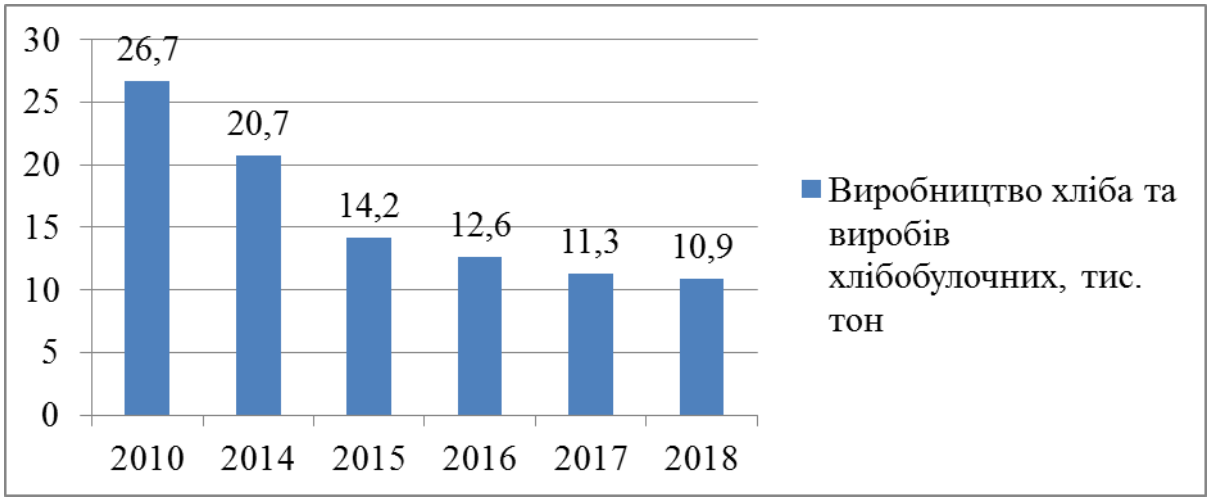


Рисунок 4 – Динаміка виробництва хліба та виробів хлібобулочних у Кіровоградській області за 2010-2018 року

Джерело: складено за даними Головного управління статистики у Кіровоградській області [1]

Отже, розвиток харчової промисловості Кіровоградської області упродовж останніх п’яти років мав переважно негативні тенденції, які полягають у значному зменшенні обсягів виробництва.

Тому необхідним є обґрунтування стратегічних перспектив розвитку харчової промисловості регіону, визначення шляхів реструктуризації регіонального управління харчовою промисловістю, формування інноваційних кластерів за участі підприємств харчової промисловості.

За оцінками фахівців, головна мета створення сучасних інтеграційних систем полягає не тільки у встановленні прямих зв’язків між учасниками, скороченні витрат та збільшенні прибутку, а й у подоланні диспаритету цін, забезпечення пропорційного розподілу доходів між секторами агропродовольчих ринків, відтворювального рівня цін у базових їх секторах, зокрема, сировинному [3].

Важливе значення в контексті підвищення ефективності функціонування підприємств харчової промисловості регіону має забезпечення зростання інвестиційної привабливості галузі для вітчизняних та зарубіжних інвесторів, створення інноваційної інфраструктури та стимулювання інноваційної діяльності в регіоні.

Список літератури

1. Головне управління статистики у Кіровоградській області: офіційний сайт. URL: http://www.kr.ukrstat.gov.ua/ (дата звернення: 13.10.2019).
2. Хрип'юк В.І. Еволюціонування державного регулювання харчової промисловості. Формування ринкових відносин в Україні. 2018. №1. С. 31-40.
3. Павлов О.І., Лисюк В.М., Деркач Т.В. Державне регулювання інтеграційних процесів на стратегічних агропродовольчих ринках. Економіка харчової промисловості. 2015. Випуск 3. Том 7. С. 32-40.
4. Водянка Л.Д. Державне регулювання інноваційної діяльності підприємств харчових галузей України. Агросвіт. 2010. №11. С. 22-26.

УДК 021.1:004.9

О. Коломієць, магістр гр. ІС-18М
Центральноукраїнський національний технічний університет

ВИКОРИСТАННЯ ЕЛЕКТРОННО-ІНФОРМАЦІЙНИХ РЕСУРСІВ У ПРОФЕСІЙНІЙ ПІДГОТОВЦІ МАЙБУТНІХ ФАХІВЦІВ

У статті досліджено особливості функціонування електронних комунікацій в закладах вищої освіти, проаналізовано сучасні напрямки використання електронно-інформаційних ресурсів у професійній підготовки майбутніх фахівців

електронно-інформаційні ресурси, інформаційно-документаційне забезпечення, електронні комунікації, електронні бібліотеки

Актуальність статті. Актуальність проблеми використання електронно-інформаційних ресурсів в закладах вищої освіти обумовлюється необхідністю застосування сучасних високотехнологічних і прогресивних підходів до організації системи інформаційно-документаційного забезпечення професійної підготовки майбутнього фахівця, духовного розвитку особистості в умовах інформатизації суспільства. Адже традиційна модель освітнього процесу супроводжується значним масивом документації, опрацювання якої часто призводить до нераціональних витрат часу, порушень послідовності та мобільності інформаційних процесів між структурними підрозділами освітнього закладу, негативно відображається на ефективності управління освітнім процесом в цілому. Обсяги технічної роботи з документами іноді заміняють основний зміст діяльності установи.

Мета статті. Проаналізувати особливості функціонування електронних комунікацій в закладах вищої освіти, визначити сучасні напрямки використання електронно-інформаційних ресурсів для забезпечення професійної підготовки майбутніх фахівців.

Ефективність документообігу і контроль за опрацюванням інформації має ключове значення в системі управління закладом вищої освіти (далі ЗВО), організації діяльності його підрозділів з метою ефективного здійснення професійної підготовки майбутніх фахівців, надання високоякісних освітніх послуг.

Основні вимоги до сучасної системи інформаційно-документаційного забезпечення діяльності освітніх закладів можна визначити таким чином: по-перше, система документації має бути максимально повною і детальною, що дасть можливість комплексно відображати інформацію щодо навчального процесу у ЗВО; по-друге – йдеться про створення єдиної моделі документів для груп однорідних завдань з використанням певного зразка; нарешті – обробку інформації слід здійснювати за допомогою технічних засобів.

Використання електронних комунікацій в інформаційно-документаційному забезпеченні управління ЗВО має створити умови для переходу від аналізу потреб закладу вищої освіти у документальній інформації до надання вільного вибору необхідних даних з інформаційного масиву і забезпечення оперативного доступу до них. Розв'язання цієї проблеми можливо на основі інтеграції нових інформаційних технологій, накопиченого арсеналу досягнень документознавства і документообігу з організаційними структурами діловодних служб ЗВО.

Нині більшість закладів вищої освіти України складають зведену й аналітичну звітності в MS Excel, MS Word, стикаючись при цьому із проблемами уніфікації документів. Тому для ЗВО актуальним є завдання автоматизації документообігу. Беззаперечним позитивом є успішне функціонування автоматизованих систем роботи з документами, таких як «Атлас Док», «АСКОД», «ДОК ПРОФ 2.0», «ФОС-СДок», «Megapolis. Документообіг», Docs Vision, Doc Flow та ін.. Вони дають можливість в автоматизованому режимі формувати детальне навчальне навантаження, робочі й навчальні плани, розклади занять тощо. Запровадження системи електронного документообігу у ЗВО має багато переваг, адже: підвищує ефективність управління інформаційно-документаційними процесами; дозволяє оптимізувати інформаційно-комунікаційне середовище ЗВО; допомагає систематизувати процеси діловодства та документообігу у ЗВО, робить більш об'єктивним процес оцінювання навчальної діяльності студентів; формує електронну базу даних документаційного масиву ЗВО; захищає документацію від несанкціонованого доступу.

Система електронного діловодства та документообігу ЗВО функціонує у мереживому режимі і має бути доступною усім структурним підрозділам для ефективності документаційного забезпечення установи. Вона має бути доступною викладачам, студентам та співробітникам освітнього закладу, що забезпечують освітній процес в межах їх повноважень. Ця система має бути незмінною протягом одного навчального року, мати зручний розповсюджений формат для відтворення електронними засобами та на паперовому носії. Саме тому впровадження електронних форм у ЗВО є необхідною умовою якісного інформаційно-документаційного забезпечення організації освітнього процесу.

Важливою ланкою базової автоматизованої системи документобігу ЗВО є т.зване колективне (за участю всіх підрозділів установи) та індивідуальне (на рівні ректорату) діловодство. Такий підхід передбачає:

- підготовку документів на основі стандартних, якщо такі є, або затверджених на рівні керівництва установи бланків;
- документування інформації про роботу підрозділів шляхом внесення в базу даних усіх протокольно створених версій документів;
- облік використання бланків, ідентифікацію створюваних і друкованих документів установи;
- механізм гарантованої ідентичної відповідності між паперовим документом і його електронною копією, яка направляється до бази даних установи.

Для забезпечення умов якісної освітньої діяльності особливе значення має достатньо сформоване інформаційно-комукаційне середовище ЗВО. Це – умови, які забезпечують діяльність користувачів з інформаційними ресурсами, реалізують інформаційні процеси, використовуючи при цьому інтерактивні засоби інформаційно-комунікаційних технологій. Нині у ЗВО формується інформаційне освітнє середовище, яке включає систему апаратних засобів, програмне забезпечення, фахівців і користувачів, бази даних тощо. Компонентами інформаційного освітнього середовища є: сайти, медіатеки, віртуальні інформаційні дошки, електронні навчальні програми, методичні розробки, ресурси Інтернету та підсистеми, які забезпечують реалізацію функцій документообігу, моніторингу й управління освітою [3].

Системне експериментування, апробація та застосування інновацій в освітньому процесі ЗВО, які символізують зміни технології навчання, також вимагають належного технічного забезпечення та контролю за їх ефективністю. Вони мають бути керованими, що неможливо здійснити без відповідного документаційного забезпечення. Тому, на нашу думку, розроблення дистанційних курсів в електронній системі MOODLE сприятиме формуванню професійних

компетентностей, передбачених стандартами освіти, проведенню діагностики, налагодженню контролю знань студентів. Система MOODLE є складовою інформаційно-освітнього середовища ЗВО, відповідає міжнародним стандартам електронного навчання. Вона орієнтована, насамперед, на підтримку інтерактивної взаємодії між учасниками освітнього процесу.

Враховуючи сучасні наукові досягнення у галузі документознавства, електронних комунікацій, можна стверджувати, що ефективне функціонування інформаційно-документаційної системи закладу вищої освіти залежить від багатьох чинників. Йдеться, насамперед, про такі чинники:

- запровадження системи електронного документообігу в усіх підрозділах ЗВО;
- ведення єдиної системи реєстрації руху документів, створення електронного обміну реєстраційними даними про документ між усіма підрозділами ЗВО;
- упровадження наскрізної системи контролю виконання документів на всіх структурних рівнях, створення можливостей оперативного доступу виконавців до бази контролю виконання у межах їх компетентностей,;
- створення єдиної бази даних нормативних документів ЗВО, системи протокольних документаційних фондів;
- використання системи електронного документообігу для обміну нормативною документацією між ЗВО тощо.

Таким чином, інформаційно-документаційне забезпечення діяльності ЗВО – це важлива ланка освітньо-комунікаційного простору в сучасних умовах розвитку вищої освіти, необхідна для забезпечення її якості. Запровадження системи електронного документообігу у ЗВО упорядковує та систематизує роботу з документаційними потоками; вирішує проблеми забезпечення повноти аналітичних даних, дублювання інформації; спрощує пошук необхідних документів, оптимізує їхнє використання і зберігання.

Питання оптимізації використання електронно-інформаційних ресурсів в стосується також роботи бібліотек закладів вищої освіти. Адже вони відіграють важливу роль у здійсненні професійної підготовки майбутніх фахівців, забезпечуючи повною мірою реалізацію зв'язку інформаційної теорії з практикою.

Невід'ємною складовою бібліотечної справи нині стають цифрові колекції, що зумовлено зростанням обсягу інформації в електронному вигляді та поширенням мереживих матеріалів у системі документальних комунікацій суспільства. Процеси архівування, створення електронних депозитаріїв в установах, розвиток глобальних відкритих архівів наукових статей призводить до зміни ролі бібліотечної справи в процесі оприлюднення наукової інформації [1,с.44]. На відміну від системи засобів масової інформації та освіти бібліотеки є інституціями сучасного суспільного процесу, що надають вільний доступ до надбань культури та знань у їх розмаїтті.

Основним вектором розвитку процесів автоматизації в бібліотеці, на думку фахівців, є формування інформаційного простору, який би дозволив здійснювати широкий доступ до даних і провадити якісне та оперативне бібліографічно-інформаційне обслуговування [2,]. Це передбачає розкриття змісту наявних ресурсів через створення бібліографічних баз даних, каталогів та картотек, за рахунок яких значно скорочується для користувачів шлях до знань. Новітні технології спрощують доступ до ресурсів бібліотеки через мережу Інтернет.

Популярними стають такі види електронних ресурсів бібліотечних установ: текстові аналоги друкованих видань; нові форми публікацій, що не мають друкованих аналогів (електронні оголошення, матеріали веб-конференцій та ін..); аудіо- та відеоінформація; мультимедійні продукти, що характеризуються постійним оновленням тощо. Очевидно, що такі ресурси вимагають й відповідного бібліотечного опрацювання, адже відрізняються від інших об'єктів каталогізації, наприклад, документів на паперових носіях, що традиційно опрацьовують у технологічних підрозділах бібліотечних установ.

Новими характеристиками, що зумовлюють особливості каталогізації електронних ресурсів та формування їх бібліографічного опису, стають: типи носіїв, режими доступу, системні вимоги, динаміка інформаційного вмісту, а також специфіка взаємодії з користувачем.

Одним із основних видів електронно-інформаційних ресурсів, що активно використовують в освітній діяльності, є електронні бібліотеки. Електронні бібліотеки – це інформаційні системи, які забезпечують формування, зберігання та ефективне використання різноманітних колекцій цифрових ресурсів і надають доступ до них через мережу Інтернет. Застосовують також дані електронно-інформаційних ресурсів, які становлять систематизовану сукупність інформаційних ресурсів, об'єднаних спільним змістом, джерелами, призначенням, авторством, способами доступу тощо. Крім цифрових матеріалів, об'єктами опрацювання є бази даних, мапи, карти користувача, посилання тощо.

За функціональною спрямованістю розрізняють електронні бібліотеки загального характеру та спеціалізовані. Перші зберігають ресурси за багатьма напрямами знань, спеціалізовані – нагромаджують і надають доступ до матеріалів певної предметної галузі. Таким чином, електронні бібліотеки забезпечують якісно новий рівень задоволення фахових потреб користувачів завдяки використанню сучасних бібліотечно-інформаційних технологій.

Впровадження електронних бібліотек на теренах України розпочалось в 1998 р. Першою на цей шлях стала Національна бібліотека України імені В. І. Вернадського, а з 2000 р. – бібліотеки закладів вищої освіти та науково-дослідних установ.

Для оптимізації роботи з електронно-інформаційними ресурсами бібліотечні установи взяли курс не лише на використання можливостей глобальних мереж, а й на створення власних інформаційних ресурсів. На базі масивів бібліографічної, реферативної, аналітичної інформації формуються електронні каталоги і картотеки, бібліографічні покажчики та реферативні видання, оцифровується наукова і методична література. У практику бібліотек входить тиражування на компакт-дисках окремих інформаційних продуктів та електронних ресурсів. А власне оптимізація електронно-інформаційних ресурсів відбувається через упорядкування, структурування і продуктивну організацію функціонування в інформаційних системах, зокрема в електронних бібліотеках.

Отже, перехід від традиційного до електронного документообігу в системі інформаційно-документаційного забезпечення діяльності ЗВО має посилити вплив інформаційних процесів на різноманітні аспекти життєдіяльності закладу вищої освіти та підвищити його конкурентоспроможність, створити умови наскрізного автоматизованого контролю на всіх етапах роботи з документами, що кардинально поліпшить якість роботи виконавців, зробить терміни підготовки документів більш прогнозованими і керованими, дозволить виконувати завдання, які складно або неможливо виконати традиційними методами.

Тому створення ефективної системи інформаційно-документаційного забезпечення діяльності ЗВО має стати провідним напрямом цілеспрямованого формування інформаційних ресурсів, реалізації управлінської діяльності щодо підвищення ефективності надання високоякісних освітніх послуг.

Список літератури

1. Галаган Л. Онлайнові ресурси президентських бібліотек світу. Наукові праці Національної бібліотеки України імені ВУ. І. Вернадського. 2010. Вип. 27. С. 44-52.
2. Майстрович Т. В. Электронный документ в библиотеке: научно-методическое пособие. Москва: Либерия – Бибинформ, 2007. № 4. 144 с.
3. Мокра М. Інформаційно-освітнє середовище в освітні системі США [Електронний ресурс]. Режим доступу: http://ena.lp.edu.ua/bitstream/ntb/23849/1/28-213-222

УДК 314.1

А. Косташ, магістр гр. МЕВ-16
Центральноукраїнський національний технічний університет

ТЕОРЕТИЧНІ АСПЕКТИ ДОСЛІДЖЕННЯ ТРУДОВОЇ МІГРАЦІЇ

Всесторонньо досліджено теоретичні аспекти трудової міграції, розкрито сутність міжнародної міграції, особливості формування міграційних процесів, виявлено, що сьогодні міжнародна трудова міграція охопила всі континенти та набула глобального характеру. Проаналізовано основні мотиви активізації міграційних процесів в Україні.
трудова міграція, міжнародна трудова міграція, міграційні процеси

В процесі становлення та еволюції міжнародного руху капіталу, міжнародної торгівлі виникає міжнародна міграція робочої сили, яка є формою руху відносно зайвого населення з одного центру накопичення капіталу до іншого. Пропозиція робочої сили надходить переважно із країн з низьким рівнем економічного розвитку і низьким рівнем зайнятості населення, тому міжнародна міграція робочої сили виконує роль регулятора економічних умов світового господарства.

Термін «міграція» походить від латинського miqratio, miqro – переселяюсь, що у загальному розумінні означає переміщення, переселення. Міграція населення - переміщення людей, пов'язане, як правило, із зміною місця проживання.

Поняття «міжнародна міграція» було започатковано у 1922 році під час Міжнародної конференції з праці Міжнародної організації праці (МОП). За визначенням МОП, мігрант – це особа, яка переміщується з однієї держави до іншої і має потребу у міжнародних міграційних послугах, що надаються міжнародними організаціями [2].

Міжнародна міграція населення, на відмінну від внутрішньої міграції, полягає у перетині державного кордону, державному контролі за фактом перетину кордону (у країні виїзду і особливо у країні в'їзду), майбутньому перебуванні в країні в'їзду, зокрема, коли це пов'язано із працевлаштуванням, навчанням або стажуванням [3].

Міграційні процеси формуються під впливом багатьох чинників, серед них виділяють соціально – економічні, політичні, правові, соціально – психологічні, екологічні, культурні. Проте, одним з головних факторів, що змушує людей приймати рішення про еміграцію є різниця у реальних доходах за однакову роботу в різних країнах.

Трудова міграція має такі особливості: власник робочої сили має юридичне право розпоряджатися власною робочою силою; існування попиту на додаткову робочу силу в країні – реципієнті; переважання впливу сукупності чинників міграції над бажанням залишитися в країні проживання.

Трудова міграція з позицій працівника є можливістю отримання пристойного місця роботи з метою підвищення життєвого рівня, за рахунок більш вигідного продажу робочої сили на ринку праці, що не належить до території постійного місця проживання мігранта.

Трудова міграція для роботодавця – можливість тимчасово використати додаткову якісну робочу силу потрібної кваліфікації, з меншими витратами на її купівлю, у порівнянні з національною робочою силою.

Сьогодні міжнародна трудова міграція охопила всі континенти та набула глобального характеру. За даними експертів, нині у світі понад 3 % населення світу мешкають за межами країни свого походження [7].

За розрахунками Світового банку, міграція забезпечує більші переваги для глобальної економіки, ніж міжнародна торгівля. На основі теоретичної моделі рівноваги світової економіки було зроблено висновок, що збільшення чисельності мігрантів у 2025 р. порівняно

з 2000 р. на 8 % забезпечить зростання глобального доходу на 0,6 %, у т. ч. для розвинених країн – на 0,4 %, а для тих, що розвиваються, – на 1,8 %. Тобто міграція не лише динамізує розвиток, а і сприяє більш справедливому розподілу глобального багатства [5, с. 53].

У 2019 році кількість міжнародних мігрантів у світі досягла орієнтовної позначки у 272 млн. осіб, що на 51 млн. осіб більше рівня 2010 року. Про це йдеться у доповіді ООН, яка була презентована 17 вересня 2019 р. у штаб-квартирі Укрінформу. За даними ООН, мігранти нині становлять 3,5% населення світу (для порівняння, у 2000 році - 2,8%). В ООН не дають оцінок наведеним цифрам, але відзначають, що при впорядкованій, безпечній, прогнозованій міграції та мобільності людей, таке переміщення може мати позитивні результати, зокрема, сприяти економічному розвитку й досягненню цілей сталого розвитку [8].

Європа утримує лідерство як пункт прагнень мігрантів (82 млн. осіб), за нею йдуть США (59 млн.) і Західна Азія (49 млн.). Зазначимо, що майже половина всіх мігрантів на планеті мешкають в десяти країнах світу: у США - 59 млн. осіб, по 13 млн. - у Німеччині й Саудівській Аравії, 12 млн. - у Росії, 10 млн. - у Великій Британії, 9 млн. - в ОАЕ, по 8 млн. - у Франції, Канаді й Австралії, 6 млн. - в Італії. Третина всіх міжнародних мігрантів походить теж лише з 10 країн.

Чисельність мігрантів з Індії за кордоном складає 18 млн. осіб, а з Мексики – другу за розміром діаспору -12 млн. Вихідці з Китаю – 11 млн., Російської Федерації – 10 млн., Сирії – 8 млн. осіб [6].

У світі продовжує зростати вимушене переселення населення унаслідок військових подій та інших кризових обставин. У 2010-2018 рр. кількість біженців і шукачів притулку зросла на 13 мільйонів, що становить чверть додаткових мігрантів за цей період. Північна Африка та Західна Азія прийняли близько 46 % біженців. Статистика свідчить, що кожен сьомий мігрант у світі молодший від 20 років, а троє з чотирьох – особи працездатного віку (20-64 років) [6].

На перебіг міграційних процесів в Україні впливає її місце у міжнародних рейтингах. Дослідження показують, що за шість місяців 2019 року у рейтингу миролюбних країн (Index The Global Peace Index) Україна піднялась з 152 на 150 місце; за рейтингом економічної свободи (Index of Economic Freedom) займає 147 місце серед 158 країн; у рейтингу легкості ведення бізнесу (Doing business) Україна посіла 71 місце; у глобальному рейтингу конкурентоспроможності (The Global Competitiveness Index), серед 63 країн світу - 54 місце [8].

Ще одним важливим фактором, що впливає на міграційні процеси в Україні є рівень оплати праці, у 2019 р. мінімальна заробітна плата в нашій країні становила 4173 грн., приблизно 122 євро. За даними статистичної служби Євросоюзу, мінімальна заробітна плата за місяць [1], у Латвії складає 430 євро, в Литві – 555 євро, в Естонії – 540 євро, у Румунії – 446,02 євро, у Словенії – 941 євро, у Греції – 783,33 євро. У Польщі мінімальна заробітна плата становить 523,09 євро, у Чехії – 518,97 євро, у Болгарії - 286,33євро. Найвищий її рівень серед країн Європейського Союзу у Люксембурзі - 2071євро, у Німеччині – 1557 євро, у Австрії – 1500 євро, у Великій Британії – 1524,52 євро на місяць. За такого рівня диференціації оплати праці та перспектив працевлаштування, з урахуванням економічних і соціальних факторів, міграційні процеси посилюються.

Для сучасної міграції характерним є явище, що дістало назву «міграційного переходу», тобто перетворення країн – постачальників мігрантів на реципієнтів. Ознаки міграційного переходу спостерігаються нині у Східній Європі, наприклад у Польщі. Країна, що внаслідок тривалої еміграції має одну з найчисельніших зарубіжних діаспор, є зараз країною призначення для сотень тисяч іноземних працівників, передусім з України [4].

Щодо України, основними мотивами активізації міграційних процесів в країні стало виникнення кордонів між державами, що утворилися на території колишнього СРСР та пов’язаних з ними митних кордонів. Це спричинило різке зниження господарських, економічних, інформаційних, культурних та інших відносин і наштовхнуло багатьох людей,

у минулому громадян єдиної держави, до бажання возз'єднатися із родинами на своїй етнічній чи історичній батьківщині.

Серед економічних чинників посилення міграції робочої сили в Україні, слід відзначити нерівномірність економічних реформ, що призвели до різкого падіння рівня життя більшої частини населення країни. Розлад міжгосподарських зв'язків, згортання виробництва на великих підприємствах, спричинили масове вивільнення працівників, відповідно погіршення їх соціально-економічного становища, посилило міжнародну міграцію. Починаючи із 1993 року, з України збільшився потік від'їжджаючих трудових мігрантів.

Вироблення сучасних підходів до регулювання міграційних процесів, стало необхідним внаслідок військового конфлікту на Сході України, викликаних ним масових внутрішніх переміщень у країні, із зовнішніх - набуття чинності Угоди про асоціацію з Європейським Союзом, переорієнтації вектору міграції українців у західному напрямі, значного посилення міграційного тиску на Європу тощо.

Свобода пересування, одне із основоположних прав людини, відкрила для українців нові можливості, однак створила й нові ризики. Вони особливо загострилися останніми роками на тлі іноземної агресії, економічних труднощів та соціально-політичної нестабільності і полягають у: значній інтенсифікації виїзду українців за кордон, передусім з метою працевлаштування; збільшенні серед емігрантів частки молоді, фахівців; прискоренні трансформації частини тимчасової заробітчанської міграції на еміграцію для постійного проживання.

Внаслідок несприятливої економічної ситуації та війни, Україна є непривабливою для іммігрантів з-за кордону, в умовах значного посилення контролю на зовнішньому кордоні ЄС на Середземномор'ї. Не можна не зважати також, на можливість збільшення транзитного, частково нелегального потоку через територію України на Захід.

Низькі доходи, бідність українського населення залишаються одним з головних чинників високої орієнтації роботи за кордоном, особливо привабливими в цьому плані для українців є країни - члени Європейського Союзу.

Список літератури

1. Eurostat : website. URL: http://ec.europa.eu/eurostat/web/main/home (Last accessed: 27.10.2019).
2. Лібанова Е.М. Зовнішня трудова міграція Українців: масштаби, причини, наслідки. Демографія та соціальна політика. 2018. №2(33). – С.11-26.
3. Літковець Ю.О. Зовнішня трудова міграція та її наслідки для української економіка. Економіка та управління національним господарством. 2019. Випуск 31. С.131- 136.
4. Малиновська О.А. Міграційна політика: глобальний контекст та українські реалії: монографія. Київ: НІСД, 2018. 472 с.
5. Международная миграция и развитие. Доклад эксперта. URL: http://docplayer.ru/27688231-Mimun-2016-mezhdunarodnaya-migraciya-i-razvitie-generalnaya-assambleya-dokladeksperta.html (дата звернення: 24.11.2019).
6. Міжнародна організація з міграції : веб-сайт. URL: http: //iom.org.ua / ua (дата звернення: 26.10.2019).
7. Миценко І.М., Стежко Н.В. Міжнародна економіка: навч. посіб. Кіровоград: КНТУ, Поліграф-Сервіс, 2013. 640 с.
8. Кількість мігрантів у світі перевищила 270 мільйонів. Укрінформ. 2019. URL: http://www.ukrinform.ua/rubric-world/2782330-kilkist-migrantiv-u-sviti-perevisila-270-miljoniv.html (дата звернення: 29.10.2019).

УДК 657

А. Кравченко, магістр гр. ООУ-18МЗ
Центральноукраїнський національний технічний університет

СТАН ТА ПЕРСПЕКТИВИ РОЗВИТКУ ОБЛІКУ І ОПОДАТКУВАННЯ МАЛИХ ПІДПРИЄМСТВ

У статті досліджено проблеми розвитку системи обліку і оподаткування діяльності малих підприємств в Україні.
малі підприємства, організаційні і методичні аспекти, облікова політика, база оподаткування, єдиний податок, європейські Директиви, МСФЗ

Постановка проблеми та її актуальність. У загальній чисельності суб'єктів підприємницької діяльності левова частка належить малим підприємствам. Так, на 2018 рік до 95 % підприємств України були малими. За статистичною інформацією на 2018 рік більше 80% малих підприємств України здійснювали діяльність у сфері оптової та роздрібної торгівлі, натомість у Кіровоградському регіоні найбільше малих підприємств функціонують в галузі сільського господарства.

На створення та розвиток малих підприємств вплинула державна політика підтримки малого підприємства, зокрема запровадження спрощених систем обліку й оподаткування. В Україні триває процес реформ облікових систем, запровадження гармонізації та стандартизації з обліку. Гармонізація передбачає нівелювання аналогічних стандартах країн членів співтовариства. Країни ЄС гармонізують системи обліку через формування та дотримання нормативних документів - директив ЄС, що безпосередньо стосується і малих підприємств. В 2019 році введено зміни до нормативної регламентації обліку та формування звітності малих підприємств.

Аналіз останніх досліджень і публікацій. Теоретичні та практичні аспекти малого підприємництва, зокрема діяльності малих підприємств, розглянуті в працях багатьох вітчизняних вчених-економістів: О. Ареф'євої, М. Білик, І. Бланка, Л. Буряка, Б. Валуєва, З. Варналія, Н. Герасимчук, О. Данілова, М. Дем'яненка, І. Запатріної, О. Орлова, П. Саблука, А. Поддєрьогіна, В. Сизоненка, А. Соколовської, В. Федосова, І. Чугунова та інших.

Проблематика обліку і формування фінансової звітності з врахуванням особливостей облікової політики малих підприємств розглядається у працях Г.А. Велша, О.В. Карпенко, В.В. Ковалева, В.М. Костюченко, М.В. Кужельного, В.О. Меца, Є.В. Мниха, Л.В. Нападовської, В.М. Пархоменка, М.С. Пушкаря, В.В. Сопка та ін.

Незважаючи на значний доробок і достатньо глибокий рівень відпрацювання потребує подальших досліджень проблематика обліку та оподаткування діяльності малих підприємств в контексті змін ринкового середовища нормативно – правової бази.

Метою статті є з'ясування проблем та перспектив розвитку обліку і оподаткування малих підприємств України та обґрунтування напрямів удосконалення оптимізації обліку та оподаткування результатів їх діяльності.

Виклад основного матеріалу. Аналіз галузевої структури малого підприємництва міста Кропивницький свідчить, що більш привабливою для розвитку бізнесу залишається невиробнича сфера, а саме оптова та роздрібна торгівля. Також представниками малого бізнесу обслуговується велика частина сфери споживчого ринку. Крім того, діяльність суб'єктів малого підприємництва зосереджується у сфері операцій з нерухомим майном, надання послуг, пошиття одягу, будівництва, ремонту житла, виробництва харчових продуктів, виготовлення вікон, виробів з деревини та металу.

Останнім часом спостерігається тенденція до зменшення кількості середніх підприємств та збільшення кількості малих підприємств м. Кропивницький. Так, у порівнянні з 2016 роком, кількісний показник малих підприємств у 2017 р збільшився на 548 одиниць. Більшу частку всіх підприємств міста склали малі підприємства 7406 одиниць

На створення та розвиток малих підприємств вплинула державна політика підтримки малого підприємства, зокрема запровадження спрощених систем обліку й оподаткування. В Україні тривалий процес реформ облікових систем, запровадження гармонізації та стандартизації з обліку. Гармонізація передбачає нівелювання у аналогічних стандартах країн членів співтовариства. Країни ЄС гармонізують системи обліку через формування та дотримання нормативних документів - директив ЄС.

У світовій практиці міжнародні стандарти фінансової звітності не отримали широкого поширення серед малих підприємств. Стандарти для малого і середнього бізнесу прості і інтуїтивно зрозумілі. В них відсутні правила обліку тих операцій, з якими малий і середній бізнес не зустрічається. Враховуючи, що малими і середніми можна назвати 95% всіх компаній в світі, стандарти для малого і середнього бізнесу отримають широке поширення в найближчому майбутньому.

Перспективним напрямком реформування системи бухгалтерського обліку є встановлення порядку ведення бухгалтерського обліку та складання фінансової звітності за єдиними правилами для всіх суб'єктів, а виключенням можуть бути підприємства, які за масштабами господарської діяльності або публічністю діяльності матимуть право на спрощений порядок.

У межах загального принципу застосування спрощених підходів ведення обліку малими підприємствами розроблено стандарт для малого та середнього бізнесу. П(С)БО 25 [3] має відмінність від МСФЗ для малих та середніх підприємств та неповною мірою відповідає директивам ЄС за цим напрямом. Після впровадження П(С)БО 25 у фахових колах сформувалось негативне ставлення до можливості реалізації малими підприємствами уніграфічної парадигми і формування фінансової звітності без ведення обліку на засадах подвійного запису (форма звітності МС). Ми вважаємо, що серед малих підприємств є такі, для яких такий підхід є обґрунтованим, проте потребують уточнення критерій надання права застосування такого підходу. На нашу думку даний підхід є прийнятним для сільського господарських підприємств, що є мікропідприємством та не використовує найману працю.

Аналіз облікової практики обстежених малих підприємств свідчить про невиваженість облікової політики та низький рівень інформаційного забезпечення управління. Так, у 90% обстежених малих підприємств накази про облікову політику відсутні, не формалізовано рішення щодо застосування спрощеного плану рахунків. Рішення щодо застосування спрощеної системи оподаткування не ґрунтується на відповідних аналітичних процедурах. Більшість респондентів визнають аргументом щодо вибору спрощеної системи оподаткування, відсутність необхідності при веденні бухгалтерського обліку дотримання норм облікових стандартів та уникнення відповідальності за їх порушення при здійсненні фіскальних перевірок. За цих умов спрощений характер формування звітності відіграє позитивну роль, але нівелюється функція обліку як інформаційного забезпечення управління на всіх його рівнях.

Огляд літературних джерел щодо сутності та значення малих підприємств для країн з ринковою економікою дає підстави стверджувати, що автори вбачають у даному секторі перспективну й значущу силу, розвиток якої сприятиме покращенню соціально-економічного стану в країні. Незважаючи на широке обговорення проблем малого підприємництва, існують розбіжності в поглядах науковців щодо класифікаційних ознак, а термінологія з даного питання залишається остаточно не визначеною на законодавчому рівні.

Дискусійним є питання застосування малими підприємствами України МСФЗ. Ми приєднуємось до погляду Іллі Тарана, який вважає що ті підприємства, які хочуть застосовувати МСФЗ для малих та середніх підприємств добровільно замість П(С)БО,

можуть зробити це в будь-який момент відповідно до чинного Закону про бухгалтерський облік [4].

На створення та розвиток малих підприємств вплинула державна політика підтримки малого підприємства, зокрема запровадження спрощених систем обліку й оподаткування.

У межах реформування політичної системи в Україні спостерігається тенденція посилення фіскального контролю діяльності суб'єктів малого підприємництва. У цьому зв'язку потребує уточнення класифікація малого підприємництва та прийняття рішень щодо фіскального контролю, що має ґрунтуватись на необхідності забезпечення умов його розвитку, який безсуперечно стосується обліку та оподаткування.

В Україні відповідно напрямів реформування облікової системи згідно з вимогами Європейських Директив внесено суттєві зміни з липня 2019 року до законодавства що регулює формування фінансової звітності малих підприємств. Оновлений стандарт тепер має назву НП(С)БО 25 «Спрощена фінансова звітність». Його норми мають застосовувати мікропідприємства, малі підприємства, непідприємницькі товариства, представництва іноземних суб'єктів господарської діяльності та підприємства, які ведуть спрощений бухгалтерський облік доходів та витрат відповідно до податкового законодавства (крім підприємств, які відповідно до законодавства складають фінансову звітність за міжнародними стандартами фінансової звітності для складання Фінансової звітності малого та мікропідприємства.

Таблицею 1 наведено порівняння норм стандартів що діяли до 2019 року та оновлених. Унесені зміни відповідають нормам ст. 14 Директиви 2013/34/ЄС, якою передбачено, що малим підприємствам дозволяється складати скорочений балансовий звіт, у якому відображаються лише статті, пронумеровані в додатках до Директиви III та IV літерами і римськими цифрами, у тому числі вимагається розкриття інформації про нематеріальні активи підприємства.

Таблиця 1 – Порівняння норм стандартів формування фінансової звітності малих підприємств

До змін	З урахуванням змін, унесених Наказом № 226	Примітки
НП(С)БО 1 «Загальні вимоги до фінансової звітності»		
Для суб'єктів малого підприємництва і представництв іноземних суб'єктів господарської діяльності встановлюється скорочена за показниками фінансова звітність у складі балансу і звіту про фінансові результати, форма і порядок складання яких визначаються П(С)БО 25 «Фінансовий звіт суб'єкта малого підприємництва», затвердженим Наказом № 39	Для мікропідприємств, малих підприємств, непідприємницьких товариств, представництв іноземних суб'єктів господарської діяльності та підприємств, які ведуть спрощений бухгалтерський облік доходів та витрат, встановлюється скорочена за показниками фінансова звітність у складі балансу і звіту про фінансові результати, форма і порядок складання яких визначаються П(С)БО 25 «Спрощена фінансова звітність», затвердженим Наказом № 39	Зазначені підприємства можуть самостійно визначати доцільність складання фінансової звітності за формами, наведеними в цьому П(С)БО
НП(С)БО 25		
П(С)БО 25 «Фінансовий	П(С)БО 25 «Спрощена	Відповідно до вимог

звіт суб'єкта малого підприємництва»	фінансова звітність»	Директиви 2013/34/ЄС
Фінансовий звіт суб'єкта малого підприємництва (1-м, 2-м)	Фінансова звітність малого підприємства (1-м, 2-м)	Фінансовий звіт малого підприємства подають: малі підприємства – юридичні особи, які визнані такими відповідно до Закону № 996 (крім тих, яким відповідно до податкового законодавства надано дозвіл на ведення спрощеного обліку доходів та витрат); представництва іноземних суб'єктів господарської діяльності
Зміни, унесені до форми № 1-м		
–	Нематеріальні активи (ряд. 1000)	Наводиться сума залишкової вартості (ряд. 1001 – ряд. 1002), яка включається в підсумок балансу
–	Первісна вартість (ряд. 1001)	Наводиться сума первісної вартості нематеріальних активів (крім гудвілу) (визначається згідно з П(С)БО 8)
–	Накопичена амортизація (ряд. 1002)	Сума амортизації об'єкта нематеріальних активів з початку його корисного використання (П(С)БО 8)

Унесено уточнення до п. 2 Наказу № 186, а саме зазначено, які підприємства мають право застосовувати спрощений план рахунків: мікропідприємства, малі підприємства, непідприємницькі товариства, підприємства, які ведуть спрощений бухгалтерський облік доходів та витрат, а також представництва іноземних суб'єктів господарської діяльності.

Якщо малі підприємства використовують МСФЗ для МСП (для малих та середніх підприємств), то вони позбавляються права на подання скороченої фінансової звітності та подають її в повному складі. У разі прийняття рішення малими підприємствами щодо використання МСФЗ для МСП, то це має знайти відображення у наказі про облікову політику підприємства з обґрунтуванням причин використання МСФЗ. У разі застосування МСФЗ для МСП малі підприємства повинні складати звітність за НП(С)БО 1.

Висновки та перспективи подальших досліджень. У межах реформування політичної системи в Україні спостерігається тенденція посилення фіскального контролю діяльності суб'єктів малого підприємництва. У цьому зв'язку потребує уточнення класифікація малого підприємництва та прийняття рішень щодо фіскального контролю, що має ґрунтуватись на необхідності забезпечення умов його розвитку, який безсуперечно стосується обліку та оподаткування.

Список літератури

1. Державна служба статистики України „Діяльність суб'єктів великого, середнього, малого та мікропідприємництва" Статистичний збірник 2017 рік. 24-25с.
2. Статистична інформація Кількість суб'єктів господарювання в Кіровоградському регіоні за видами економічної діяльності у 2017 році. [Електронний ресурс] – режим доступу: http://www.kr.ukrstat.gov.ua/?r=stat/2018/10/finans/stat_inf_rik_finansy18
3. Положення (стандарт) бухгалтерського обліку 25 «Спрощена фінансова звітність», затв. наказом Міністерства фінансів України від 25.02.2000 р. № 39 [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/z0161-00
4. Таран Ілля Практика застосування міжнародних стандартів фінансової звітності № 9, вересень 2019 року 20-23 с

УДК 338.242.2

П. Криворучко, магістр гр.АДМ-18М-1,4
Центральноукраїнський національний технічний університет

ТЕОРЕТИЧНІ ПІДХОДИ ДО УДОСКОНАЛЕННЯ МЕНЕДЖМЕНТУ НА ПІДПРИЄМСТВАХ В СУЧАСНИХ ЕКОНОМІЧНИХ УМОВАХ

Для забезпечення належного рівня функціонування автотранспортного підприємства необхідні нові підходи до удосконалення менеджменту. В статті розглянуті актуальні питання управління підприємствами автотранспортних перевезень в Україні. Виділено основні чинники, що характеризують поточну ситуацію на таких підприємствах. Теоретично обґрунтовано можливості використання контролінгу, мотивації та інших інструментів удосконалення менеджменту автотранспортних підприємств.
автотранспортне підприємство, менеджмент, контролінг, мотивація персоналу

Постановка проблеми. Ефективність діяльності будь-якої організації досягається шляхом добре організованого менеджменту. Формування та реалізація менеджменту підприємствами та окремими об'єктами в цей час здійснюється на підставі різних підходів: системного (організація розглядається як цілісна кібернетична система); ситуаційного (діяльність підприємств планується в залежності від значимості та зміни ситуаційних факторів); функціонального (передбачається управління набором функцій (однорідних або спеціалізованих), які зосереджуються в окремих підрозділах, що будуються в ієрархічні структури); процесного (виділення бізнес-процесів і управління ними для досягнення максимальної ефективності діяльності) та інших.

Аналіз останніх досліджень і публікацій. Існує велика кількість фрагментарних досліджень, присвячених окремим проблемам менеджменту на транспортних підприємствах, зокрема слід виділити праці таких вчених, як М. Бідняк, О. Заяц, Ю. Когут, О. Криворучко, С. Міщенко, Н. Муромець та ін. У роботах вищезазначений авторів розкриваються різні сторони функціонування автотранспортних підприємств та акцентується увага на найбільш актуальних, але достатньо вузькоспеціалізованих аспектах стратегічного менеджменту вантажоперевезень. Однак, слід зазначити, що питання удосконалення менеджменту на автотранспортних підприємствах в Україні з урахуванням сучасної економічної ситуації залишаються актуальними та потребують дослідження.

Цілі статті. Мета даної статті полягає у розвитку теоретичних основ удосконалення менеджменту автотранспортних підприємств.

Виклад основного матеріалу. Автотранспортні вантажоперевезення для України – не новий вид господарської діяльності, але нині й досі не розроблені ефективні моделі

менеджменту вітчизняних автотранспортних підприємств, які б давали їм можливість на рівних конкурувати із європейськими та світовими лідерами цієї галузі.

Зауважимо, що сьогодні в кожному автотранспортному підприємстві варто, перш за все, розробити методику оцінки вартості послуг, структурувати основні складові собівартості, провести аналіз динаміки цих показників та розробити основні напрями їх оптимізації для вжиття своєчасних коригуючих заходів. При цьому, доцільно сформувати таку тарифну політику підприємства, щоб досягти максимального балансу економічних інтересів споживачів послуг та підприємств, що забезпечуватиме стабільність тарифів, їх гнучкість та прогнозованість, які б дозволяли адекватно реагувати на зміни зовнішніх умов та потреб ринку, досягнення визначених цілей для максимальної ефективності функціонування.

При цьому важливою є побудова системи фінансової відповідальності, реальне впровадження управління за центрами фінансової відповідальності. Але, на жаль, у багатьох автотранспортних підприємств немає чітко визначених показників керованості персоналу, на підставі яких визначалась би необхідність створення, виокремлення, або, навпаки, об'єднання структурних підрозділів. Існуюча структура підрозділів автотранспортне підприємство переважно склалась історично на основі типових структур та розвивалась переважно за принципом «функція-людина», тобто створення або виокремлення нових структурних одиниць за наявності функціонально виокремлених задач або відповідних кваліфікованих фахівців.

В адміністративно-фінансових підрозділах автотранспортного підприємства немає чітко встановлених критеріїв для нормування чисельності персоналу. Існуюча чисельність працівників, як правило, склалась історично та була визначена переважно суб'єктивно – керівниками відповідних підрозділів. Те ж саме стосується наявності окремих заступників у складі підрозділів.

Раціональним підходом у діяльності автотранспортного підприємства є використання певних критеріїв для визначення необхідності створення окремих структурних підрозділів у організаційній структурі підприємства, які базуються на потребах у виконанні функцій і бізнес-процесів, їх обсягах, спеціалізації, контролі, тощо.

Насамперед, такі критерії повинні включати необхідність розподілу повноважень для уникнення конфлікту інтересів та оптимальну кількість функціональних напрямів/підлеглих, якими здійснюється управління при збереженні ефективного контролю (норма керованості).

При створенні внутрішніх нормативних документів, які визначають той чи інший напрям діяльності підприємства, загальноприйнятим є вважати, що положення визначає основні принципи, правила і вимоги певного процесу. Регламент описує хід виконання процесу, його взаємозв'язок з іншими процесами, ролі виконавців і результати. Інструкція визначає послідовність кроків, необхідних для виконання певної дії. Методика описує сукупність підходів, алгоритмів розрахунку, формул, способів і прийомів для виконання певної дії.

Наявність окремо заступників у структурних підрозділах не є ефективною в організаційних структурах та приводить до зниження норми керованості та ефективності управління. Необхідно розробити та впровадити в автотранспортних підприємствах відповідні принципи, критерії та норми для визначення необхідності створення окремих адміністративних підрозділів у організаційній структурі підприємств та розрахунку їх чисельності, у тому числі з урахуванням можливості автоматизації процесів управління.

Для визначення норми керованості на рівні адміністративного персоналу доцільно використовувати мінімальну норму у п'ять штатних одиниць, як необхідну умову для створення нових відділів. Для забезпечення норми керованості для створення управлінь/департаментів на рівні адміністрації доцільно використовувати

Впровадження системи електронного документообороту та використання безпаперових технологій у бізнес-процесах дає можливість підприємствам зменшити навантаження на працівників, підвищити ефективність праці та оптимізувати чисельність

задіяного персоналу, зменшити витрати на матеріали для здійснення паперового документообороту та впорядкувати роботу з паперовими носіями, впорядкувати та прискорити процеси прийому та обробки документів, як внутрішніх так і зовнішніх, отримати єдине сховище документів, де організований швидкий та зручний пошук документів та яке відповідає сучасним вимогам інформаційної безпеки.

Окрім того, розвиток підприємства стає неможливим без комплексної системи мотивації на основі мотивуючих та демотивуючих факторів для кожної окремої категорії робітників, з урахуванням статі, віку та темпераменту кожної особистості. Тому керівникам необхідно не тільки стимулювати матеріально, але і прагнути, щоб підлеглі отримували задоволення від роботи; відчували себе особистостями; вірили в надійність і стабільність підприємства; бачили необхідність своєї роботи; були задоволеними від свого статусу в колективі. Керівництво підприємства повинне вживати заходи по постійному вдосконалюванню компенсаційного пакета, змінюючи його зміст відповідно до побажань співробітників. Для цього керівництво повинне періодично вивчати думку персоналу з питань можливих напрямків зміни змісту переліку пільг і компенсацій.

Висновки. Загалом шляхи удосконалення системи менеджменту автотранспортного підприємства повинні зосереджуватися на комплексному порядку удосконалення системи управління підприємством і всіма складовими частинами його для того, щоб забезпечити ефективність організаційних, кадрових і технічних рішень, процесів прийняття рішень та покращення інформаційних потоків. Важливим також є поліпшення інформаційної системи менеджменту з метою поліпшення якості інформації, а також можливостей її швидкого використання. Основним завданням удосконалення менеджменту автотранспортного підприємства є побудова таких управлінських систем, що забезпечують виконання необхідних дій і процедур для одержання найкращого ринкового результату. Удосконалення підходів до управління мотивацією персоналу в складі менеджменту підприємства дозволить поліпшити його господарську діяльність, оскільки сприятиме закріпленню кваліфікованих кадрів.

Список літератури

1. Бідняк М.Н., Омельянович О.Р., Заяц О.В. Теоретичні аспекти контролінгу. / Михайло Несторович Бідняк, Олексій Романович Омельянович, Ольга Василівна Заяц // Вісник. ¾ К.: НТУ ¾ 2012. ¾ Вип. 26, ст. 253-258.
2. Заяц О.В. Контролювання, моніторинг і діагностика як передумови контролінгу / О.В. Заяц // Економіка та управління на транспорті. – К.: НТУ, 2016. – Вип. 3, ст. 134-140.
3. Когут Ю.О. Моделювання бізнес-процесів АТП // Економіка транспортного комплексу: Збірник наукових праць. – Харків: Видавництво ХНАДУ. – 2010. – Вип. 16. – 212 с.
4. Криворучко О.М. Розробка стратегій управління персоналом автотранспортного підприємства [Текст]: [наук.-метод. рек.] / Криворучко О.М., Водолажська Т.О.; Харк. нац. автомоб.-дор. ун-т. – Х.: ХНАДУ, 2013. – 35 с.
5. Мазаракі А.А. Основи менеджменту. Харків: Фоліо, 2014. – 846 с.
6. Міщенко С.П. Управління автотранспортними підприємствами в умовах нестабільної економічної ситуації в Україні // Розвиток методів управління та господарювання на транспорті.– № 38. -2012. – С . 132-142.
7. Муромець Н.Є. Забезпечення стійкого функціонування автотранспортної системи регіону [Текст]: монографія / Муромець Наталія Євгенівна, Чорноус Оксана Іванівна ; ПВНЗ «Донец. акад. автомоб. трансп.». – Донецьк: ВІК, 2010. – 277 с.
8. Шинкаренко В.Г. Удосконалення автотранспортних послуг [Текст] / Шинкаренко В.Г., Ананко І.М.; Харк. нац. автомоб.-дор. ун-т. – Х. : ХНДАУ, 2011. – 33 с.

УДК: 657

О. Крячко, магістр гр. ОО-18МЗ-1,4
Центральноукраїнський національний технічний університет

ЕКОЛОГІЧНА ДІЯЛЬНІСТЬ ЯК ЕЛЕМЕНТ КОНЦЕПЦІЇ СТАЛОГО РОЗВИТКУ СУСПІЛЬСТВА

У статті розкрито сутність концепції сталого розвитку суспільства, її складові та взаємозв'язок між ними. Визначено пріоритетний напрям розвитку суспільства на сучасному етапі. Визначено сутність екологічної діяльності підприємств як складової сталого
концепція сталого розвитку суспільства, екологічна складова сталого розвитку, соціальна складова сталого розвитку, економічна складова сталого розвитку, екологічна діяльність

Актуальність дослідження. Кінець XX - початок XXI ст. характеризується поглибленням кризових явищ у всіх сферах світового розвитку. Така ситуація вимагає від людства формування нового світогляду, нових цінностей, коригування цілей і пріоритетів. Як результат за найбільш прийнятну мету було визначено сталий розвиток людства. Концепція сталого розвитку містить абсолютно нові погляди на сутність та проблеми світоустрою. Слідування концепції сталого розвитку передбачає суттєві зміни в усіх сферах суспільного життя, віддаючи перевагу цивілізованому співіснуванню природи та суспільства. Одним із найважливіших напрямів тут є ощадливе використання природних ресурсів, розвиток нових, екологічно орієнтованих галузей і видів діяльності, впровадження «зелених технологій», що має забезпечити гармонійне узгодження економічного, соціального і екологічного розвитку.

Проблеми збереження навколишнього середовища у процесі здійснення підприємствами господарської діяльності досліджували такі вітчизняні вчені: Ю.А. Краснова [1], І.Я. Кулиняк [2], О. Михайленко [3], Г.М. Проскура [4], С. Совгіра [5], С.А. Якимчук [6]. Теоретико – методологічні та практичні напрацювання представлені працями зарубіжних науковців: А. Бєлоусова, Г. Вінтера, А. Гофмана, Н. Еліаса, М. Моувена, В. Палія, Д. Панкова, Я. Соколова, Д. Хенсена, А. Шеремета та інших.

Мета, завдання, об'єкт дослідження. Мета дослідження полягає у вивченні сутності екологічної діяльності підприємств, місця екологічної складової у системі сталого розвитку, визначенні проблем екологічної діяльності суб'єктів господарювання.

Результати дослідження. Концепція сталого розвитку набула актуальності у 20-му сторіччі і до набуття свого сучасного змісту пройшла певні етапи, на кожному з яких превалювали різні проблеми (рис. 1).

Рисунок 1 – Етапи та основні напрями концепції сталого розвитку

Збереження довкілля у концепції сталого розвитку на перше місце було висунуто лише у 80-тих роках 20 сторіччя, коли погіршення стану навколишнього середовища набуло загрозливих масштабів.

У 1972 році на проблеми довкілля увагу світової громадськості звернув Римський клуб. Вперше питання збереження навколишнього середовища було порушено на Конференції ООН з довкілля людини (1972, м. Стокгольм). Конференція визнала актуальність екологічних проблем та необхідність вжиття міжнародних заходів для їх розв'язання.

У 1980 році вийшла «Всесвітня стратегія охорони природи» (ВСОП), підготовлена Міжнародною спілкою охорони природи (МСОП), яка затвердила курс на сталий розвиток та розкрила його зміст. Наріжним питанням цієї стратегії було принципово нове положення: збереження природи нерозривно пов'язане з питаннями розвитку, тобто розвиток суспільства повинен відбуватися за умови збереження природи.

Світове співтовариство визнало, що збалансований розвиток «повинен стати пріоритетним питанням порядку денного міжнародного співробітництва» [1]. Загальноприйнятим є розуміння збалансованого розвитку як гармонійного поєднання економічних, соціальних та екологічних складових розвитку. Лише досягнення збалансованості між ними забезпечить перехід до такого суспільного розвитку, який не виснажуватиме природні та людські ресурси, а тому матиме можливість тривати досить довго.

Концепція збалансованого (сталого) розвитку стала відповіддю на виклик часу. Вона є альтернативою панівній моделі сучасного розвитку, що ґрунтується на розгляді природи лише як джерела сировини для виробництва різних товарів. Збалансований розвиток визначено ключовим принципом усіх політик ЄС.

З огляду на євроінтеграційні прагнення України, варто зазначити, що принцип збалансованого розвитку закріплено в установчому Амстердамському договорі ЄС (Договір про ЄС, 1997 рік) який є основою для розробки і прийняття стратегій і програм в Україні. Згідно з ним Договором будь-яку політику ЄС слід розробляти так, щоб вона враховувала економічні, соціальні та екологічні аспекти, а досягнення цілей в одній зі сфер політики не стримувало б прогресу в іншій.

Слідуючи принципам та вимогам Договору ЄС та загальній Стратегії збереження навколишнього середовища у світі, Президент України розпорядженням від 31 жовтня 2011 року № 309/2011-рп уповноважив Міністра екології та природних ресурсів України на підписання від імені України Нагойсько-Куала-Лумпурського додаткового протоколу про відповідальність і відшкодування до Картахенського протоколу про біобезпеку (15 жовтня 2010 року у м. Нагої). Цим самим було затверджено і підтверджено курс України на сталий розвиток.

Поняття "сталий розвиток" у нашій країні з'явився відносно недавно, як переклад терміну «устойчивое развитие» з російської мови, а не безпосереднього перекладу цього терміна з англійської. Саме в такому вигляді утвердився він і в законодавстві України, хоча по суті є сполученням слів з протилежним змістом (сталий – постійність, розвиток – передбачає наявність змін). Загалом термін «сталий розвиток» з'явився у 1980 році, коли вийшла «Всесвітня стратегія охорони природи» (ВСОП), підготовлена Міжнародною спілкою охорони природи (МСОП).

Поняття «сталий розвиток» почали широко застосовувати після публікації у 1987 році звіту Міжнародної комісії з довкілля та розвитку «Наше спільне майбутнє», підготовленого під керівництвом Г. Х. Брундтланд. Концепція сталого розвитку набула провідного статусу після Конференції ООН з довкілля та розвитку (1992, м. Ріо-де-Жанейро) і була відображена в прийнятому на конференції Порядку денному на 21 століття.

Таблиця 1 - Аналіз трактування та розуміння поняття “сталий розвиток”

Джерело, автор	Трактування
Вікіпедія	Ста́лий розвиток – загальна концепція стосовно необхідності встановлення балансу між задовільненням сучасних потреб людства і захистом інтересів майбутніх поколінь, включаючи їх потребу в безпечному і здоровому довкіллі.
Конференція ООН з навколишнього середовища і розвитку	сталий розвиток – це такий розвиток суспільства, який задовольняє потреби сучасності, не ставлячи під загрозу здатність наступних поколінь задовольняти свої власні потреби.
О. Невелєв	економічно, соціально та екологічно збалансований розвиток певних територій і розташованих на них міських та сільських поселень, спрямований на узгоджене формування і функціонування економічної, соціальної та екологічної складових цього розвитку на основі раціонального використання всіх видів ресурсів
В. П. Кухар	розвиток, що самопідтримується, це ідеологія розумної й обґрунтованої діяльності людини, яка живе у злагоді з природою та створює умови для кращого життя собі і наступним поколінням.
О. І. Котикова	модель функціонування системи із обмеженими параметрами, яка забезпечує збалансовану динамічну рівновагу між компонентами інтегрованої екосистеми протягом визначеного проміжку часу
В. Барановський	розвиток, що забезпечує певний тип рівноваги, тобто баланс між соціально-економічними та природними його складовими
Б. Данилишин, Л. Шостак	такі відносини в суспільному виробництві, завдяки яким досягаються оптимальні пропорції нормалізації якісного стану середовища, економічного зростання і зростання духовних і матеріальних потреб людей
Л. Корнейчук	розвиток без виходу ресурсопотоку за межі регенеративних і поглинаючих можливостей навколишнього середовища.
Концепція програми «Сталий розвиток України»	модель економічного зростання, в якій використання ресурсів спрямоване на задоволення потреб людини при збереженні навколишнього середовища, так що ці потреби в розвитку можуть бути задоволені не тільки в сьогоденні, але й для майбутніх поколінь

Як видно із трактувань, наведених у таблиці, сталий розвиток передбачає у своєму складі три головні компоненти: природоохоронну і соціальну, при цьому, на сьогодні екологічна складова займає пріоритетне місце.

Основним у реалізації концепції сталого розвитку є забезпечення узгодження та збалансування усіх трьох складових, які у своєму взаємозв’язку висувають конкретні завдання (рис. 2).

Виходячи з сутності складових сталого розвитку можна визначити взаємозв’язок між ними. Взаємний зв’язок соціальної та екологічної складових визначає необхідність збереження однакових прав сьогоднішніх і майбутніх поколінь на використання природних ресурсів. Взаємозв’язок соціальної та економічної складових потребує забезпечення справедливості при розподілі матеріальних благ між людьми й надання цілеспрямованої допомоги бідним прошаркам суспільства. Взаємозв’язок екологічної та економічної складових потребує вартісної оцінки наслідків впливів людини на довкілля.

З точки зору економічного підходу Концепція сталого розвитку передбачає оптимальне використання обмежених ресурсів та застосування ресурсозберігаючих технологій. Сучасний розвиток економіки характеризується наростанням обсягів інформації

та знань. Сьогодення можна охарактеризувати як перехід до інформаційного суспільства, що приводить до зміни структури сукупного капіталу на користь людського, збільшуючи потоки фінансів, інформації та інтелектуальної власності.

Рисунок 2 – Взаємозв'язки складових Концепції сталого розвитку

Соціальна складова сталого розвитку орієнтована на людський розвиток, на збереження стабільності суспільних і культурних систем, на зменшення кількості конфліктів у суспільстві. Згідно з нею, людина має стати не об'єктом, а суб'єктом розвитку, має стати активним учасником у процесах формування своєї життєдіяльності, прийнятті й реалізації рішень, контролі за їх виконанням. Важливе значення для реалізації соціальної складової сталого розвитку відіграє справедливий розподіл благ між людьми, збереження культурного капіталу і його розмаїття.

Висновок. На перше місце у забезпеченні сталого розвитку виступає сьогодні екологічна складова. З точки зору екології**,** сталий розвиток має забезпечити цілісність біологічних і фізичних природних систем, їх життєздатність, від чого залежить глобальна стабільність усієї біосфери.

Реалізація положень концепції сталого розвитку сьогодні є першочерговим завданням людської спільноти загалом, та кожної держави, зокрема. При цьому вирішення цих завдань, що витікають із взаємозв'язків складових сталого розвитку є найголовнішим при формуванні екологічної політики на всіх рівнях суспільства: державному, регіональному, кожного суб'єкта господарювання, кожного громадянина**.**

Список літератури

1. Краснова Ю. А. Деякі підходи щодо визначення поняття екологічно небезпечної діяльності [Електронний ресурс] / Ю. А. Краснова // Науковий вісник Національного університету біоресурсів і природокористування України. Серія : Право. - 2013. - Вип. 182(1). - С. 151-158. - Режим доступу : http://nbuv.gov.ua/UJRN/nvnau_prav_2013_182(1)__22
2. Кулиняк І. Я.Перспективні напрями екологічно орієнтованої діяльності підприємств [Електронний ресурс] / І. Я. Кулиняк, Г. І. Куцик // Вісник Чернівецького торговельно-економічного інституту. Економічні науки. - 2015. - Вип. 4. - С. 47-53. - Режим доступу: http://nbuv.gov.ua/UJRN/Vchtei_2015_4_7
3. Михайленко О. Визначення підходів до трактування сутності сталого розвитку [Електронний ресурс] / О. Михайленко, Невелєв О. // Збірник наукових праць Черкаського державного технологічного університету. Сер. : Економічні науки. - 2014. - Вип. 37(1). - С. 124-129. - Режим доступу: http://nbuv.gov.ua/UJRN/Znpchdtu_2014_37(1)__21

4. Проскура Г. М.Прийняття та вплив Орхуської конвенції на доступ до екологічної інформації в Україні [Електронний ресурс] / Г. М. Проскура // Юридичний вісник. Повітряне і космічне право. - 2018. - № 2. - С. 83-88. - Режим доступу: http://nbuv.gov.ua/UJRN/Npnau_2018_2_13
5. Совгіра С. Екологічне мислення – вища форма пізнавальної діяльності людини [Електронний ресурс] / С. Совгіра // Збірник наукових праць Уманського державного педагогічного університету. - 2012. - Ч. 4. - С. 319-325. - Режим доступу: http://nbuv.gov.ua/UJRN/ _2012_4_43
6. Якимчук С. А. Зарубіжний досвід у сфері охорони навколишнього природного середовища [Електронний ресурс] / С. А. Якимчук // Економічний часопис-XXI. - 2013. - № 7-8(2). - С. 17-20. - Режим доступу: http://nbuv.gov.ua/UJRN/ecchado_2013_7-8(2)__6

УДК 330.341

Р. Кубальський, магістр гр. АДМ-18М-1,4
Центральноукраїнський національний технічний університет

ТЕОРЕТИЧНІ ПІДХОДИ ДО УПРАВЛІННЯ ІННОВАЦІЙНИМ РОЗВИТКОМ ПІДПРИЄМСТВА

У статті розглянуті актуальні питання теоретичного характеру, пов’язані із управлінням інноваційним розвитком сучасного підприємства. Відзначено, що інноваційний розвиток підприємства є важливою умовою підвищення якості продукції чи послуг, а також нарощування темпів і обсягів виробництва. Окреслено значущість інноваційного розвитку для підприємства. Виділено основні особливості управління інноваційним розвитком сучасного підприємства, такі, як стратегічне планування, об’єднання в інноваційно-інтегровані структури, застосування цифрових технологій, розвиток корпоративної культури.
підприємство, інноваційний розвиток, управління, цифрові технології

Постановка проблеми. Однією зі стратегічно важливих складових економічного розвитку в сучасних умовах є інноваційна сфера, оскільки вона створює основу для якісного й динамічного економічного зростання національної економіки та є індикатором ефективності її функціонування. Тому дослідження питання розвитку інноваційного та науково-технічного потенціалу, а також створення і підтримка національної інноваційної системи України є актуальними з теоретичної і практичної точки зору. Запорукою успішного функціонування будь-якого підприємства є його здатність до ведення інноваційної діяльності. Разом із тим, враховуючи значний рівень ризику та необхідність значних фінансових витрат, які супроводжують інноваційну діяльність, коло підприємств, здатних до повноцінної реалізації програм інноваційного розвитку, є досить обмеженим. Проблема інноваційного розвитку підприємств України є актуальною, проте, все ще невирішеною.

Аналіз останніх досліджень і публікацій. Вивченню питань інноваційного розвитку економіки присвячено багато досліджень вітчизняних науковців. На наш погляд, доцільно виокремити праці таких вчених, як О. Амоша, Г. Андрощук, В. Антонюк, О. Бутенко, В. Геєць, С. Давимука, А. Землянкін, О. Корнух, Н. Краснокутська, В. Кучинський, Т. Скрипко, О. Сторожук, Л. Федулова, І. Шовкун, Л. Шульгіна та ін. Не применшуючи значення їх праць, слід відзначити, що проблеми удосконалення підходів до активізації інноваційного розвитку підприємств все ще залишаються невирішеними і потребують досліджень.

Мета статті. Метою написання даної статті є дослідження теоретичних засад здійснення інноваційного розвитку підприємств в Україні.

Виклад основного матеріалу. Проведене нами дослідження дозволяє відзначити, що у працях, присвячених вивченню інноваційної діяльності приділяється недостатньо уваги аналізу підходів до управління інноваційним розвитком підприємства з урахуванням сучасного етапу розвитку економіки України, зокрема модернізації та цифрової трансформації.

З теоретичної точки зору інновації можна розглядати як технологічні, комерційні, економічні, соціальні, екологічні тощо. В Законі України «Про інноваційну діяльність» поняття «інновації» трактується, як «новостворені (застосовані) і (або) вдосконалені конкурентоспроможні технології, продукція або послуги, а також організаційно-технічні рішення виробничого, адміністративного, комерційного або іншого характеру, що істотно поліпшують структуру та якість виробництва і (або) соціальної сфери» [8]. Таким чином, інновації стосуються як виробничої сфери, так і сфери послуг (транспорт, торгівля, банківська діяльність тощо), оскільки вони ґрунтуються на рішеннях виробничого та комерційного характеру.

Обов'язковою властивістю інновації є науково-технічна новизна і виробнича придатність. Комерційна реалізація по відношенню до інновації виступає як потенційна властивість, для досягнення якої необхідні певні зусилля. Інновацію-результат потрібно розглядати з урахуванням інноваційного процесу. Для інновації в рівній мірі важливі всі три властивості: науково-технічна новизна, виробнича застосовність і комерційна реалізованість. Відсутність будь-якого з них негативно позначається на інноваційному процесі. Основу вироблення інноваційної стратегії підприємства становлять теорія життєвого циклу продукту або послуги (періоду від зародження ідеї, створення новинки та її практичного використання до моменту зняття з виробництва), ринкова позиція підприємства і науково-технічна політика, яка реалізується підприємством.

Необхідність розробки стратегічних планів інноваційного розвитку виникає в зв'язку з постійною і складною взаємодією внутрішніх і зовнішніх факторів, що впливають на функціонування підприємства. Відтак, вони змушені приймати довгострокові рішення стосовно маркетингу, покращення технології, удосконалення продукції чи послуги, підготовки та перепідготовки персоналу, збільшення гнучкості виробництва, зниження витрат сировини та матеріалів, зниження споживання енергії, оновлення основних фондів та інших питань. Галузеві особливості, невизначеність зовнішнього середовища, рівень конкурентоспроможності підприємства, ступінь адаптації до ринку визначають специфіку прийнятих стратегічних рішень.

Аналіз інноваційного розвитку в Україні показує, що питанням активізації інноваційної діяльності в країні належить велика роль. Основи інноваційної політики нашої країни закладені в «Стратегії інноваційного розвитку України на 2009-2018 роки та на період до 2039 року» [11]. Разом із тим необхідно відзначити, що інноваційна діяльність в Україні поки не є джерелом підвищення конкурентоспроможності країни на світовому ринку. Однією з проблем інноваційного розвитку в нашій державі на сьогодні є незавершеність наукових досліджень та їх відірваність від виробництва. Завершені прикладні розробки часто не мають свого продовження у вигляді комерціалізації і впровадження у виробництво.

Важливою ознакою інноваційного розвитку підприємства є результат використання його інноваційного потенціалу, тобто створення або поліпшення товару чи послуги, вдосконалення технології виробничого процесу. На сучасному етапі розвитку економіки визначальними у функціонуванні підприємств, виробництві наукомісткої продукції є інноваційно-інтегровані структури, в яких кожен з учасників отримує певні гарантії стабільного попиту на свою продукцію, перспективного інноваційного розвитку. Крім того, розвиток інноваційного потенціалу сучасного підприємства неодмінно пов'язаний із застосуванням цифрових технологій.

Інноваційна культура як складова інноваційного розвитку є мірою сприйнятливості підприємства до нововведень, наявності досвіду впровадження нових проєктів, розвинутого інноваційного менеджменту, лояльного ставлення персоналу до впровадження інновацій.

При пошуку шляхів активізації інноваційного розвитку підприємства велику увагу також потрібно приділяти інформаційній захищеності інноваційного потенціалу підприємства, що полягає в можливості протистояти зовнішнім загрозам. В епоху становлення цифрової економіки до основних таких загроз можна віднести наступні: слабкий розвиток цифрової інфраструктури; кібертероризм; посилення промислового шпигунства;

крадіжки даних з промислових інформаційних систем; зумисна фальсифікація даних і документів; помилки в програмному забезпеченні; цифрова безграмотність персоналу; брак «цифрових» талантів на вітчизняних підприємствах; ризики, пов'язані зі швидкою зміною інформаційних технологій; порушення функціонування складних інформаційних систем [10].

Висновки. Хоча існують різні погляди вчених на визначення сутності поняття інноваційного розвитку підприємства, для його активізації потрібні певні зусилля організаційного характеру, а також достатнє наукове, технологічне та інвестиційне забезпечення. Інноваційний розвиток будь-якого підприємства є безальтернативним шляхом виживання та зміцнення його конкурентних позицій у ринковому середовищі господарювання. Інновації стосуються усіх аспектів функціонування підприємства і є результатом здійснення певних заходів. Динамічні зміни ринкових умов господарювання вимагають від підприємств здійснення безперервних змін для утримання і зміцнення існуючих ринкових позицій. Однак, ці заходи повинні бути стратегічними, тобто підприємства мають їх заздалегідь планувати, передбачати можливі кон'юнктурні зміни і здійснювати превентивні дії, а не бути змушеними різко реагувати на зовнішні зміни. З метою мінімізації ризиків інноваційного характеру, пов'язаних з цифровою трансформацією підприємства необхідно створити умови для формування безпечних інформаційних систем та систем захисту від кіберзлочинності.

Список літератури

1. Активізація інноваційної діяльності: організаційно-правове та соціально-економічне забезпечення: монографія / О.І. Амоша, В.П. Антонюк, А.І. Землянкін та ін. / НАН України. Ін-т економіки промисловості. – Донецьк, 2007. – 328 с.
2. Бутенко О.А. Основні напрями та пріоритети інноваційної діяльності в Україні / О.А. Бутенко // Держава та регіони. Серія: Економіка та підприємництво, 2006. – № 3. – С. 28–30.
3. Геєць В.М. "Інноваційна Україна – 2020": основні положення Національної доповіді (стенограма наукової доповіді на засіданні Президії НАН України 13 травня 2015 р.) / В.М. Геєць // Вісник Національної академії наук України. – 2015. – № 7. – С. 14–22. – Режим доступу: http://nbuv.gov.ua/UJRN/vnanu_2015_7_5
4. Корнух О.В. Стратегічне управління інноваційним розвитком підприємства / О.В. Корнух // Ефективна економіка. – 2013. – № 12. – С. 3–10.
5. Краснокутська Н. В. Інноваційний менеджмент: Навч. посібник. – Київ : КНЕУ, 2003. – 504 с.
6. Кучинський В.А. Оцінка і розвиток інноваційного потенціалу підприємства / В.А. Кучинський, А.Д. Гайдукова // Вісник НТУ «ХПІ». – 2014. – № 65(1107). – С. 139–147.
7. Національні інноваційні системи: еволюція, детермінанти результативності: монографія / Г.О. Андрощук, С.А. Давимука, Л.І. Федулова – К. : Парлам. Вид-во, 2015. – 512 с.
8. Про інноваційну діяльність : Закон України // Відомості Верховної Ради України (ВВР). – 2014. – № 2–3. – Ст. 1.
9. Скрипко Т.О. Інноваційний менеджмент: підручник / Т.О. Скрипко. – К. : Знання, 2011. – 423 с.
10. Сторожук О.В. Потенційні ризики та можливості цифрової економіки / О.В. Сторожук, О.В. Заярнюк // Стратегічні пріоритети трансформації економіки в умовах цифровізації : матеріали Міжнародної науково-практичної конференції, Запоріжжя, 29–30 жовтня 2019 р. Національний університет «Запорізька політехніка», Запоріжжя : ФОП Мокшанов В.В., 2019. – С. 238–239.
11. Стратегія інноваційного розвитку України на 2009–2018 роки та на період до 2039 року // Державне агентство України з інвестицій та розвитку [Електронний ресурс]. – Режим доступу : http://www.in.gov.ua
12. Шовкун І.А. Фінансове забезпечення інноваційної діяльності в контексті неоіндустріалізації економіки України / І.А. Шовкун // Фінанси України. – 2014. – № 12. – С.83–95.
13. Шульгіна Л.М. Сучасні концепції стратегічного управління інноваційним розвитком підприємства / Л. М. Шульгіна, В. В. Юхименко // Маркетинг і менеджмент інновацій. – 2011. – № 3. – С. 79–84.

УДК 021.6

В. Кузьменко, магістр гр. ІС-18М
Центральноукраїнський національний технічний університет

ДОКУМЕНТАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ РЕКЛАМИ АВТОЗАПРАВНОГО КОМПЛЕКСУ ТОВ «ОККО-РІТЕЙЛ»

У статті досліджено документні ресурси ТОВ «ОККО-Рітейл» як джерело розвитку та вдосконалення основної діяльності установи
документаційні ресурси, автозаправний комплекс, документ, документальний фонд

Актуальність статті. Основними різновидами документів, що функціонують в PR-підрозділі, є документація, що забезпечує ефективне та довготривале встановлення гармонійних відносин між агентством та корпораціями галузевих напрямків та між співробітниками ТОВ «ОККО-Рітейл». Оскільки, окрім усних комунікацій важливу частину на підприємстві займає документна комунікація, то важливо простежити за розвитком та функціонуванням документних масивів, оскільки від цього залежить раціональність організації документаційного забезпечення інформаційної діяльності відділу реклами. Матвієнко О. В. зазначає, що «Документаційне забезпечення інформаційної діяльності охоплює питання документування, організації роботи з документами в процесі здійснення діяльності та систематизації їх архівного зберігання і являє собою діяльність спеціальних працівників щодо створення документаційно-інформаційної бази на різних носіях для використання працівниками у процесі реалізації їх функцій» [8]. Будь-який документ ТОВ «ОККО-Рітейл» проходить усі стадії свого життєвого циклу: від створення до зберігання або знищення.

Метою даної статі є розгляд особливостей документаційно-інформаційного забезпечення відділу реклами та вдосконалення роботи служби зв'язків з громадськістю комерційного підприємства, що функціонує в інформаційному середовищі України.

Для написання даної статті та розробки теми використовувалися праці українських (В. Г. Королько [7], Г. Г. Почепцов [9], О. В. Матвієнко [8], В. С. Білоус [1]), російських (О. М. Чуміков [10], М. П. Бочаров [3], С. О. Варакута [5]) та зарубіжних (С. Катліп [6], Ф. А. Буарі [4], С. Блек [2]) авторів.

Завданнями даної публікації є: дослідити функції, структуру та принципи організації відділу public relations в ТОВ «ОККО-Рітейл», проаналізувати сучасний стан документаційно-інформаційного забезпечення PR-діяльності в організації, запропонувати методи покращання роботи на основі аналізу показників ефективності діяльності відділу реклами.

Основним видом документованої інформації в PR-відділі є маркетингова інформація, що відіграє суттєву роль у визначенні ринкової частки і ринкової позиції ТОВ «ОККО-Рітейл», у виявленні ринку. Від її повноти, достатності та якості викладу у документах залежить успіх або невдача підприємства на ринку. Саме тому документообігу приділяється велика увага, оскільки керівництво організації розуміє, що правильна та раціональна організація роботи з документами – важлива складова частина процесу управління і прийняття управлінських рішень, яка істотно впливає на оперативність та якість діяльності підприємства.

Основними завданнями, які ставить керівництво ТОВ «ОККО-Рітейл» до документаційного забезпечення інформаційної діяльності як комплексу заходів, можна вважати:

зниження інформаційних потоків відділу до мінімуму;

забезпечення спрощення та здешевлення процесів збору, обробки та передачі інформації за допомогою новітніх технологій автоматизації цих процесів;

недопущення створення відомостей, звітів, зведень не передбачених посадовою інструкцією та положенням про відділ зв'язків з громадськістю;

забезпечення єдиного порядку документування, організації роботи з документами.

У PR-відділі ТОВ «ОККО-Рітейл» відсутній спеціаліст, до функціональних обов'язків якого входила б організація документообігу у відділі, тому посадові обов'язки справочинця виконують спеціалісти public relations обох напрямів.

Для забезпечення виконання завдань документаційного забезпечення інформаційної діяльності відділу зв'язків з громадськістю, спеціалісти виконують такі функції:

здійснення початкової експедиційної обробки вхідних документів;

ведення інформаційно-довідкової роботи із документами відділу;

машинописне виготовлення документів;

копіювання, тиражування та оперативне розмноження документів;

розробка та проектування бланків документів;

підготовка документів до відправлення;

організація зберігання документів в підрозділах відділу зв'язків з громадськістю;

контроль за коректністю оформлення документів, що мають бути підписаними керівником відділу;

здійснення контролю за правильністю оформлення та формування в підрозділах відділу справ, що будуть передаватися до зберігання або знищення;

забезпечення знищення, зберігання справ та оперативного використання документної інформації.

Як на будь-якому підприємстві, документація в PR-відділі ТОВ «ОККО-Рітейл» поділяється на вхідну, вихідну та внутрішню. Ці три категорії документів складають загальний документообіг відділу.

Внутрішні документи – документи, створені в PR-департаменті, і не призначені для виходу за її межі. Цей вид документації, відповідно до діяльності інформаційного агентства, умовно можна розділити на наступні категорії.

PR-документи, що визначають організаційну базу стратегічної та оперативної PR-діяльності підприємства. До такого виду PR-документів відносять концепції, PR-кошториси, бюджет відділу тощо. Основна їх мета – оцінювання та прогнозування діяльності PR-відділу, стратегій впровадження інформаційного продукту та оцінювання прибутковості реалізації продукції. Цей вид документів в підрозділі має конфіденційний характер. Доступ до них має лише керівництво, керівник відділу зв'язків з громадськістю, бухгалтерія та відповідальний керівник певного PR-проекту.

Головним внутрішнім документом, якого дотримуються протягом інформаційної діяльності PR-відділу є план роботи відділу. У змісті даного документа відображаються перелік завдань відділу; терміни їх виконання; відомості про відповідальних виконавців; відомості про потрібні ресурси; порядок здійснення контролю; зміст основних заходів забезпечення та взаємодії з іншими спеціалістами та підрозділами; облік результатів виконаних завдань.

Розробляють, узгоджують та затверджують план керівник відділу та керівники зовнішньої та корпоративної комунікації.

Так, до плану заходів маркетингової діяльності ТОВ «ОККО-Рітейл» на включено такі заходи:

реклама на біг-бордах;

рекламні листівки, буклети;

реклама в ЗМІ;

брендування автотранспорту;

проведення дегустації;

аудіореклама в торгів. мережі супермаркетів;

ТВ-реклама;

виготовлення роздаткових матеріалів для лінійної мережі (сувенірна продукція) до свят;

семінари, тренінги комерційного відділу;

реклама у транспорті;

участь у виставках;

проведення соцопитувань;

проведення прес-конференцій.

Всі інші види внутрішніх PR-документів на підприємстві (річний звіт, PR- концепції, бюджет відділу) розробляються та впроваджуються в дію за необхідності. Наприклад, PR-концепція розробляється лише після проведення дослідження, правильної постановки цілей, визначення стратегії та цільових аудиторій певного PR-заходу. PR-бюджет відділу реклами складається щорічно на основі оцінки рівня ресурсів, необхідних для проведення інформаційної діяльності та оцінки вартості та доступності цих ресурсів.

До другої групи відносять документи, що регламентують діяльність підприємства: «Положення про відділ реклами», накази та розпорядження керівництва, посадові інструкції працівників, службові повідомлення, основні нормативно-правові акти, що регламентують діяльність усього інформаційного агентства. Основними завданнями такого виду документації є інформування працівників про зміни, що відбуваються у відділі, на підприємстві та в його оточенні; регламентування та координація дій працівників при виконанні поетапного завдання, вирішення спірних питань щодо чинного законодавства в інформаційній сфері.

Для встановлення сприятливого клімату із споживачами спеціалісти відділу використовують такі види документів, як корпоративні видання: календарі, буклети, інформаційні листи.

Вихідні документи – документи, що призначені для відправлення у інші організації. Цей вид документації у відділі реклами представлений PR-документами, що випускаються у вигляді продукту інформаційної діяльності підрозділу. Це є press-releases, інформаційні листи, брошури, press-kits, заяви для преси. Основним завданням вихідних документів є доведення до споживачів інформації певного характеру.

Перед розробкою та складанням вихідних документів, спеціалісти відділу визначають такі моменти:

предмет матеріалу (інформація про новий продукт, новини від керівництва, повідомлення для працівників);

ключові ідеї – сформульоване уявлення про основні ідеї матеріалу;

обсяг та формат майбутнього матеріалу (press-release, брошура, календар тощо);

призначення та мета матеріалу (інформування, переконання, заохочення);

У відділі реклами ТОВ «ОККО-Рітейл» повноцінно функціонує електронний документообіг, що полегшує працю спеціалістів та скорочує час на пошуки потрібного документа і дозволяє реалізувати такі процеси:

організацію єдиного порядку роботи з документами у підрозділах;

організацію індивідуальної та спільної змістової підготовки документів у підрозділах;

обмін документами між структурними підрозділами інформаційного агентства;

реєстрацію руху документів, включаючи візування у керівництва;

створення належних умов для документаційного та організаційно-технічного забезпечення роботи керівництва, своєчасне забезпечення повною, точною та достовірною інформацією;

одержання звітів на основі інформації про документ і стан його виконання.

Отже, можна констатувати, що відділ реклами ТОВ «ОККО-Рітейл» використовує лише новітні технології обробки інформації та створення електронного документообігу на підприємстві, що дозволяє повністю виключити наявність паперових документів, зекономити

кошти на обробці документів та звільнити час для інноваційної діяльності працівників інформаційного агентства.

Список літератури

1. Білоус В.С. Зв'язки з громадськістю (паблік рилейшнз) в економічній діяльності: навч. посібник. Київ: КНЕУ, 2005. 275 с.
2. Блэк С. Введение в public relations. Ростов – на –Дону.: Изд-во «Феникс», 2003. 159 с.
3. Бочаров М.П. История паблик рилейшнз: обычаи, бизнес, наука. Москва: Изд-во «Известия», 2000. 176 с.
4. Буари Ф.А. Паблик рилейшнз или стратегия доверия. Москва: Изд-во «Инфра-М», 2001. 96с.
5. Варакута С.А. Связи с общественностью: учеб. пособие. Москва, 2001. 245с.
6. Катлип С.М. Паблик рилейшнз. Теория та практика: учебн.пособие. Москва, 2000. 614 с.
7. Королько В.Г. Основы паблик рилейшнз. Київ: «Ваклер», 2001. 528с.
8. Матвієнко О.В. Основи електронного документообігу: Навч.посібник / О.В.Матвієнко, М.Н.Цивін. Київ: Центр учбової літератури, 2008. 112 с.
9. Почепцов Г. Паблік рилейшнз: навч. посіб. Київ, 2000. с. 23.
10. Чумиков А.Н. Креативные технологии «паблик рилейшнз»: учеб.пособие. Москва: Изд-во «Новая Россия», 1998. 216 с.

УДК 021.6

М. Кучеренко, магістр гр. ІС-18М
Центральноукраїнський національний технічний університет

ЗАГАЛЬНА ХАРАКТЕРИСТИКА ТА СТРУКТУРА САЙТУ ДЕРЖАВНОГО АРХІВУ КІРОВОГРАДСЬКОЇ ОБЛАСТІ

У статті досліджено веб-сайт Державного архіву Кіровоградської області як документально-інформаційну систему та визначено його оптимальні характеристики.
веб-сайт, Державний архів Кіровоградської області, документально-інформаційна система

Актуальність статті. Архівні установи України є активними суб'єктами інформаційних процесів. Вони постійно здійснюють інформаційну діяльність з метою забезпечення суспільства ретроспективною інформацією, тобто створюють умови для всебічного використання відомостей, що містяться в документах Національного архівного фонду. Тож, ключовими напрямками організації якнайширшого доступу до інформації належить переведення в електронну форму довідкового апарату архівів та архівних документів, а також розвиток веб-сайтів архівів нашої держави, використання сучасних методів репрезентації соціально значущої ретроспективної документної інформації дозволять поглибити процеси їх організаційно-функціональних трансформацій у сучасному інформаційному середовищі, забезпечить надійне підґрунтя переходу до формування єдиного архівного інформаційного простору.

Мета статті. дослідити веб-сайт Державного архіву Кіровоградської області (далі – ДАКО) як документально-інформаційну систему та визначити його оптимальні характеристики.

Зовнішній вигляд кожного сайту є унікальним, проте в усіх сайтів можна знайти спільні за функціональністю частини. На будь-якому сайті першою відкривається головна сторінка. Її розробці приділяють особливу увагу, оскільки дослідження показали, що люди не здатні читати інформацію, що відображається на моніторі, так уважно, як книжки або журнали.

Порядком функціонування веб-сайтів органів виконавчої влади (у редакції

27.03.2015 р.)[1] визначено вимоги до структури та оформлення веб-сайту, встановлює порядок до інформаційного наповнення та шляхи забезпечення доступності користувачів (в т.ч. з вадами зору та слуху – на основній або альтернативній (за наявності) версії офіційного веб-сайту).

Зокрема, що стосується структури, то організація інформаційних матеріалів на веб-сайті має ієрархічну структуру, що передбачає розміщення даних на декількох рівнях в розділах сайту (на веб-сторінках). Усередині веб- сторінок допускаються упорядковані або окремі перехресні посилання на довільні рівні ієрархії, у залежності від тематичного зв'язку між даними. Такий взаємозв'язок становить гіперструктуру сайту і забезпечує максимальну прозорість його структури. Контроль за актуальністю гіперпосилань здійснюється програмно та візуально.

Загальна структура веб-сайту складається з: частини – найбільша одиниця розподілу сайту, що відповідає одному з головних об'єктів; розділу – сукупність даних та супутні їм елементи структури та дизайну, що відповідають окремій темі. Розділ може включати декілька сторінок; сторінки – окрема сукупність даних HTML-структури; елементів сторінки – фрейм, текст, таблиця, форма, зображення. Елементи сторінки є складовими частинами або "одноосібними" носіями блоків (елементів) інформації; документу – файл відмінної від HTML-сторінки структури, на який є посилання зі сторінок сайту.

На практиці, відкриті дані на веб-сайті ДАКО розподілені за наступними функціональними напрямками[2].

– Головна сторінка (на сторінці відображуються основні новини та події пов’язані з активністю ДАКО).

– Про архів (посилання містить інформацію про керівництво архіву, його структуру, основні завдання, фонди, історію створення та ін.).

– Нормативна база (за цим покликанням можна знайти Різного роду документи: положення, накази, методичні розробки, інструкції та ціни на послуги, що надає архів).

– Галузеві програми.

– Державні послуги (містить в собі перелік платних послуг, які можуть надаватися архівними установами, що утримуються за рахунок бюджетних коштів та порядок користування документами Національного архівного фонду України, що належать державі, територіальним громадам, у Державному архіві Кіровоградської області).

– Відкриті дані.

– Державні закупівлі.

– Регуляторні акти.

– Інформуємо громадськість (вкладка має посилання на вкладки: Плани; Звіти; Правила внутрішнього трудового розпорядку; Список юридичних осіб - джерел формування НАФ, які передають документи до Державного архіву Кіровоградської області; Графік особистого прийому громадян керівництвом; Перелік послуг, які надаються безоплатно та на умовах оплати Державним архівом Кіровоградської області; Архіви пропонують).

– Міжнародна діяльність.

– Запобігання проявам корупції (включає в себе рішення колегії, накази, заходи, звіти, інформації декларації про доходи та видатки, заходи щодо реалізації Закону України "Про очищення влади").

– Вакансії.

– Інтернет-приймальня (містить контактну інформацію, включаючи електронну адресу public@dakiro.kr-admin.gov.ua.).

– Звернення громадян (Містить посилання на нормативно-правові акти, Рішення колегії, Порядок організації роботи з проведення особистого прийому громадян у Держархіві області, Порядок виконання запитів у Державному архіві Кіровоградської області, Соціально-правові запити, Генеалогічні запити, Бланки заяв, Відомості про місцезнаходження документів ліквідованих та реорганізованих підприємств, установ та організацій.).

– Наші консультації.

– Доступ до публічної інформації (Система обліку публічної інформації, яка є у володінні державного архіву області, Нормативна база, Порядок оскарження рішень Державного архіву Кіровоградської області, дій чи бездіяльності, Розташування місця, де надаються необхідні запитувачам форми і бланки установи, Перелік видів публічної інформації, розпорядником якої є Державний архів Кіровоградської області);

– Розсекречення архівних документів

– Документальні виставки on-line.

– Публікації на порталі (Збірники наукових праць, Монографії, Документальні видання, Спеціальні довідники, Анотовані реєстри описів).

– Архіви у ЗМІ (Архіви на радіо і телебаченні, Публікації в пресі).

– Пам'ятні та знаменні дати Другої світової війни 1939-1945рр.

– Видатні особистості нашого краю.

– Архівні установи області.

Більша частина відкритих даних доступна не лише для перегляду, але і для експорту (як правило, в формат pdf, рідше – в xlsx).

Крім цього, головне меню сайту містить поле для користувацького пошуку, посилання на веб-сторінки з новинами (оновлюються кожного робочого дня) та інформацію про ДАКО, проте даний пошук фактично здійснюється лище за допомогою пошукової системи Google. Також на сайті є вбудована система перекладу для іноземних відвідувачів, дана іконка знаходиться у правому верхньому куті сайту.

Існують інструментальні засоби, які можуть допомогти у виявленні вразливостей в Web-сайтах та Web-додатках. Для автоматизованого пошуку використовують спеціальні програми - сканери безпеки і найбільш поширені наступні:

– xSpider – платний російський продукт з обмеженим доступом Сайт сканеру - http://www.ptsecurity.ru/ ;

– Shadow Security Scanner має специфічну побудову на основі інтелектуального ядра. Російський інтерфейс, але опис вразливостей англійською, шукає вразливості у серверному програмному забезпеченні. Сканер платний. Сайт сканеру http://montekidlo.org.ua/Shadow.Security.Scanner.v7;

– Acunetix Web Vulnerability Scanner 6 – в цей програмний комплекс входять сканер безпеки, пошуковий агент, інструмент аналізу повідомлень, а також пояснення Web-безпеки і розширена база даних перевірок безпеки для всіх поширених платформ Web-серверів. Основний недолік це дуже повільна робота. Так на сканування сайту середньої складності витрачається час більше 10 годин. Сайт сканеру - http://www.acunetix.com/vulnerability-scanner/ ;

– Nikto – швидкий безкоштовний сканер написаний на Perl. Працює майже у реальному часі. Із недоліків можна відмітити наявність помилкових спрацьовувань.

Сайт сканеру - http://cirt.net/nikto2 ; З безкоштовних сканерів доступними є Acunetix Web Vulnerability Scanner 6 та Nikto Хоча ці інструменти можуть забезпечити аудитору гарний огляд можливих вразливостей, вони не можуть замінити участь людини в їх оцінці. Є і недолік у наявності гарних сканерів, бо це ще й інструмент хакерів. Вони сканують необхідний їм сайт, знаходять вразливості, а потім втручаються на сайт.

Стратегія використання безкоштовних сканерів може бути наступною:

– Автоматичне сканування сайтів Порталу за допомогою швидкого сканеру;

– Збирання інформації отриманої від сканера;

– Розсилання отриманої інформації Web-майстрам сайтів Порталу Теоретичний матеріал по вразливостям сайтів та Web-сервісів, а також опис та інструкції використання відомих платних та безкоштовних сканерів зібрано авторами на Web-сайті http://dakiro.kr-admin.gov.ua/ . Для побудови сайту використано CMS Joomla, що надало можливість online та offline зв’язку з Web-майстрами сайтів ДАКО, крім цього надана можливість переписати безкоштовні сканери. Рекомендації для Web-майстрів та Web-програмістів зібрано та розміщено на Web-сайті у розділі “ Захист сайтів та їх безпека”.

Сайт користується послугами on-line сервісу для підрахунку відвідувань Kampyle (software), відповідні дані виводяться на головній сторінці сайту в лівому нижньому куті екрану (рис 1).

Рис 1. Відвідуваність сайту по країнам[2]

Статистика популярності веб-сайту, обсяги трафіку, географія аудиторії, ключові пошукові фрази можуть бути проаналізовані за допомогою даних компанії Aexa та PR-CY (таблиця 1).

Таблиця 1. Аналіз значимості сайту державного архіву Кіровоградської області за обраними показникамиhttp://dakiro.kr-admin.gov.ua/ (за даними компанії Aexa та PR-CY)[4]

Показник	Значення		
IP адреса, сервер	195.62.15.59, Україна		
Перегляди	День	Тиждень	Місяць
	2 508	17 556	75 240
Відвідувачі	День	Тиждень	Місяць
	627	4 389	18 807
Структура посилань	Внутрішні посилання	577	71,1%
	Зовнішні посилання	237	15,1%
Рейтинг у світі	331 166		
Рейтинг в Україні	2 859		
Географія аудиторії (за останні 30 днів)	Україна – 69,8% трафіку, Інші країни 30,2%		
Ключові слова	Фраза	Запитів в місяць	Позиція сайту в результатах пошуку
	Устинівка перше вересня20018	20,3%	9
	департамент екології Кіровоград	13,43	7
	ОДА	5,53	19
	Кіровоград обл.. держадміністрація	4,16	7
	кіровоградська область	22,83	10
Час, проведений на кожній сторінці сайту і в цілому на ньому	У цілому час, проведений на сайті – 00:02:14 Переглядів сторінок на одного відвідувача – 4		

Отже ми бачимо, що основною аудиторією сайту є Українці 69,8%, проте сайт також має значну популярність і серед web – користувачів Росії (9246 переглядів), США (4 227 переглядів), та Німеччини (1 130 переглядів), Ізраїль (835 переглядів). Проте досить дивними виглядають теги сайту по ключовим словам, що пов'язано з низькою клієнтоорієнтованістю організації. Так на приклад запит «Генеалогія Кропивницький» у пошуковій системі google лише за 4 покликанням адресує користувача на сайт http://dakiro.kr-admin.gov.ua/, та

абсолютно ігнорується те, що на карті сайту є покликання «Генеалогічні запити».

Основною проблемою подібного типу вкладок є те, що вони жодним чином не індексуються, оскільки, на практиці вони навіть не мають своєї окремої сторінки, в даному випадку, хоч на карті сайту є покликання на «Генеалогічні запити», але на практиці користувач опиняється на вкладці «Звернення громадян» http://dakiro.kr-admin.gov.ua/zap.php, дана проблема є масовою на сайті, і стосується як і переліку платних, безкоштовних послуг, та ін.

Слід зазначити, що веб-сайт Державного архіву Кіровоградської області був відмічений одним з найкращих (станом на 2016 р.) у дослідженні Л. Божук «Інформаційні ресурси і сервіси Інтернет в роботі державних архівів України»[3], зокрема за критерієм наявності власних сторінок в соціальних мережах для активного спілкування з представниками громадськості та інститутами громадянського суспільства, засобами масової інформації. Враховуючи, що важливим показником актуальності веб-сайтів державних архівних установ є своєчасне і оперативне поновлення інформації на власних сайтах, авторкою відмічено, що за досліджуваний період (2015-2016 рр.) понад 50% архівів оновлюють новини здебільшого лише раз на місяць, тоді як регулярне оновлення новин та анонсів на офіційних сайтах спостерігалося у «держархівах Волинської, Дніпропетровської, Закарпатської, Кіровоградської, Миколаївської, Одеської, Полтавської, Херсонської областей»[3].

Висновки. Отже, веб-сторінка ДАКО має чимало недоліків, проте переважна кількість недоліків пов'язана із специфікою роботи організації, та не достатньою зацікавленістю адміністрації в просуванні сайту. Також важливим недоліком у веб-дизайні офіційної сторінки ДАКО є його слабка адаптованість до перегляду з мобільних засобів екраном менш ніж 10 дюймів. Проте, слід зазначити, що подібні проблеми є типовими для сторінок обласних та центральних архівів в Україні.

З метою поліпшення удосконалення веб-сторінки ДАКО необхідно:

- Забезпечити доступ до інформації для користувачів з вадами зору та слуху з урахуванням вимог, як того вимагає діюче законодавство (Порядок оприлюднення у мережі Інтернет інформації про діяльність органів виконавчої влади, затвердженого постановою КМУ від 04.01.2002 р. N3).
- Інформація на офіційному веб-сайті ДАКО повинна залишатися доступною при відключеному дизайні офіційного веб-сайту, збільшеному розмірі шрифтів та на монохромному екрані.
- Елементи управління, які надають можливість користувачу змінити розмір шрифту, кольоровий контраст, розміщаються на початку кожної веб-сторінки альтернативної версії офіційного веб-сайту органу виконавчої влади, а за її відсутності – на початку кожної веб-сторінки основної версії.
- При використанні на веб-сайті ДАКО графічних кодів підтвердження при авторизації, повинен існувати звуковий аналог чи доступна текстова версія підтвердження авторизації.
- Сайт ДАКО повинен мати пошукову систему, інтегровану із системою пошуку Єдиного веб-порталу Державної архівної служби України. Для сайту пріоритетом є пошук на сайті, другий ступінь пріоритету – Єдиний веб-портал, третій - сайти відповідної тематики в УА-неті.
- Своєчасно поновлювати інформацію на всіх сторінках веб-сайту ДАКО.

Список літератури

1. Про порядок функціонування веб-сайтів органів виконавчої влади: Наказ Держкомітету інформ. політики, телебачення та радіомовлення України, Держкомітет зв'язку та інформатизації України від 25.11.2002р. №327/225. (редакція 27.03.2015). URL: https://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=z1022-02 (дата звернення 10.11.2019).
2. Веб-сайт ДАКО. URL: http://dakiro.kr-admin.gov.ua/ (дата звернення: 13.10.2019).

3. Божук Л. Інформаційні ресурси і сервіси Інтернет в роботі державних архівів України. Вісник Київського національного університету імені Тараса Шевченка. К., 2016. Вип.3 (130). С.14- 18. file:///C:/Users/admin/Downloads/VKNU_Ist_2016_3_5.pdf
4. Аналіз сайту. PR.CY. https://pr-cy.ru/ ; https://www.alexa.com/pro/ (дата звернення: 14.10.2019).

УДК 633

М. Кушніров, магістр гр. ЕО-18М
Л. Коломієць, доц.
Центральноукраїнський національний технічний університет

ЕКОЛОГІЧНА ОЦІНКА ДОЦІЛЬНОСТІ ВПРОВАДЖЕННЯ ПЕРЕРОБНИХ КОМПЛЕКСІВ ДЛЯ ОТРИМАННЯ БІОГАЗУ

Проаналізовано питання поширення технологій з використання відновних джерел енергії, можливість отрмання біогазу з місцевих відходів тваринництва та біомаси.
викиди, викопне паливо, відходи, вторинні енергетичні ресурси, біогаз, когенерація, електроенергія, органічне добриво

В умовах наростання потужностей світового господарства збільшується і кількість різноманітних забруднень навколишнього середовища. Викиди від промисловості погіршують стан атмосфери, скиди недостатньо очищених стічних вод забруднюють світовий океан, а відходи поглинають все більші території, до того ж забруднюючи все довкола через вертикальну та горизонтальну міграцію безлічі шкідливих речовин у складі багатокомпонентних сумішей ТПВ. Необхідні заходи із раціонального використання викопних видів палива, спалювання якого ще й значно забруднює довкілля, та пошук шляхів отримання альтернативної енергії. Деякі види відходів можуть стати цінною сировиною для видобутку останньої. Засадами сталого економічного і соціального розвитку є охорона довкілля, раціональне використання природних ресурсів та збереження екологічної безпеки життєдіяльності населення. Тому в Кіровоградській області провадиться екологічна політика, спрямовану на поліпшення стану довкілля шляхом впровадження екологічно збалансованої системи природокористування та збереження природних екосистем.

Актуальність. Актуальним на сьогодні є організація системи поводження з відходами, що передбачає першочергово їх сортування на місці утворення та подальшу своєчасну переробку в залежності від виду відходів з отриманням вторинної сировини або енергії. Відходи галузей рослинництва та тваринництва мають унікальний біохімічний склад, що дозволяє утилізувати їх з отриманням біогазу та цінного органічного добрива. При цьому вплив на довкілля когенераційних комплексів є мінімальний.

Мета дослідження. обгрунтувати доцільність впровадження комплексу із переробки відходів переробної галузі та тваринництва з отриманням біогазу та електроенергії.

Завдання: - вивчити стан довкілля в умовах нераціонального природокористування
- проаналізувати тенденції розвитку сучасної енергетики
- вивчити місцеві умови, в яких планується впровадження когенераційного комплексу.

Об'єкт дослідження: стан навколишнього середовища в умовах раціонального використання вторинної сировини.

Предмет дослідження: вирішення питання раціональної утилізації органічних відходів на території Капітанівської селищної ради.

Результати досліджень.

Світове господарство щорічно викидає в атмосферу більше 15 млрд.тонн вуглекислого газу, 200 млн. т оксиду вуглецю, понад 500 млн. т вуглеводнів, 120 млн. т золи та ін.

Загальний обсяг викидів забруднюючих речовин в атмосферу становить більше 19 млрд. т.

Основними забруднюючими речовинами, які надходять в атмосферу при спалюванні палива, є тверді частинки (зола, сажа), оксиди сірки (SO2 і SO3), оксиди азоту (NO і NO2). При неповному згорянні палива в газоподібних викидах можуть накопичуватися оксиди вуглецю (CO), вуглеводні типу CH4, C2H4, поліциклічні ароматичні вуглеводні, бензапірен (C20H12), а також п'ятиокис ванадію (V2O5). Останні дві сполуки належать до класу надзвичайно небезпечних. Діоксид (SO2) і триоксид (SO3) сірки є головними компонентами забруднення природного середовища при спалюванні палива [1].

Для оптимізації стану атмосферного повітря необхідно впровадження нових прогресивних технологій виробництва, планування заходів зі зменшення обсягів викидів забруднюючих речовин в атмосферу, переведення котелень на альтернативні види палива.

Ряд підприємств, відповідно до заходів щодо скорочення викидів забруднюючих речовин та терміну виконання, передбачених у дозволах на викиди, проводять модернізацію пилогазоочисних установок, встановлюють циклони, підвищують ступені очищення на джерелах викидів, здійснюють заміну пилогазоочисного обладнання, розробляють та встановлюють додаткові системи очищення.

Хімічний склад викидів забруднюючих речовин в атмосферу у 2016 р. характерний такому і в попередні роки, оскільки напрямки промислового використання та технології залишаються майже незмінні (табл.1). [2,3]

Таблиця 1 - Хімічний склад викидів забруднюючих речовин, %, 2018р.

Речовини у вигляді твердих суспендованих частинок	34,00
Оксид вуглецю	18,60
Сполуки азоту	13,30
Діоксид сірки	7,00
Метали та їх сполуки	2,73

Зростання надходжень токсичних речовин у навколишнє середовище, перш за все, впливає на здоров'я населення, погіршується якість продуктів сільського господарства, відбувається вплив на клімат окремих регіонів і стан озонового шару землі, загибель флори і фауни. Оксиди вуглецю, що поступають в атмосферу, сірки, азоту, вуглеводні, пил і так далі мають різну токсичну дію на організм людини.

В Кіровоградській області основними забруднювачами атмосферного повітря були і залишатимуться ще тривалий час підприємства енерго- та теплозабезпечення, а також виробництва будівельних матеріалів. На них припадає понад 70% усіх викидів оксиду азоту, сполук сірки, пилу та вуглеводнів (табл.2). Внаслідок порушень технологічного процесу можуть відбуватися аварійні викиди шкідливих речовин.

Таблиця 2 – Середні та максимальні концентрації забруднюючих речовин (в кратності ГДК) в атмосферному повітрі міст

Назва забруднюючої речовини	ГДК, мг/м^3	Середня концентрація, мг/м^3	Максимальна з разових концентрацій, мг/м^3
Кропивницький			
Пил	0,5	1,9	1,2
Розчинні сульфати	-	0,4	0,1
Діоксид азоту	0,2	0,8	0,35
Оксид вуглецю	5,0	0,6	1,0

Формальдегід	0,035	1,4	0,3
Діоксид сірки	0,5	0,4	0,1
Оксид азоту	0,4	0,3	0,1
Сажа	0,15	0,7	1,3
Олександрія			
Пил	0,5	1,7	1,2
Розчинні сульфати	-	0,4	0,1
Діоксид сірки	0,5	0,4	0,1
Діоксид азоту	0,2	0,8	0,35
Сажа	0,15	1,2	1,3
Світловодськ			
Пил	0,5	0,47	0,6
Діоксид сірки	0,5	0,22	0,2
Оксид вуглецю	5	0,33	0,6
Діоксид азоту	0,2	0,07	0,7
Оксид азоту	0,4	0,66	0,4
Формальдегід	0,035	0,66	1,01

У сучасному світі спостерігається стійка тенденція до розвитку відновлюваних джерел енергії (ВДЕ) та поступового заміщення ними традиційних джерел, адже тільки так можна знизити рівень забруднення довкілля. У 2015 році світові інвестиції у ВДЕ склали 349 млрд.дол., а частка відновлюваної енергетики у нововстановлених потужностях у світі вперше склала понад 50%.

У ЄС даний показник за підсумками 2016 року склав 87%. Факт надходження рекордних інвестицій та стрімкий розвиток ВДЕ відбуваються сьогодні, незважаючи на найнижчі за 13 років ціни на нафту та газ, що підтверджує незворотність переходу до відновлюваних джерел енергії у світі. Це особливо важливо в ракурсі екологічної оцінки впливу людини на довкілля протягом останніх століть надзвичайно потужної експлуатації природних сировинних та енеретичних ресурсів [4-6].

Приблизно з 2012 року в Україні спостерігається поступове зростання встановлених потужностей ВДЕ, але складна економічна ситуація в країні сьогодні не сприяє досягненню цілей, прийнятих у Національному плані дій з відновлюваної енергетики, по досягненню 11% частки ВДЕ у енергоспоживанні. Станом на кінець 2016 ріку встановлено 1117 МВт потужностей ВДЕ, які виробляють близько 1% у загальному обсязі відпущеної електроенергії. Найбільшу частку серед ВДЕ в Україні займають вітрові та сонячні електростанції, на яких у 2016 році було вироблено 925 ГВт*год та 492 ГВт*год електроенергії відповідно.

Економічно-доцільний потенціал впровадження ВДЕ в Україні станом на 2030 рік оцінюється у 16-22 ГВт, в порівнянні з 1,1 ГВт, що фактично встановлені на кінець 2016 року. Потенціал впровадження ВДЕ в теплоенергетиці навіть більший, та за оцінками експертів може повністю замістити традиційні джерела енергії, що включають викопні види палива, природний газ і т.п., - до 2030 року. Так, за оцінками IRENA, у 2030 році з ВДЕ може бути вироблено близько 57 млн. Гкал теплової енергії, з яких значна частка (32,7 млн Гкал) – біомаса. Виконання даного прогнозу дозволить економити близько 7 млрд. м3 природного газу щороку.

За умови стабільного економічного та політичного середовища, та покращення умов фінансування проектів ВДЕ, Україна зможе значною мірою модернізувати та забезпечити енергонезалежність електричної та теплової генерації за рахунок технологій відновлюваної енергетики. Світові інвестиції у відновлювану енергетику мають позитивну динаміку росту. Так, у період із 2004 по 2016 роки середньорічний приріст інвестицій склав 12,5%. Абсолютний рекорд було встановлено у 2015 році, коли об’єм інвестицій у відновлювані джерела енергії склав 349 млрд. дол., у той час, коли світові ціни на нафту перебували майже на історичному мінімумі.

2015 рік також відомий тим, що вперше в історії у структурі нових встановлених енергетичних потужностей у світі частка відновлюваних джерел енергії зайняла більшість та склала 54%, підкресливши довгостроковий загальносвітовий тренд переходу від традиційної генерації до ВДЕ. У період з 2007 по 2015 рік частка ВДЕ у встановлених енергетичних потужностях та у виробництві енергії у світі зросла вдвічі.

Біоенергетика – галузь енергетики, заснована на використанні біопалива, яке виробляється з біомаси, - має стійке положення серед інших альтернативних галузей паливної енергетики, використовується на Україні та у світі віддавна, а нині має на озброєнні багато сучасних розробок та технологій використання [7,8].

У структурі встановлених електроенергетичних потужностей в Україні вугільна генерація (ТЕС та ТЕЦ) займає більше 50%. Найменшу частку займають ВДЕ ~2%. Загальний тренд виробництва електроенергії в Україні має тенденцію до скорочення – на ~14% за останні 3 роки. Найбільшу частку у виробництві займають АЕС – 54% всієї електроенергії в Україні в 2016 році, тоді як ТЕС мають частку у 32%. При цьому, з 2013 року відбулися певні зміни у структурі виробництва електроенергії – частка АЕС зросла на 10% та частка ТЕС скоротилася на 8%. Такі зміни зумовлені проблемами поставок вугілля, основне місце видобування якого (Донбас) досі знаходиться у зоні АТО.

Альтернативні джерела в Україні виробляють лише ~1% всієї електроенергії. Найбільшими споживачами електроенергії є промислові підприємства, які споживають 42% електроенергії в Україні. Зокрема найбільша частка споживання у промисловості припадає на підприємства металургійної галузі – 58% від споживання промисловістю або 25% від загального в Україні.

Наступним за величиною споживачем після промисловості є населення із часткою у 30%. Більша частина матеріально-технічної бази наявних потужностей з виробництва електроенергії в Україні зношена та неефективна. За даними Інституту відновлюваної енергетики НАН України, атомні блоки наближаються до закінчення строку проектної експлуатації. Понад 70% атомних блоків потребуватимуть подовження строку експлуатації у найближче десятиліття. Крім того, 42,2% ЛЕП напругою 220-330 кВт експлуатуються більш ніж 40 років, а 64,4% основного устаткування трансформаторних підстанцій випрацювали свій розрахунковий технічний ресурс. Недостатньою на сьогодні є пропускна спроможність ліній електропередач для видачі потужності АЕС і передачі надлишкової енергії. У розподільчих мережах значна кількість об'єктів також відпрацювала свій ресурс: 40,5% електричних мереж і 37,6% трансформаторних підстанцій потребують реконструкції або заміни.

За даними НКРЕКП станом на кінець 2016 року галузь ВДЕ в Україні налічує вже 170 компаній та 291 об’єкти енергетики. Протягом 2016 року найбільший приріст продемонструвала сонячна енергетика – 36 нових суб’єктів і 47 нових об’єктів електрогенерації.

Потужність об’єктів енергетики, що виробляють електроенергію з біомаси, протягом 2013-2016 років збільшилась в 6,5 разів. Найбільше потужностей було введено в експлуатацію у 2013 та 2014 роках – 11 та 18 МВт, відповідно. Проте протягом останніх двох років проекти з біомаси майже не реалізовувались і в 2016 році в секторі було введено лише одну електростанцію потужністю 3,5 МВт. Виробіток електроенергії з біомаси виріс у 2.5 рази за останні 4 роки. У 2016 році станції на біомасі відпрацювали на повну потужність 2 051 годину, що відповідає коефіцієнту використання встановленої потужності у 23.4% [9,10].

Як свідчить досвід розвинених країн, органічні відходи доцільно переробляти, зокрема отримувати теплову енергію, та використовувати її на власні потреби, або перетворювати на електроенергію. Крім того, значні відстані перевезення підвищують небезпеку забруднення довкілля внаслідок розливів нафти та нафтопродуктів. Це погіршує стан грунту та води, викликає необхідність вартісних заходів з очищення, ліквідації забруднення та його наслідків. Знижується біорізноманіття, стійкість екосистем. Врешті екологічні наслідки цих порушень проявляються погіршенням здоров’я людини, що

викликає збільшення видатків на медицину. Для збереження генофонду людської популяції важливо у всіх галузях дотримуватися принципу природоподібних технологій, раціонального використання природної сировини, гармонійного впливу на довкілля. Вклавши кошти в довгострокову перспективу збереження навколишнього природного середовища, ми робимо безцінний вклад в гарантії благополучного існування людства на планеті, та якісного середовища життя для прийдешніх поколінь.

Галузь тваринництва забезпечує населення різноманітними, поживними та смачним продуктами харчування. Зокрема птахівництво чинить значний тиск на довкілля, спричиняючи утворення відходів, викидів, стічних вод та забруднення грунту. Щоб знизити несприятливі прояви, необхідно налагоджувати локальну систему поводження з відходами. Тому розглянемо модель побудови біогазової установки для птахофабрики, що утворює 100 т відходів щоденно.

Спільно з робочою групою ТОВ «ПВІ «Миколаївагропроект» на замовлення ТОВ «АФ ім. Чкалова» нами на території Капітанівської с/ради, що в Новомиргородському районі Кіровоградської обл. було проведено визначення доцільності планової діяльності з будівництва та експлуатації комплексу по переробці органічних відходів (продуктів життєдіяльності тваринництва, відходів цукрового виробництва і т.п.) в біогаз з послідуючою трансформацією в електричну, або використання теплової енергії; та розробка проектної документації комплексу когенерації [11].

Згідно даних проектної документації, вартість будівництва та пусконаладочних робіт біогазової установки, здатної переробляти відходів у обсязі 100 т/добу, складає 275764,222 тис.грн., технічні показники підприємства наведено в таблиці 3.

Таблиця 3 – Характеристики роботи біогазової установки

№п/п	Характеристики	Розмірність	Значення		
1	Продуктивність переробки сировини	т/добу	20	100	200
2	Вихід біогазу	$м^3$/добу	2600	13000	26000
3	Споживана електроенергія	кВт*год.	16	60	100
4	Споживана теплова енергія	кВт*год.	54	60	100
5	Обслуговуючий персонал	осіб	1	2	2
6	Площа, яка відводиться під об’єкт	га	0,20	0,50	0,65
7	Вихід твердих добрив	т/добу	10	50	100
8	Вихід рідких добрив	$м^3$/добу	7	35	70

Біогаз, згідно даних, підтвердженим Державним агентством з енергоефективності та енергозбереження України (електронний ресурс http://saee.gov.ua/uk/ae/bioenergy), - отриманий з відходів птахівництва, містить біля 70% метану, отже, чистого газу, придатного до спалювання, із кожних 100 т сировини, що дає 1300 $м^3$ біогазу, отримаємо 9100 $м^3$.

Розрахуємо собівартість виготовлення біогазу. Річні витрати на виробництво біогазу становитимуть 2100 тис. грн./рік, термін експлуатації установки 15 років. Протягом року установка може виробити 4745 тис.м3 метану, що відповідає 33215 тис.м3 природного газу в тепловому еквіваленті (теплоутворююча спроможність 1 м3 біогазу – 7 кВт):

4745 тис.м3 * 7 кВт = 33215 тис.м3

В розрахунковий період приймаємо вартість природного газу 6950 грн. за 1000 м3.

Вартість тепла та енергії, отриманого із біогазу, складе 230844,250 тис.грн.:

33215 тис.м3 * 6,95 грн./м3 = 230844,250 тис.грн.

Тоді собівартість газу (витрати, розділені на кількість отриманого газу за рік) складе 63 грн./1000 м3:

2100 тис.грн. / 33215 тис.м3 = 63 грн./ 1000 м3 газу

Виконаємо оцінку економічної ефективності переробки відходів птахівництва, прийнявши, що споживання газу птахофабрикою складає 1400 тис.м3 за рік.

Всього з відходів птахофабрики отримуємо 33215 тис.м3 /рік біогазу.

На потреби птахофабрики використовується 1400 тис. м3 /рік, для обігріву біореактора потрібно 219 кВт*год. /рік, це 26,7 м3/добу, а за рік:

26,7 м3 * 365 = 9745,5 м3/ рік

Разом на власні потреби підприємство використовує:

1400 тис. м3 /рік + 9745,5 м3/ рік = 149745,5 м3 /рік.

Решту біогазу можна реалізувати споживачам за ринковою ціною.

33215 тис.м3 /рік - 149745,5 м3 /рік = 33065254,4 м3 /рік

33065254,4 м3 /рік * 6,95 грн. /м3 = 229803,518 тис.грн. /рік

Згідно даних проекту звіту з ОВНС, - інвестиції на будівництво, монтаж біогазової установки, сюди ж входить проектна документація, вартість обладнання та інші витрати складають 275764,222 тис.грн.

Окупність впровадження біогазової установки згідно проектних розрахунків складе 1,2 роки:

275764,222 тис.грн. / 229803,518 тис.грн. /рік = 1,2 роки.

Впроваджуючи біогазові установки, досягається значна економія вичерпних природних енергетичних ресурсів, зводиться до мінімуму забруднення повітря, води та грунту, отримуються цінні екологічно безпечні добрива для галузі рослинництва, яка забезпечує поступання кормів та продуктів харчування, не виникає потреба у відведенні нових площ під нагромадження відходів.

Висновок. Використання вторинних енергетичних ресурсів дозволяє зекономити природну енергетичну сировину, яка не відновлюється (нафти, газу, горючих сланців, торфу), а запаси останньої стрімко знижуються. Зважаючи, що для різних виробництв, в різних географічних умовах і т.д. всі енергоресурси не є однаково доступними і доцільними у використанні, для людства важливо зберегти якомога на довший час запаси всіх видів енергії, та використовувати їх комбінуючи, поєднуючи, або надаючи перевагу в залежності від кожних конкретних обставин. Так, якщо на певній території є запас або джерело якихось місцевих енергетичних ресурсів для виробництва біогазу зокрема, - первинних, чи вторинних, в першу чергу варто скористатися саме ними. Адже витрати на транспортування чи доставку палива можуть бути економічно невигідними через територіальну віддаленість. Таким чином, використовуючи вторинну енергетичну сировину, підприємство забезпечує власні потреби, реалізовує надлишок, отже після настання періоду окупності – 1,2 роки, - вже матиме прибуток, тобто досягається еколого-економічний ефект проведених заходів.

Список літератури

1. Заверуха Н. Основи екології: Навчальний посібник для вищих навчальних закладів/ Нелі Заверуха, Валентин Серебряков, Юрій Скиба,. - К.: Каравела, 2006. - 365 с.
2. Екологічний паспорт Кіровоградської області (2015 р.) – 87 с.
3. Регіональна доповідь про стан навколишнього природного середовища Кіровоградської області у 2016 році. - 2017 р.
4. Клименко В. В., Кравченко В. І., Боков В. М., Гуцул В. І. Технологічні основи виготовлення біопалива з рослинних відходів та їх композитів: Монографія. /За ред. В.В. Клименка – Кропивницький: ПП «Ексклюзив-Систем», 2017. – 162 с.
5. Бабієв Г.М., Дероган Д.В., Щокін А.Р. Перспективи впровадження нетрадиційних та відновлюваних джерел енергії в Україні. // ЕЛЕКТРИЧНИЙ Журнал,- Запоріжжя: ВАТ "Гамма",1998 №1, - С.63-64.
6. «Розвиток відновлюваних джерел енергії в Україні». - Звіт Міністерства регіонального розвитку, будівництва та житлово-комунального господарства України.- березень 2016 р. – 36
7. Нестеренко Е.В. Применение биогазовых технологий при утилизации органических отходов/ Е.В. Нестеренко // Науковий вісникбудівництва. 2009. –No.52. [Електронне видання]. –Режим доступу. – http://www.nbuv.gov.ua/old_jrn/natural/Nvb/2009_52/nesterenko.pdf. –(дата звернення: 12.07.2016).
8. Г. Кант «Біологічне рослинництво: можливості біолого-динамічних систем» (1986). - 234с.
9. Поводження з відходами тваринництва: переваги технології анаеробного зброджування / Національний екологічний центр України. –Київ.–2015. –24 с.
10. Методика узагальненої оцінки технічно–досяжного енергетичного потенціалу біомаси. –К.: Тов. «Віол–принт». –2013. –25 с.
11. Проект звіту «Комплекс по переробці органічних відходів (посліду, силосу та жому цукрового буряка) в біогаз з виробництвом електричної, та теплової енергії».: ТОВ «ПВІ «Миколаївагропроект». – 2018. – 57 с.
12. Дероган Д.В., Щокін А.Р. Перспективи використання енергії та палива в Україні з нетрадиційних та відновлюваних джерел.//Бюл. "Новітні технології в сфері нетрадиційних і відновлюваних джерел енергії", Київ: АТ "Укренергозбереження",1999.- №2, - С.30-38.

УДК 338.47

К. Лубцова, магістр гр. АДМ-18М-1,4
Центральноукраїнський національний технічний університет

РОЗВИТОК ПІДПРИЄМСТВ ДОРОЖНЬОЇ ГАЛУЗІ УКРАЇНИ: СТРАТЕГІЧНІ ПРІОРИТЕТИ

В статті розглянуті актуальні питання стратегічного розвитку підприємств дорожньої галузі України в сучасних економічних умовах, визначено чинники, що гальмують розвиток підприємств дорожнього господарства України. Запропоновано стратегічні пріоритети розвитку підприємств дорожньої галузі. Визначено, що згідно стратегічного підходу оцінка ефективності реалізації управлінських заходів з підвищення конкурентоспроможності дорожнього підприємства реалізується за внутрішніми факторами стратегічного середовища.

підприємство, дорожнє господарство, стратегічні пріоритети, державна політика

Постановка проблеми. В сучасних важливим чинником, що визначає соціально-економічний розвиток та економічну безпеку країни, є транспорт, зокрема його інфраструктура. Сьогодні галузь транспорту загалом задовольняє потреби української економіки та населення у перевезеннях, проте дорожнє господарство є недостатньо розвиненим, що є перешкодою на шляху відновлення економічної активності та виведення економіки України на траєкторію сталого зростання.

Тому дослідження питання інноваційного розвитку підприємств дорожньої галузі України є актуальними з теоретичної і практичної точки зору.

Аналіз останніх досліджень і публікацій. Питання діяльності підприємств

дорожнього господарства досліджують у своїх працях Є. Луцкін, В. Семесько, В. Галушко та інші.

Але, не дивлячись на значну кількість наукових праць, присвячених даній тематиці, питання удосконалення стратегічного управління розвитком підприємств дорожньої галузі України залишаються актуальними.

Мета статті. Метою написання даної статті є дослідження стратегічних пріоритетів розвитку підприємств дорожньої галузі України в сучасних умовах.

Виклад основного матеріалу. В Україні державну політику у сфері дорожнього господарства реалізує Державне агентство автомобільних доріг України (Укравтодор), діяльність якого спрямовується і координується Кабінетом Міністрів України через Міністра інфраструктури. Її належна реалізація потребує професійних ресурсів та навичок як стратегічного планування та розробки політики, так і управління суб'єктами господарювання державного сектору економіки. Проте наявна система управління дорожньою галуззю України має низку недоліків, основними з яких є зосередження всіх функцій з планування і організації ремонтно-будівельних робіт на місцевих дорогах в Укравтодорі; суміщення критичних повноважень (замовник – виконавець – контролер); фактична монополізація ринку робіт з експлуатаційного утримання автомобільних доріг загального користування державною компанією акціонерне товариство «ДАК «Автомобільні дороги України»», що приводить до відсутності конкуренції; неврахування інтересів та пріоритетів соціально-економічного розвитку регіонів; відсутність можливості органам місцевого самоврядування впливати на планування ремонтно-будівельних робіт на місцевих дорогах.

Однією з ключових проблем розвитку вітчизняного автодорожнього господарства залишається проблема фінансування ремонтних і будівельних робіт у цій сфері. В цілому, фінансування діяльності дорожнього господарства відбувається згідно з Законом України «Про джерела фінансування дорожнього господарства України», який передбачає створення Дорожнього фонду з наступним розподілом бюджетного фінансування: 60% – фінансове забезпечення будівництва, реконструкції, ремонту і утримання автомобільних доріг загального користування державного значення, а також виконання проектно-вишукувальних та науково-дослідних робіт; 35% – фінансове забезпечення будівництва, реконструкції, ремонту і утримання автомобільних доріг загального користування місцевого значення, вулиць і доріг.

Характер, зміст і спрямованість діяльності дорожнього підприємства визначаються збалансованістю інтересів безпосередніх учасників процесу стратегічного управління, що знаходить своє відображення у вигляді певної місії і цілей. При цьому, перший крок полягає у формулюванні місії, яка є засобом вираження сутності існування підприємства, його призначення та має свою оригінальність і особливе значення для працівників.

Через те, що перед підприємством майже щоденно постають усе нові й нові завдання, життєвий цикл місії завжди обмежений у часі. Аналіз середовища забезпечує базу для вироблення стратегії та дозволяє підприємству здійснити свою місію і досягти своїх цілей. На даному етапі задачею стратегічного управління розвитком є підтримка балансу взаємодії підприємства з зовнішнім середовищем, що, виходячи з принципів системного підходу, знаходить відображення у трьох процесах:

- отримання ресурсів із зовнішнього середовища – вхід (для дорожнього підприємства – матеріальні,

трудові, техніко-технологічні, фінансові ресурси та ресурси управління для будівництва, ремонту та експлуатації автомобільних доріг);

- перетворення ресурсів в продукт – перетворення (для дорожнього підприємства – реалізація технологічного процесу будівництва, ремонту та експлуатації автомобільних доріг);

- передача продукту в зовнішнє середовище – вихід (для дорожнього підприємства – збудовані, реконструйовані, відремонтовані та існуючі на належному рівні автомобільні дороги).

Аналіз зовнішнього середовища спрямований на з'ясування перспективних позитивних результатів, що можуть бути досягнуті підприємством у випадку успішного виконання стратегічних дій та прогнозування можливих ускладнень в результаті невизначеності зовнішніх факторів. Аналіз включає вивчення впливу економічної, правової, політичної, екологічної, соціальної, науково-технічної й технологічної складових суспільства на стан розвитку підприємств дорожньої галузі країни загалом.

Аналіз внутрішнього середовища розкриває конкурентний потенціал дорожнього підприємства, що є дієвим у процесі досягнення визначених цілей, і проводиться за такими напрямами: організація управління; характеристика процесу виробництва; рівень інноваційного потенціалу; рівень кадрового потенціалу; фінанси; маркетинг; організаційна культура тощо.

Висновки. Сьогодні актуалізується проблема використання таких інструментів стратегічного менеджменту як стратегічний моніторинг та аналіз стратегічного середовища (зовнішнього, безпосереднього або проміжного, внутрішнього), діагностика стану підприємства. Оцінка ефективності реалізації обраних управлінських заходів з удосконалення стратегії підвищення конкурентоспроможності дорожнього підприємства реалізується за групами внутрішніх факторів стратегічного середовища, які найбільш суттєво здійснюють вплив на процес формування конкурентоспроможності підприємства. Урахування зовнішніх факторів стратегічного середовища відбувається на етапі визначення цілей управління конкурентоспроможністю дорожнього підприємства та етапі вивчення структури підрядного ринку.

Комплексний підхід до вирішення проблем дорожнього господарства дозволить оновити основні фонди підприємств дорожнього комплексу і, відповідно, підвищить їх конкурентоспроможність як на українському ринку, так і за кордоном. Національна транспортна стратегія України на період до 2030 року передбачає вирішення частини з цих проблем, але цей процес знаходиться на початковому етапі та є підґрунтям для подальших досліджень.

Список літератури

1. Асаул А. Н. Формирование конкурентного преимущества субъектов предпринимательства в строительстве / А. Н. Асаул, Ш. М. Мамедов, Е. И. Рыбнов, Н. В. Чепаченко; Под ред. А. Н. Асаула. СПб.: АНО «ИПЭВ», 2014. 240 с.
2. Галушко В.О. Проблеми та перспективи розвитку дорожньої галузі / В.О. Галушко // Дорожня галузь України. – 2011. – № 2. – С. 12-15.
3. Гевлич, Л. Л. Стратегічна діагностика підприємства : монографія / Л. Л. Гевлич. – Донецьк : Юго-Восток, 2007. – 199 с.
4. Дергаусов М. Особливості транспортної політики в Україні при її адаптації на міжнародних ринках // http://www.vesna.org.ua.
5. Костевко В. І. Методологічні питання оцінювання ефективності інноваційної діяльності підприємства / Костевко В.І. // Вісник Національного університету "Львівська політехніка". Проблеми економіки та управління. – 2011. – № 698. – С. 66 – 73.
6. Кулицький С. Проблеми розвитку мережі автомобільних доріг в Україні [Електронний ресурс] / С. Кулицький // Україна: події, факти, коментарі. – 2017. – № 22. – С. 56–65. – Режим доступу: http://nbuviap.gov.ua/images/ukraine/2017/ukr22.pdf. – Назва з екрану.
7. Лігоненко, Л. О. Антикризове управління підприємством: теоретико-методологічні засади та практичний інструментарій : монографія / Л. О. Лігоненко. – К. : Київ. нац. торг.-екон. ун-т, 2001. – 580 с.
8. Луцкін Є. С., Серьогіна Н. В. Основні проблеми та можливості розвитку дорожньо-транспортної інфраструктури України. Вісник ОДАБА. 2016. № 63. С. 223-229. : сайт. URL : http://mx.ogasa.org.ua/handle/123456789/2108 (дата звернення : 01.12.2019).
9. Мельник, О. Г. Інноваційні системи економічної діагностики підприємства на засадах індикаторів / О. Г. Мельник, І. Б. Олексів, Н. Ю. Подольчак, Р. В. Шуляр. – Львів : Магнолія. – 2009. – 241 с. 4. Савицкая, Г. В. Анализ хозяйственной деятельности предприятий / Г. В. Савицкая. – Минск : Новое знание, 2001. – 688 с.
10. Овсюк М.О. Удосконалення методів конкурентоспроможності будівельного підприємства в умовах кризи / М.О. Овсюк // Науковий журнал «Бізнес Інформ». –2011. – № 6. – С. 65-67.

11. Семеcько В. М. Аутсорсинг і перспективи розвитку транспортної логістики / В.М. Семеcько // Економіка та держава. – 2006. – №1. – С. 57–59.
12. Сокиринська, І. Г. Діагностика фінансового забезпечення діяльності підприємства / І. Г. Сокиринська // Фінанси України. – 2003. – № 1. – С. 88–95.
13. Хома, І. Б. Формування та використання систем діагностики економічної захищеності промислового підприємства : монографія / І. Б. Хома. – Львів : Видавництво Національного університету «Львівська політехніка», 2012. – 504 с.
14. Якименко Н. В. Необхідність створення торгово–транспортних логістичних центрів в сучасних умовах господарювання / Н.В. Якименко // Вісник економіки транспорту і промисловості: Зб. наук. праць. – Харків: УкрДАЗТ, 2007. – №20. – С. 132–136.

УДК 657

А. Михайлишин, магістр гр. ОО-18М
А. Бондаренко, магістр гр. ОО-18М
Центральноукраїнський національний технічний університет

ПЕРСПЕКТИВИ РОЗВИТКУ ОБЛІКУ НЕОБОРОТНИХ АКТИВІВ ТА ВИТРАТ БЮДЖЕТНИХ УСТАНОВ

У статті досліджено необоротні активи та витрати як об’єкти бюджетного обліку. Окреслено проблеми та визначені напрями їх розв’язання стосовно обліку і оподаткуванню операцій з необоротних активів та обліку і контролю витрат в бюджетній сфері.
необоротні активи, бюджетна сфера, оподаткування, витрати, амортизація

Постановка проблеми та її актуальність. Необоротні активи бюджетних установ є однією з найбільш вагомих складових нефінансових активів. У структурі активів бюджетних установ нефінансові активи посідають значну питому вагу (70 – 95%), при цьому переважно вони представлені саме необоротними. До складу необоротних активів входять основні засоби, інші необоротні матеріальні активи, нематеріальні активі (НА), довгострокові біологічні активи, капітальні інвестиції та інвестиційна нерухомість. В умовах реалізації Стратегії модернізації системи бухгалтерського обліку та фінансової звітності в державному секторі перманентно оновлюється чинне законодавство з регулювання обліку, що безпосередньо стосується і необоротних активів. По операціях з необоротними активами виникають податкові наслідки. Податкове законодавство за цим сегментом характеризує наявність проблемних моментів та суперечливість.

Зважаючи на постійний дефіцит коштів у бюджетній сфері важливо забезпечити систему обліку та контролю максимально спрямовану на зростання ефективності витрат. У цьому контексті інформаційне забезпечення витратами, що забезпечується ефективною системою обліку та перманентного контролю.

Аналіз останніх досліджень і публікацій. Проблеми обліку і оподаткування необоротних активів викликають особливий інтерес у представників економічної науки. Значний внесок у формування теоретичних основ та розробку підходів до проблеми обліку і оподаткуванню необоротних активів, їх використання здійснили такі вчені-економісти: П.Й. Атамас, М.Т. Білуха, Ф.Ф. Бутинець, Н.Г. Виговська, З.В. Гуцайлюк, З.В. Задорожний, Г.Г. Кіреєйцев, В.Г. Козак, Я.Д. Крупка, А.М. Кузьмінський, Б.М. Литвин, Н.М. Малюга, М.С. Пушкар, В.С. Рудницький, П.Т. Саблук, В.В. Сопко, Л.К. Сук, Н.М. Ткаченко, І.Д. Фаріон, П.Я. Хомин, Б.Ф.Усач та інші.

Проблематики оподаткування, зокрема податкових наслідків по операціях з необоротними активами, присвячені праці таких фахівців як І. Назарбаєва, О. Куліба, Л. Швець та ін.

Розробки науковців мають велику цінність для економічної науки, але у переважній більшості їхні дослідження спрямовані на розроблення загально-методичного забезпечення бухгалтерського обліку та оподаткування і не враховують специфічних умов функціонування необоротних активів бюджетних установ. З огляду на це потребує подальшого дослідження проблематика обліку та оподаткування необоротних активів.

Не зважаючи на значний доробок вітчизняних та закордонних науковців подальше дослідження сутності витрат установ державного сектору, як об'єкту управління та проблематика інформаційного забезпечення управління має суттєве значення як у теоретичному аспекті так і стосовно необхідності вирішення методичних питань на рівні суб'єктів державного сектору.

Метою статті є з'ясування проблемних аспектів обліку та оподаткуванню операцій з необоротних активів та витрат як об'єктів бюджетного обліку

Виклад основного матеріалу. Термін «Необоротні активи» використовується як фахівцями так і науковцями у різних сферах, зокрема управлінській, фінансовій, обліковій. Спостерігається наявність неоднозначних підходів до трактування цієї категорії. Ми погоджуємось з науковцями які вважають, що важливим є забезпечення єдності трактування загальних термінів, що застосовуються. Саме це сприяє гармонічному розвитку економічної системи. Як економічна категорія необоротні активи представлені у різних джерелах. Так Вікіпедія надає таке визначення: необоротні активи - це сукупність майнових цінностей, які багаторазово беруть участь у процесі господарської діяльності підприємства. Таке визначення зводить необоротні активи лише до матеріальних, хоча при наданні прикладів необоротних активів до їх складу відносять і фінансові і нематеріальні активи. Вважаємо, що таке визначення є некоректним.

В зарубіжній обліковій практиці поняття «необоротні активи» позначаються різними термінами: постійні активи; власність, споруди та обладнання; матеріальні постійні активи, довгострокові, капітальні (неліквідні) тощо. Так, в Швейцарії довгострокові активи в активі балансу об'єднані в єдину групу – основні засоби; в Німеччині – основний капітал та фінансові активи; в Естонії – основне майно (довгострокові фінансові інвестиції, матеріальне основне та нематеріальне майно). В англомовних країнах – це довгострокові активи. [1 с 55]

У Великобританії та в Австралії всі довгострокові активи в балансі представлені в розділі «Основний капітал», який складається з нематеріальних і матеріальних активів та інвестицій.

У сучасній економічній літературі термін необоротні матеріальні активи трактують неоднозначно. У словнику іноземних слів, за редакцією І.В. Лехіна та інших представлено більш широке трактування поняття «необоротні матеріальні активи» та наведено різні підходи:

частина засобів виробництва, що беруть участь у створенні продукту протягом кількох виробничих циклів. При цьому за один виробничий цикл вони втрачають лише частину своєї вартості, зберігаючи свою натуральну-речову

форму;

різноманітні верстати, механізми, інструменти, двигуни, тощо, тобто це ті засоби, за допомогою яких люди виготовляють продукцію, виконують роботи, надають послуги;

частина виробничих фондів у вигляді сукупності засобів праці, які мають вартість і беруть участь у процесі виробництва протягом багатьох виробничих періодів, не змінюючи при цьому свою форму і властивості, а їх вартість переноситься на вартість продукції поступово, по мірі зношення, через амортизаційні відрахування.

Я.Д. Крупка зазначає, що при трактуванні сутності необоротних матеріальних активів відстежується взаємозв'язок двох сторін одного процесу: інвестиції ресурсів, тобто їх

вкладення на формування необоротних матеріальних активів і одержання результату у вигляді «дієвого активу» для тривалого і ефективного використання у виробничому процесі.

Найбільш поширеним у сучасній фаховій літературі є визначення необоротних матеріальних активів, як «основних засобів» та «капітальних інвестицій».

В Україні декларовано гармонізацію обліку фінансового та обліку з метою оподаткування, проте з огляду на різноспрямованість цільових функцій фінансового та фіскального обліку об'єктивним є виникнення податкових різниць. Відповідно до вимог П(С)БО 17 «Податок на прибуток» при нарахуванні податку у разі наявності позитивних тимчасових податкових різниць сума податку не відображується у складі витрат за Дт рахунку 98 «Податок на прибуток» , а знаходять відображення за Дт 17 «Відстрочені податкові активи». [2]

У фінансовій звітності бюджетних установ відсутній розділ Необоротні активи, а матеріальні необоротні активи відображують у розділі І Матеріальні активи, фінансові необоротні активи бюджетних установ представлені у розділі ІІ Фінансові активи. В Україні діють у державному секторі облікові стандарти розроблені відповідно до вимог міжнародних. Так, облік основних засобів регламентовано НП(С)БО 121 «Основні засоби» , облік нематеріальних активів НП(С)БО 122 «Нематеріальні активи», облік необоротних фінансових інвестицій НП(С)БО 133 «Фінансові інвестиції», облік інвестиційної нерухомості НП(С)БО 129 «Інвестиційна нерухомість». [3]

Податкові наслідки по операціях з необоротними активами у платників податків виникають як в частині ПДВ, так і з податку на прибуток та податку на нерухомість. У разі придбання необоротних активів, що забезпечують діяльність, результати якої оподатковуються, платниками ПДВ у платників ПДВ на підставі факту реєстрації податкової накладної виникає податковий кредит. Проблемним в обліку розрахунків з бюджетом з ПДВ, зокрема в частині придбання необоротних активів, є застосування транзитних рахунків 644.1 та 644.2 та представлення у фінансовій звітності дебетового сальдо в частині податкового кредиту в активі балансу не зважаючи на те, що його облік ведуть на пасивному рахунку 64. Більш прийнятним, на нашу думку, є підхід за яким цей податковий кредит буде знаходити відображення на рахунку 37 субрахунок 377 «Інші дебітори» - субрахунок 3-го порядку 377 «Податковий кредит за першою подією проплата постачальнику»; 377 «Податковий кредит не підтверджений податковою накладною». Податкові наслідки з ПДВ по операціях з необоротними активами виникають також і у платників ПДВ бюджетних установ.

Податкові наслідки в частині ПДВ по операціях з необоротними активами виникають також при здійсненні продажу та ліквідації необоротних активів. Ці податкові наслідки є суперечливими та неоднозначними, що обумовлено ймовірністю різних причин списання необоротних активів по яких термін корисної експлуатації не вийшов. Ці ускладнення обумовлені вимогою п.п. 14.1.191 пункту 14.1 статті 14 Кодексу [4] постачання товарів - будь-яка передача права на розпоряджання товарами як власника, у тому числі продаж, обмін чи дарування такого товару, а також постачання товарів за рішенням суду. При цьому відповідно до підпункту цього підпункту постачанням товарів також вважаються ліквідація платником податку за власним бажанням необоротних активів, які перебувають у такого платника.

Таким чином не зважаючи на гармонізацію фінансового обліку та обліку з метою оподаткування в частині необоротних активів мають місце розбіжності між цими видами обліку. Вони стосуються термінології, класифікації та відображення окремих операцій. Проявляються вони насамперед через різниці, встановлені ст. 138 ПКУ. І хоча назва цієї статті Різниці, які виникають при нарахуванні амортизації необоротних активів, йдеться в ній не лише про амортизацію. Відповідно проблеми облікової практики, які виникають у платників податку на прибуток щодо обліку з метою оподаткування необоротних активів, не тільки численні, а й досить різноманітні. До проблемних належать питання амортизації необоротних активів які тимчасово не використовуються. Тимчасове невикористання основних засобів може бути викликано різними причинами. По-перше, основні засоби

потребують періодичного ремонту, поліпшення, а інколи навіть модернізації чи реконструкції, під час проведення яких їх використання неможливе. По-друге, інтенсивність використання основних засобів, зокрема виробничого обладнання, залежить від потреб ринку. Зменшення потреб у тій чи іншій продукції і, відповідно, відсутність замовлень призводять до простоїв виробництва. По-третє, використання деяких видів основних засобів взагалі має сезонний характер.

Проблема обумовлена також різницею у трактуванні саме податковим законодавством на відміну від бухгалтерського понять *основні засоби* та *невиробничі основні засоби, різниця полягає в тім, що для бухгалтерського обліку ці об'єкти є однозначними а для обліку з метою оподаткування різними*. Так, саме згідно з вимогами податкового законодавства невиробничі основні засоби не підлягають амортизації з метою оподаткування. Це підтверджує зміст роз'яснень та консультацій наданих ДФСУ. Проте, спостерігаються позитивні зрушення і в останніх податкових роз'ясненнях мова йдеться про право нарахування амортизації із метою оподаткування.

Проблемними з точки зору податкових наслідків є операції з такими необоротними активами як інвестиційна нерухомість, незавершене будівництво та малоцінні необоротні матеріальні активи.

Бюджетні установи стосовно основних засобів здійснюють ремонтні роботи, спрямовані на підвищення техніко-економічних можливостей (модернізація, модифікація, добудова, дообладнання, реконструкція тощо) об'єкта, що приведе в майбутньому до збільшення економічних вигід. Такі роботи вважаються **поліпшенням об'єкта** основних засобів, а витрати на їх здійснення збільшують первісну вартість відповідного об'єкта. У обліку такі витрати відображають на субрахунку **капітальних інвестицій (субрахунок 1311** «Капітальні інвестиції в основні засоби»**)**. Роботи з поліпшення об'єкта основних засобів здійснюють за рахунок капітальних витрат, передбачених у кошторисах на виконання зазначених робіт. Підставою для визнання таких витрат є збільшення завдяки їм очікуваного терміну корисного використання об'єкта, кількості та/або якості робіт, послуг, які надаються цим об'єктом. Рисунком 1 представлено різні види поліпшень необоротних активів, зокрема основних засобів у бюджетних установах.

Рисунок 1 – Приклади поліпшення необоротних активів, зокрема основних засобів у бюджетних установах

Вартість поточного і капітального ремонту основних засобів не зараховується на збільшення їх балансової вартості, а списується на поточні витрати установи за рахунок відповідних джерел фінансування. Витрати на проведення ремонту основного засобу (поточного і капітального) визнаються **витратами звітного періоду**, в якому вони були здійснені **(субрахунок 8013 або 8113 «Матеріальні витрати»**).

Висновки та перспективи подальших досліджень. На підставі вивчення та узагальнення наукової літератури, нормативної регламентації та методичних матеріалів стосовно відображення в обліку та звітності в Україні та за кордоном необоротних активів є

можливим визнати, що в цілому методологія обліку в Україні наближається до регламентації відповідно з міжнародними системами. Перспектива розвитку вітчизняної системи обліку необоротних активів пов'язуються з уточненням термінології та класифікації, зокрема в частині трактування необоротних активів та таких їх складових, як інвестиційна нерухомість, матеріальні необоротні активи. Потребує удосконалення нормативно – правова база ідентифікації та обліку в Україні інвестиційної нерухомості, також має місце розбіжність структури фінансової звітності підприємств та бюджетних установ. Ми вважаємо, що необоротні активи мають бути представлені у звітності бюджетних установ окремим розділом. При здійсненні аналітичних процедур сучасна побудова звітності ускладнює розрахунки, як наприклад, при визначенні показників оцінки фінансового стану.

Список літератури

1. Семйон В.С. Бухгалтерський облік необоротних активів в Україні та Угорщині: порівняльний аспект : автореф. дис. на здобуття наук. ступеня канд. екон. наук: 08.00.09. Житомир, 2010. 23 с.
2. Положення (стандарт) бухгалтерського обліку 17 «Податок на прибуток», затв. наказом МФУ від 03.10.2007 р. № 1100. URL: http://zakon3.rada.gov.ua/laws/show/z1054-03
3. Національні положення (стандарти) бухгалтерського обліку в державному секторі. Затверджені наказом Мінфіну України від 18 травня 2012, Бюл. № 568, зареєстровано в Міністерстві юстиції 06 червня 2012 р. за № 903/21215. – Режим доступу: http://www.minfin.gov.ua/
4. Податковий кодекс України від 02.12.2010 р. № 2755-VI. URL: http://zakon2.rada.gov.ua/laws/show/2755-17/paran8575#n8575

УДК 336.1:352

Л. Моклюк, магістр гр. ФС-18МЗ
Центральноукраїнський національний технічний університет

СУТНІСТЬ ТА ОСОБЛИВОСТІ ФОРМУВАННЯ ДОХОДІВ МІСЦЕВИХ БЮДЖЕТІВ

У статті досліджено основні наукові підходи до сутності поняття «доходи місцевих бюджетів» з позиції деяких науковців. Проаналізовано стан та особливості формування дохідної частини місцевих бюджетів. Запропоновано напрямки розширення джерел формування доходів місцевих бюджетів.
місцеві бюджети, децентралізація, доходи місцевих бюджетів, міжбюджетні трансферти, податок на доходи фізичних осіб, місцеві податки і збори

Постановка проблеми. Визначальну роль у соціально-економічному розвитку територій відіграють місцеві бюджети, адже саме через них здійснюються основні видатки на утримання закладів освіти, охорони здоров'я, культури, фінансування молодіжних програм, житлово-комунального господарства тощо. В умовах децентралізаційних процесів, які нині набирають стрімких обертів, перед органами місцевого самоврядування постає нагальне завдання забезпечення достатнього наповнення дохідної частини місцевих бюджетів. Чинна система акумулювання доходів місцевих бюджетів України характеризується низьким рівнем частки власних надходжень, що відображається нарощуванням обсягів міжбюджетних трансфертів. У цьому контексті актуальним є дослідження особливостей формування доходів бюджетів на місцевому рівні та розробка пропозицій щодо їх збільшення.

Аналіз останніх досліджень і публікацій. Істотний внесок у дослідження процесу формування доходів місцевих бюджетів зробили такі відомі вчені, як: В. Базилевич, О.

Василик, Н. Власюк, О. Кириленко, В. Кравченко, В. Опарін, К. Павлюк, Ю. Пасічник, О. Сунцова, В. Федосов, І. Чугунов, Н. Чуйко, С. Юрій та інші.

Метою статті є дослідження теоретичних аспектів формування доходів місцевих бюджетів та розробка пропозицій щодо їх збільшення.

Виклад основного матеріалу. Ст. 2 Бюджетного кодексу України визначає доходи бюджету як «податкові, неподаткові та інші надходження на безповоротній основі, справляння яких передбачено законодавством України (включаючи трансферти, плату за надання адміністративних послуг, власні надходження бюджетних установ)» [2].

Слід зазначити, що серед представників наукової спільноти не існує єдиної точки зору щодо визначення сутності та змісту категорії «доходи місцевих бюджетів». В залежності від об'єкту та предмету дослідження вони акцентують увагу на економічних відносинах, на правовому характері, на матеріальному втіленні цієї категорії, а також на організаційних формах та методах формування доходів місцевих бюджетів.

Так, В. Кравченко, визначає доходи місцевих бюджетів, як «кошти, які надходять до відповідних місцевих бюджетів у розмірах і порядку, встановлених законодавчо» [7, с. 399].. Також він вказує, що доходи місцевих бюджетів включають: власні або закріплені доходи, відрахування від регульованих доходів, дотації, субсидії, субвенції та інші трансферти та додає, що вони розподіляються на податкові і неподаткові, таким чином визначаючи форми та методи, за якими вони формуються. Отже, вчений підходить до сутності доходів місцевих бюджетів через законодавчо визначений порядок їх формування.

Спільну думку, що доходи місцевих бюджетів формуються в результаті акумуляції та наповнення власних і закріплених коштів, а також трансфертів, мають О. Кириленко [5, с. 140] та С. Савчук [15, с. 88]. У своїх визначеннях вони акцентують увагу на організаційних формах залучення коштів до місцевих бюджетів.

О. Василик та К. Павлюк зазначають, що економічна сутність доходів місцевих бюджетів виявляється у формуванні грошових фондів, які є фінансовим забезпеченням діяльності місцевих рад і місцевих державних адміністрацій [3, с. 176]. Отже, науковці роблять наголос на матеріальному втіленні даної економічної категорії.

М. Чечетов, Н. Чечетов й А. Бережна вважають, що доходи бюджету як економічна категорія відображають відносини щодо формування бюджетних фондів всіх рівнів та спеціалізованих цільових фондів [17, с. 106].

На думку Н. Власюка, доходи місцевих бюджетів – це кошти, що надходять у постійне користування на безповоротній основі та забезпечують стабільність бюджету і фінансування його видатків [4].

За С. Юрієм та Й. Бескидом, доходи місцевих бюджетів поділяються на доходи, які формуються внаслідок дій і рішень, прийнятих органами місцевого самоврядування та доходи, які на довготривалій основі передаються до місцевих бюджетів у повному розмірі або у встановленій для усіх бюджетів єдиній частині [18].

В. Кулик стверджує, що доходами бюджету є кошти, що надходять у постійне користування на безповоротній основі, які забезпечують стабільність бюджету і фінансування його видатків [8].

На думку В. Базилевича, доходи централізованих фондів держави та органів місцевого самоврядування відображаються у грошових відносинах, які виникають між державою, юридичними і фізичними особами у процесі вилучення й акумуляції частини вартості валового внутрішнього продукту в загальнодержавному та місцевих фондах з метою їхнього подальшого використання, тобто для здійснення державою й органами місцевого самоврядування своїх функцій [1, с. 51].

Ю. Пасічник визначає доходи місцевих бюджетів як «…сферу економічних відносин суспільства, яка пов'язана з формуванням, розподілом та використанням фінансових ресурсів регіонального рівня і використовується місцевими органами для забезпечення поточних і перспективних завдань розвитку регіону» [14, с. 360]. Він акцентує увагу не

тільки на економічному змісті, а і на меті формування доходів місцевих бюджетів та напрямках їх використання.

Розвиток децентралізаційних процесів спонукають науковців та практиків приділяти пильну увагу питанням формування доходів місцевих бюджетів.

Суб'єктами системи формування доходів місцевих бюджетів виступають органи державної влади, органи місцевого самоврядування, громадяни, асоціації органів місцевого самоврядування, бюджетні установи, громадські некомерційні організації та приватний сектор.

Про важливе значення доходів місцевих бюджетів свідчить динаміка їх частки у перерозподілі ВВП та у доходах зведеного бюджету держави (табл. 1)

Таблиця 1 - Динаміка доходів місцевих бюджетів України у 2014–2018 рр. [13]

Показники	Роки					2018р. у % до 2014
	2014	2015	2016	2017	2018	
1. Доходи місцевих бюджетів (без урахування міжбюджетних трансфертів), млрд. грн.	101,1	120,5	170,8	229,5	263,5	260,63
2. Доходи зведеного бюджету України, млрд. грн.	456,1	652,0	782,9	1017,0	1184,3	259,66
3. ВВП, млрд. грн.	1586,9	1988,5	2383,2	2982,9	3558,7	224,25
4. Частка перерозподілу ВВП через місцеві бюджети, %	6,37	6,06	7,17	7,69	7,4	116,17
5. Частка доходів місцевих бюджетів у доходах зведеного бюджету, %	22,17	18,48	21,82	22,57	22,25	100,36

Дані табл. 1 свідчать, що сукупний обсяг власних доходів місцевих бюджетів (без урахування міжбюджетних трансфертів) протягом 2014–2018 рр. збільшився на 162,4 млрд. грн., або більше ніж у 2,5 рази (260,63%) і становив 2018 р. 263,5 млрд. грн., що є позитивним явищем.

Однак, частка доходів місцевих бюджетів у доходах зведеного бюджету України за результатами 2018 р. становила лише 22,25% проти 22,57% у 2017 р. А у 2013 році цей показник становив 23,76%, що свідчить про суттєве його зниження, незважаючи на проведення бюджетно-податкової реформи 2015р., якою ніби розширено склад доходів місцевих бюджетів, у напрямі бюджетної децентралізації місцевих органів влади. Така ситуація є негативною, адже є свідченням того, що вітчизняній бюджетній системі притаманна висока концентрація бюджетних ресурсів на рівні державного бюджету. це доказ того, що в Україні й надалі спостерігається високий рівень централізації бюджетних коштів, що абсолютно суперечить взятому курсу на децентралізацію.

Частка перерозподілу ВВП через місцеві бюджети протягом 2014–2018 рр. зросла на 1,03 в.п. унаслідок випереджаючого зростання обсягу доходів місцевих бюджетів (260,63%) над ростом обсягів ВВП (224,25%) і становила 2018 р. 7,4%.

Незважаючи на постійне зростання всіх основних складових доходів місцевих бюджетів (зокрема, за останні 7 років в середньому в 2,5 рази), офіційні трансферти займали і продовжують займати найбільшу питому вагу у доходах місцевих бюджетів. Середній показник по Україні становив в 2012 році – 55,2%, в 2018 році – 53,2%. При цьому частка податкових надходжень за останні одинадцять років навіть знизилася: в 2008 році вона становила 43,0%, а в 2018 році – 41,3%. Інші види доходів займають незначну питому вагу в загальній сумі доходів місцевих бюджетів: частка неподаткових надходжень коливається в межах 6-7%, а частка інших доходів (від операцій з капіталом, урядів зарубіжних країн та

міжнародних організацій, цільових фондів) в 2012 році становила 1,1%, а в 2018 році – 0,5% (рис. 1).

Саме за допомогою міжбюджетних трансфертів на місцевому рівні вирішують питання компенсації бюджетам нижчого рівня витрат на виконання делегованих повноважень, вартість яких перевищує бюджетні можливості місцевих органів влади, а також проблеми, зумовлені нерівномірністю мобілізації доходів бюджетів та соціальні проблеми, пов'язані зі специфікою розвитку регіонів та їх економічною спроможністю.

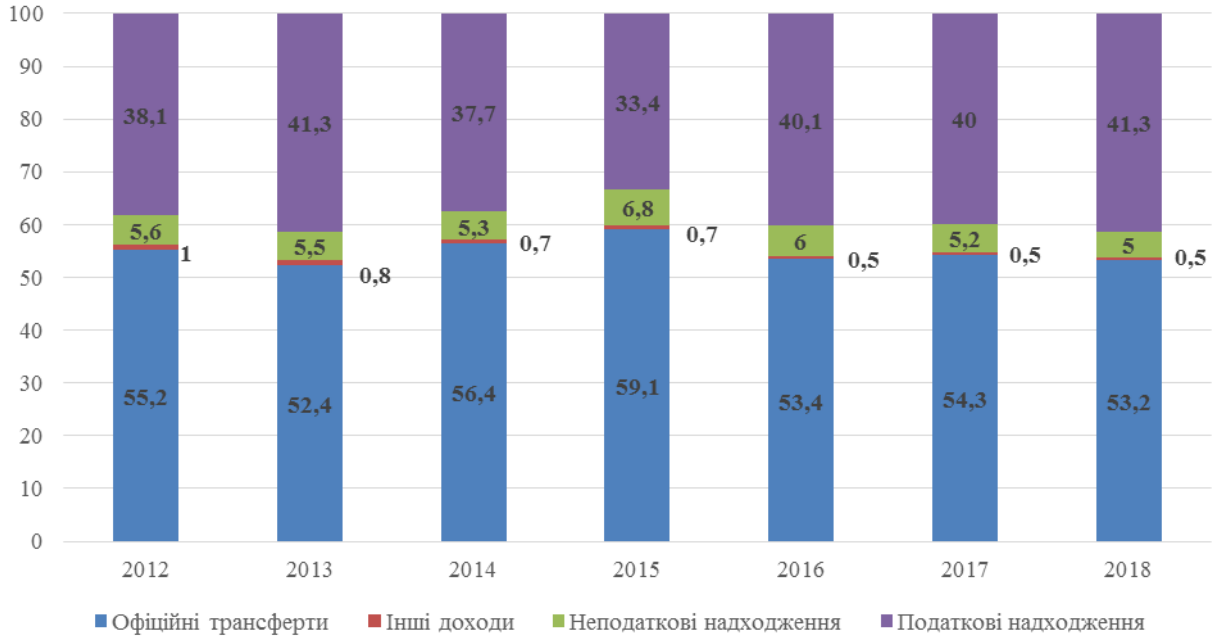


Рисунок 1 - Структура доходів місцевих бюджетів [13]

Очевидно, що тенденції, коли вагому частку доходів місцевих бюджетів становлять трансферти, суперечать принципам бюджетної децентралізації, позаяк останні – це пасивний інструмент в руках держави, за допомогою якого вона вирішує питання збалансування місцевих бюджетів, фінансування соціально-економічного розвитку територій тощо і тим самим послаблює зацікавленість місцевої влади в нарощуванні власної дохідної бази.

З прийняттям Концепції реформування місцевого самоврядування та територіальної організації влади в Україні [6] та внесенням змін до Бюджетного кодексу України в 2014 р., структура розподілу доходів місцевих бюджетів між рівнями бюджетної системи України зазнала змін. А саме, відбулися зміни у структурі розподілу податку на доходи фізичних осіб, екологічного податку, податку на прибуток.

У результаті цих змін розподіл надходжень від ПДФО між ланками бюджетної системи відбувається за новими правилами:

– 60% податку зараховують до загального фонду бюджетів міст обласного (республіканського) значення, районних бюджетів чи бюджетів об'єднаних територіальних громад, що створюються згідно із законом і перспективним планом формування територій громад;

– 15% потрапляють у дохід загального фонду обласних бюджетів;

– 40% направляють до бюджету Києва;

– 25% скеровують до державного бюджету, а з ПДФО, що сплачується (перераховується) на території міста Києва – 60%. Також до державного бюджету зараховуються надходження від ПДФО з пасивних доходів (проценти за депозитами) та військовий збір [2].

Нині з-поміж податкових надходжень чільне місце посідає податок на доходи фізичних осіб (ПДФО) – це прямий податок, яким оподатковуються доходи фізичної особи

(табл. 2).

Таблиця 2 - Частка ПДФО у податкових доходах місцевих бюджетів України та ВВП у 2014–2018 рр. [13]

Показники	Роки					2018р. у % до 2014
	2014	2015	2016	2017	2018	
1. ПДФО, зарахований до місцевих бюджетів, млрд. грн.	62,6	54,9	79,0	110,7	138,2	220,8
2. Податкові доходи місцевих бюджетів, млрд. грн.	87,3	98,2	146,9	201,0	232,5	266,3
3. ВВП, млрд. грн.	1586,9	1988,5	2383,2	2982,9	3558,7	224,25
4. Частка ПДФО, %:						
4.1. У податкових доходах місцевих бюджетів	71,71	55,91	53,78	55,07	59,44	82,9
4.2. У ВВП	3,94	2,76	3,31	3,71	3,88	98,5

Незважаючи на суттєве збільшення обсягу надходжень ПДФО, зарахованого до місцевих бюджетів протягом досліджуваного періоду, у 2,2 рази, його частка в структурі податкових надходжень місцевих бюджетів зменшилася на 12,27 в.п. і становила у 2018 р. лише 59,44%.

Частка надходжень ПДФО, зарахованого до місцевих бюджетів у ВВП протягом 2014–2018 рр., зменшилася на 0,06 в.п. унаслідок випереджаючого росту обсягу ВВП (224,25%) над ростом надходжень цього виду податків (220,8%) і становила 2018 р. 3,88%.

Попри зниження частки ПДФО, зарахованого до місцевих бюджетів протягом 2014–2018 рр., на 12,27 в.п., фіскальна роль цього виду податкових доходів є очевидною, адже у 2018 р. більше половини (52,45%) сукупних надходжень місцевих бюджетів сформовано за його рахунок.

Особливе місце в структурі формування доходів місцевих бюджетів займають місцеві податки та збори. Місцеві ради встановлюють єди-ний податок та податок на майно (в частині транспортного податку та плати за землю та в частині податку на нерухоме майно, відмінне від земельної ділянки), визначають ставку збору за місця паркування транспортних засобів та туристичного збору. Їх частка у формуванні доходів місцевих бюджетів протягом 2014-2018рр., незважаючи на номінальне збільшення їх обсягу, хоч і збільшилась, але становить лише 23,1 (у розвинених країнах від 30% до 70%), що свідчить про недостатню фінансову незалежність та відсутність стимулів до нарощення своєї власної доходної бази органами місцевого самоврядування (табл. 3).

Таблиця 3 - Динаміка місцевого оподаткування України за видами податкових надходжень у 2014–2018 рр. [13]

Показники	Роки					2018р. у % до 2014
	2014	2015	2016	2017	2018	
1. Місцеві податки і збори, млрд. грн.	8,1	27,0	42,3	52,6	61,0	52,9
2. Доходи місцевих бюджетів (без урахування міжбюджетних трансфертів), млрд. грн.	101,1	120,5	170,8	229,5	263,5	260,63
3. ВВП, млрд. грн.	1586,9	1988,5	2383,2	2982,9	3558,7	224,25
4. Частка місцевих податків і						

зборів, %:						
4.1. У доходах місцевих бюджетів	8,0	22,4	24,8	22,9	23,1	15,1
4.2. У ВВП	0,5	1,4	1,8	1,8	1,7	1,2

Важливим є єдиний податок, адже мале підприємництво є надзвичайно динамічним елементом економіки країни і має серйозний фіскальний потенціал. Єдиний податок займає найсуттєвіше місце у структурі надходжень від місцевих податків та зборів до місцевих бюджетів.

Держава може збільшувати обсяг надходжень єдиного податку до місцевих бюджетів шляхом регулювання факторів впливу на його обсяги, а саме: величину ВВП; рівень платоспроможності населення; рівень тіньової економіки; валютний курс та рівень інфляції. Для зменшення рівня тіньової економіки держава має створити прозорі умови для ведення бізнесу в Україні, підвищити рівень довіри до державних органів, удосконалити податкову систему.

Перспективою розвитку місцевого оподаткування, на наш погляд, є повернення податку на рекламу, який було скасовано із запровадженням Податкового кодексу України. На сьогоднішній день у період інформатизації суспільства, реклама відіграє велику роль, саме тому, ми вважаємо, податок на рекламу буде не лише важливим фіскальним інструментом, але й важелем соціально-економічного регулювання. Ставка податку на рекламу повинна бути диференційована не лише залежно від тривалості розміщення реклами (0,5 % – за розміщення реклами на тривалий термін, 0,1 % – від вартості послуг за розміщення одноразової реклами), але й залежно від виду рекламних послуг [11].

Наступним кроком щодо побудови ефективної системи місцевого оподаткування є запровадження утилізаційного збору. Механізм запровадження утилізаційного збору такий:

1) автоматичне введення утилізаційного збору на неекологічні товари;

2) введення ставки утилізаційного збору на рівні 7% від вартості неекологічного товару;

3) цільовий характер утилізаційного збору, що передбачає використання надходжень такого збору виключно на заходи зі збору неекологічних товарів та їх утилізацію або повторну переробку;

4) віднесення утилізаційного збору до місцевих зборів обов'язкового характеру.

Запровадження утилізаційного збору сприятиме вирішенню не лише ряду складних екологічних питань, але й збільшенню фінансових можливостей місцевих органів влади у сфері покращення стану навколишнього природного середовища [10].

Неподаткові надходження відіграють незначну роль у формуванні доходів місцевих бюджетів, хоча їх можна розглядати як вагоме потенційне джерело зміцнення місцевих бюджетів. Перелік неподаткових доходів залежить передусім від того, які платні послуги можуть надавати населенню органи місцевого самоврядування, і від забезпечення муніципалітетів об'єктами комунальної власності. Доцільніше уникати масового відчуження комунальної власності, натомість зосередитися на отриманні доходу від надання в оренду таких об'єктів.

Також обсяги неподаткових надходжень місцевих бюджетів можна збільшити шляхом розширення спектра необов'язкових платних послуг, що надаються органами місцевого самоврядування населенню на ринкових засадах, в першу чергу тих, які пов'язані з виконанням власних повноважень місцевих рад [9].

На сьогоднішній день існує значний резерв збільшення надходжень до місцевих бюджетів, який пов’язаний із детінізацією економіки, легалізацією заробітної плати. Нажаль, реальні повноваження у органів місцевого самоврядування щодо застосування дієвих заходів до суб’єктів господарювання, які виплачують заробітну плату нижче мінімальної та, відповідно, ухиляються від сплати податків, відсутні.

Основними причинами ухилення від сплати податків, є: складність у розрахунках податкових сум, нераціональна структура оподаткування, негативне відношення до існуючої податкової системи – жорстка податкова система багато в чому не стимулює працю виробника, а, навпаки, підштовхує його до утаювання прибутків та несплати податків [12].

На динаміку формування доходів місцевого бюджету впливає значні міграції населення, викликані економічними причинами: високим рівнем безробіття в регіоні або нижчим порівняно з іншими регіонами рівнем заробітної плати. Внаслідок такого переміщення населення у менш благополучному регіоні зменшується кількість працездатного населення, що, відповідно, зменшує потенційну базу оподаткування. Ці чинники негативно впливають на збільшення доходів місцевих бюджетів.

Отже, оскільки саме податкові надходження формують основний обсяг власних доходів місцевих бюджетів, питання підвищення ефективності податкового адміністрування виходить на передній план у контексті децентралізації. Однак, варто зауважити, що у сучасних реаліях лише підвищення податкових ставок не здатне забезпечити місцеві бюджети необхідними фінансовими ресурсами, адже допоки кількість малоприбуткових та збиткових підприємств у регіонах залишається значною, поширене тіньове ведення бізнесу, відбувається зростання цін та тарифів, зокрема й на житлово-комунальні послуги, а реальні доходи населення скорочуються, то зростання податкового навантаження не принесе очікуваного результату, а лише спричинить поглиблення кризових явищ. Тому на шляху до забезпечення нарощування податкових доходів місцевих бюджетів стратегічною метою місцевої влади має стати сприяння економічному розвитку регіонів [16].

Список літератури

1. Базилевич В.Д. Державні фінанси: Навч. посіб. / В.Д. Базилевич, Л.О. Баластрик. – К.: Атіка, 2002. – 368 с.
2. Бюджетний кодекс України від 08.07.2010 р. №2456-VI. - URL: //zakon1.rada.gov.ua/lows/show/2456-17.
3. Василик О.Д. Бюджетна система України: підручник / О.Д. Василик, К.В. Павлюк. – К.: – Центр навчальної літератури, 2004. – 544 с.
4. Власюк Н.І. Реформування системи міжбюджетних відносин в Україні: переваги і недоліки / Н.І. Власюк // Глобальні та національні проблеми економіки. – Миколаївський національний університет імені В.О. Сухомлинського. – 2010. – № 10. – С. 751-754.
5. Кириленко О.П. Місцеві фінанси: Навчальний посібник. - Тернопіль: Астон. - 2004. - 192 с.
6. Концепція реформування місцевого самоврядування та територіальної організації влади в Україні. - URL: https://zakon.rada.gov.ua/laws/show/333-2014-р.
7. Кравченко В.І. Місцеві фінанси України: Навч. посіб. – К.: Т-во “Знання”, КОО, 1999. – 487 с.
8. Кулик І.О. Шляхи удосконалення управління місцевими бюджетами. - URL: http://www.kbuapa.kharkov.ua/e-book/conf/2012-2/doc/2/11.pdf.
9. Луніна І. О. Диверсифікація доходів місцевих бюджетів [Текст] / [Луніна І. О., Кириленко О. П., Лучка А. В. та ін.]; за ред. д-ра екон. наук І. О. Луніної; НАН України; Інститут екон. та прогнозув. – К., 2010. – 320 с.
10. Мартинюк І.В. Утилізаційний збір для неекологічних товарів / І.В. Мартинюк, О.Ю. Дубовик // Агросвіт. Науково-практичний журнал. ТОВ. "ДКС Центр"— 2014. — 8. — С. 37—42.
11. Мартинюк І.В., Богатирьова Є.М. Місцеве оподаткування в Україні: сучасний стан та перспективи розвитку. - URL: http://www.economy.in.ua/pdf/6_2019/7.pdf.
12. Набатова Ю.О. Фактори впливу на обсяги податкових надходжень місцевих бюджетів / Ю.О. Набатова, А.О. Богуславська // Ефективна економіка. – 2017. – № 9. - URL: http://www.economy.nayka.com.ua/?op=1&z=5773.
13. Офіційна веб-сторінка Державної служби статистики України. URL: http://www.ukrstat.gov.ua.
14. Пасічник Ю.В. Бюджетна система України та зарубіжних країн: Навч. посіб. / Ю.В. Пасічник. – К.: Знання-Прес, 2002. – 495 с.
15. Савчук С.В. Теоретико-концептуальні засади визначення доходів бюджетів як об’єкта бюджетного планування / С.В. Савчук // Наука й економіка. – 2012. - № 1. – С. 81-88.
16. Хотенко О. Податкові джерела доходів місцевих бюджетів / О. Хотенко, О. Смірнова // Веб-сайт ГО “Інститут податкових реформ”, 2017. – URL: http://ngoipr.org.ua/blog/podatkovi-dzhereladohodiv-mistsevyh-byudzhetiv/.
17. Чечетов М.В. Бюджетний менеджмент: навч. посіб. в 2 ч. / М. В. Чечетов, Н. Ф. Чечетова, А. Ю. Бережна. – Харків : ІНЖЕК, 2004. Ч. 1. – 2004. – 560 с.

18. Юрій С.І. Бюджетна система України / С.І. Юрій, Й.М. Бескид. – Навчальний посібник. – Київ: НІОС, 2004. – 400 с.

УДК 930.253

І. Моторіна, магістр гр. ІС-18М
Центральноукраїнський національний технічний університет

ІСТОРІЯ СТВОРЕННЯ ТА ФУНКЦІОНУВАННЯ ДЕРЖАВНОГО АРХІВУ КІРОВОГРАДСЬКОЇ ОБЛАСТІ

Досліджено питання створення, реорганізації та функціонування Державного архіву Кіровоградської області, визначено основні напрямки роботи сучасної архівної установи.
архів, архівна установа, документ, інформаційна установа, зберігач інформаційного ресурсу, архівний фонд

Актуальність статті. За Конституцією України «культурна спадщина» охороняється законом. Держава забезпечує збереження історичних пам'яток та інших об'єктів, що становлять культурну цінність, вживає заходів для повернення в Україну культурних цінностей народу, які знаходяться за її межами" Скарбниці документальної пам'яті нації – архіви – є інформаційними системами, в яких застосовуються інформаційні технології під час опрацювання, класифікації, використання документів. Водночас архіви є установами державного управління і багатьма своїми функціями тісно пов'зані зі сферами державного життя [3, с. 13].

Серед галузей науки і навчальних дисциплін гуманітарного циклу, роль і значення нині яких неухильно зростає, одне з чільних місць посідає архівознавство тобто система наукових знань про архіви, архівну справу, її історію, теорію і практику.

Архівознавство – це наукова система, яка вивчає історію, теорію і практику архівної справи, її правові та економічні засади, архівний менеджмент та інформаційні системи, принципи формування і використання архівного фонду, технологію зберігання та реставрації документів.

З цього означення архівознавства як наукової системи випливає його суть як навчальної дисципліни, що висвітлює й вивчає історію, теорію і практику архівної справи.

На нашу думку, архівознавство займає чільне місце в суспільстві, так як, ця дисципліна береже історичну пам'ять. Саме архівознавство вторгається в усі сфери життя, насамперед духовного. Серед найважливіших питань архівознавства важливе місце займає удосконалення організації управління діяльністю архівних установ. До них відносять пошук нових методів відбору і реєстрації документів, облік і зберігання, їх класифікацію тощо.

Різні сторони функціонування архівних установ було вивчено такими дослідниками, як Мицак І., Стаховський Д., Климова К., Бутич І., Матяш І. та ін.

Так, дослідником Шурубою А. було розглянуто питання створення та впровадження стандартів з організації зберігання документів, документознавець та бібліографознавець Ю.Столяров значну увагу приділяє питанню функціонування архівного документного ресурсу серед ресурсів інших інформаційних установ, дослідниця Г.Швецова-Водка розглядає особливості визначення поняття документ в архівознавстві.

Дослідження здійснено в напрямі виконання законів України «Про Національний архівний фонд та архівні установи», «Про Національну програму інформатизації», «Про доступ до публічної інформації» та ін.

Мета статті виділити основні етапи створення та розвитку ДАКО, коротко окреслити сучасну документно-інформаційну діяльність даної архівної установи.

Задля реалізації головної мети дослідження необхідно було розв'язати такі основні завдання: окреслити періоди діяльності державного архіву Кіровоградщини, розглянути напрямки інформаційної діяльності архіву.

Досліджуючи архівну роботу в Україні у повоєнні роки, науковці виділяють три основні періоди:

1. «Охоплює період від визволення України у 1944 р. до XX з'їзду КПРС у 1956 р. Це період перебування архівних установ у складі МВС, повної сталінської диктатури в усіх сферах життя, приховування недоліків і написання праць у дусі пануючої ідеології. Для цього періоду характерний не стільки науковий підхід у висвітленні проблеми, як написання статей інформаційного характеру про різні аспекти архівної роботи. Майже всі статті з даної проблеми того періоду написані архівістами, що пояснюється як їхньою професійною зацікавленістю, так і обмеженням доступу науковців до архівних джерел у вказаний період. Значну частину серед цих праць становлять спогади учасників оперативних груп УДА НКВС УРСР і окремих архівістів про перші кроки по відбудові архівного господарства після звільнення України від загарбників, заходи щодо розшуку вивезених окупантами матеріалів тощо.

2. Охоплює період після XX з'їзду КПРС і аж до розвалу СРСР. Для цього етапу характерне зростання науково-дослідної роботи в цілом у, щопозитивно вплинуло і на стан розробки праць з історії архівної справи. Відбулося загальне пожвавлення у роботі дослідників з архівними документами, причиною чого стало розсекречення значної кількості архівних фондів і збільшення допуску дослідників у архіви. Як наслідок, праці з історії архівної справи почали з'являтися не тільки зпід пера архівістів, а і дослідників з різних наукових установ, що дало можливість простежити розвиток архівного будівництва як з "середини", так і з "зовнішнього" боку, тобто бачення цієї проблеми людьми, зацікавленими у об'єктивному висвітленні питання. Слід відмітити, що більшість праць з даної проблеми вийшла саме у період хрущовської "відлиги", тобто період відносної лібералізації і плюралізму думок, що підносить цінність цих робіт. Але і в період утвердження тоталітаризму і аж до розвалу СРСР з'явилося чимало праць, які посіли достойне місце у дослідженні цього питання, хоча радянська епоха наклала на них свій негативний відбиток.

3. Етап охоплює останнє десятиріччя, тобто період української історіографії в умовах незалежної України. Праці цього етапу вигідно відрізняються від попередніх своїм неупередженим ставленням і об'єктивністю, намаганням позбутися стереотипів минулого. Автори намагаються проводити джерелознавчу критику, що сприяє найбільш об'єктивному висвітленню даної проблеми. Дослідження з історії розвитку архівної справи в Україні у розглядуваний період з'явилися вже у перші повоєнні роки. Вони висвітлювали шляхи подолання тих проблем, які постали перед архівістами при відновленні архівної мережі України і нормального функціонування архівних установ, проблему підготовки кадрів тощо» [6].

Як справедливо зазначають дослідники, «водночас до особливостей розвитку галузі в різних регіонах республіки виявлено менше уваги, історія Державного архіву Кіровоградської області висвітлена фрагментарно» [10].

Вивчення історії створення та функціонування ДАКО дослідниками Марченко М. [10], Шевченко С. [10], Трибуцька О. [8] дозволило нам виокремити такі етапи функціонування ДАКО:

Початок XX ст. – відсутні державні архівні установи на Кіровоградщині, що зумовило втрату важливої частини інформаційно-документного ресурсу регіону.

1917 р. – організація при Єлисаветградському ревкомі комісії для проведення обстеження відомчих архівів, що стало першою спробою створення державної архівної установи на Кіровоградщині.

Жовтень 1920 р. – прийняття рішення Єлисаветградським повітвиконкомом щодо створення повітового архіву, який, на жаль, так і не було створено.

17 листопада 1925 р. Президією окрвиконкому ухвалено рішення про організацію окружного архівного управління (окрархіву), з цього періоду фактично і починається історія потужної сучасної інформаційної установи – Державного архіву Кіровоградської області.

1925 – 1930 рр. - Зінов'євське окружне архівне управління.

У листопаді 1930 р. замість окружного архівного управління створено Зінов'євське місцеве архівне управління.

У березні 1932 р. Зінов'євське місцеве архівне управління реорганізовано в Зінов'євський державний історичний архів, що підпорядковувався Одеській обласній архівній управі.

1943 р. – Зінов'євський державний історичний архів отримав назву Кіровський державний історичний архів внаслідок перейменування нашого міста.

У 1939 р. зі створенням Кіровоградської області Кіровський державний історичний архів було реорганізовано у Кіровоградський обласний державний архів, створено архівний відділ УВС по Кіровоградській області, що здійснював керівництво архівною справою регіону.

У 1941 році Кіровоградський обласний державний архів перейменовано в Державний архів Кіровоградської області (ДАКО).

У липні 1941 р., у зв'язку з наближенням німецьких загарбників до м. Кіровограда частину документів ДАКО було евакуйовано.

9 січня 1944 року архівний відділ УВС у Кіровоградській області поновив свою роботу.

У 1958 р. Державний архів Кіровоградської області перейменовано в Кіровоградський обласний державний архів.

06 червня 1980 р. Кіровоградський обласний державний архів перейменовано в Державний архів Кіровоградської області.

Як справедливо зазначає О.Трибуцька, «нині Державний архів Кіровоградської області є найбільшою скарбницею документів з історії Кіровоградщини. Документальний фонд держархіву складає 1 млн. 299 тис.615 од. зб. управлінської документації та 5 тис 296 од. зб. документів особового походження, що охоплюють період з 1759 по 2010 роки, 218 од. зб. науково-технічної документації, 251 од. зб., 260 од. обл. кінодокументів, 23 тис. 357 од. обл. фотодокументів, 285 од. зб., 334 од. обл. фонодокументів, 26 од. зб., 50 од. обл. відеодокументів» [8].

Висновки. Отже, Державний архів Кіровоградської області – потужна інформаційна установа, що є насамперед зберігачем надважливої частини інформаційного ресурсу Кіровоградщини зокрема та України загалом. Наразі ж дана інформаційна установа, окрім зберігання інформаційного ресурсу, зусиллями свої професійно підготовлених та кваліфікованих працівників здійснює і інші функції, як-от: центрів-створювачів первинних документів, центрів-генераторів баз даних, центрів, які здійснюють аналітичну обробку інформаційного ресурсу за запитами конкретних споживачів.

Список літератури

1. Закон України «Про Національний архівний фонд та архівні установи». Відомості Верховної Ради України (ВВР). 1994. N 15.
2. ДСТУ 2732:2004. Національний стандарт України. Діловодство й архівна справа. Терміни та визначення понять. Київ: Держспоживстандарт України, 2005.36 с.
3. Архівознавство: підручник для студентів історичних факультетів вищих навчальних закладів України /За газ. ред Я. С. Калакури та І. Б. Матяш. Київ: Видавн. дім «КМ Академія», 2002. 349 с.

4. Архівознавство: підручник / Авт. кол.: Боряк Г. В., Дубровіна Л. А. та ін. 2-е вид., виправлене і допов. Київ: Академія, 2002. С.156 – 158.
5. Матяш І. Б. Сучасна українська архівістика: організація, проблеми, завдання. Бібліотекознавство. Документознавство.Інформологія. 2004. № 1. С.45 – 50.
6. Мицак І. Історіографія розвитку архівної справи в україні (1943- середина 1960-х рр.). Історіографічні дослідження в Україні. 2002. 11. С. 152 – 165.
7. Новохатський К. Документ Національного архівного фонду – документальна пам'ятка історії та культури: співвіднесення понять. АУ. 1999. № 1 – 6. С.26 – 34.
8. Трибуцька О.А. Державному архіву області – 85! Архіви України. 2010. № 5. С. 91 – 103.
9. Швецова-Водка Г. Визначення документа в архівознавстві. Студії. К., 1999. Т. 4. С. 99 – 102.
10. Шевченко С.І., Марченко О.М. Перший етап становлення радянської архівної справи в Зінов'євську (1920 – березень 1925 рр.). Спеціальні історичні дисципліни. 2011. Число 18 С. 237-241.
11. Шуруба А. Нові українські стандарти з організації зберігання документів національного архівного фонду України. Студії з архівної справи і документознавства. Київ: УДНДІАСД, 1999. Т.4. С. 52 – 57.

УДК С 930

О. Мудра, магістр гр. ІС-18М
Центральноукраїнський національний технічний університет

НОВІ НАДХОДЖЕННЯ НУМІЗМАТИЧНОЇ КОЛЕКЦІЇ КІРОВОГРАДСЬКОГО ОБЛАСНОГО КРАЄЗНАВЧОГО МУЗЕЮ В КОНТЕКСТІ ІСТОРІЇ ФОРМУВАННЯ ЙОГО ФОНДІВ

Формування музейної колекції та її складових безпосередньо пов'язана з історією виникнення та розвитку самого музею. Нумізматична колекція не є винятком із цього правила. Відповідно досліджуючи історію музею відкривається можливість простежити час виникнення музейної нумізматичної колекції, шляхи її поповнення та склад.

Мета даного дослідження полягає в описі та аналізі нових надходжень нумізматичної колекції Кіровоградського обласного краєзнавчого музею в контексті формування його фондів.

Так склалося, що історія формування колекції музейних предметів Кіровоградського обласного краєзнавчого дослідження як і самого музею не стала предметом спеціальних наукових досліджень. Абсолютна більшість авторів (Босько. В., Григор'єва Т, Здір Л., Колесник Л., Левочко В., Пархомчук В., Хоменко І., Яцук М.) піднімали ці питання в публікаціях в періодичних виданнях. Виняток складає доповідь Адаменко В. присвячена розвитку музейної справи на Кіровоградщині на міжвузівській науковій конференції з історичного краєзнавства, в якій було означено основні етапи розвитку музейної справи, починаючи від історико-географічного музею Єлисаветградського земського реального училища [1]. В окремому розділі колективної монографії, присвяченого витокам технічної освіти в Єлисаветграді, Орлик В.М. цитує звіт про стан реального училища за 1887р., де мова йде про заснування музею [13]. Тупчієнко М.П., спеціально не торкаючись історії виникнення музею, звертає увагу саме на муєзнавчий аспект археологічних досліджень засновника музею В.М. Ястребова [14]. У свою чергу, кіровоградська дослідниця Печериця Т., в контексті вивчення джерелознавчої спадщини П.З Рябкова, приділяє увагу його музейній і археологічній діяльності [10].

Робота базується на використанні історичного методу, методу наукового опису та аналізу та порівняльно-типологічного методу.

Джерельною базою послужили надходження 2019 р. до нумізматичної колекції Кіровоградського обласного краєзнавчого музею, документи групи «Архівні джерела» цього музею та документи фонду 60 Державного архіву Кіровоградської області (ДАКО).

Перш ніж зупинитися на характеристиці нових надходжень до нумізматичної колекції музею коротко охарактеризуємо історію його виникнення та розвитку. Кіровоградський обласний краєзнавчий музей є спадкоємцем найстарішого музейного закладу міста, що виник при Єлизаветградськогму земському реальному училищі. Він був створений на основі колекції наочних предметів історико-географічного музею при Єлизаветградськогму земському реальному училищі. У 1882 р. це училище змінило статус з приватного на державне. Однією з умов зміни статусу цього навчального закладу було створення історико – етнографічного музею наочних предметів, а вже наступного 1883 року викладач історії та географії цього училища, Володимир Миколайович (1855-1898) був призначений завідувачем «историко-географическим музеем», що був ним створений [13]. Через кілька років у доповіді ревізійної комісії по ЄЗРУ за 1887 р. говориться, що «в нынешнем году положено основание местному археологическому и этнографическому музею, устроеному по инициативе и личным трудом преподавателя истории и географии В.Н. Ястребова прискромной затрате со стороны правления 50 руб. на раскопки». Власне вважається, що це перше фінансування археологічних досліджень правлінням училища, яке мало поповнити археологічну колекцію училища й дало початок офіційному існуванню музею та його колекції. Початково, як відзначає сам В.М Ястребов, музейна колекція формувалася за рахунок добровільних пожертвувань і складалася з наочних посібників для викладання історії та географії, а також невеличкого «археологічного» зібрання з 342 предметів, в тому числі: 270 монет і медалей, 57 документів, рукописної карти Єлисаветградської провінції XVIII ст., 3-х кам'яних молотків і цінне зібрання предметів скіфської епохи з кургану поблизу села Мартиноша Єлисаветградського повіту. Як бачимо, з так званої «археологічної колекції», абсолютна більшість була представлена нумізматичним матеріалом, решта - пам`ятки, що репрезентують інші допоміжні історичні дисципліни: сфрагістику, палеографію, картографію і в дуже не значній кількості – археологію [14].

Після смерті Володимира Миколайовича, в грудні 1898 року, музей практично припинив своє існування, а колекція розійшлася по рукам [9].

Справу Ястребова В.М. майже через 20 років продовжив громадський діяч, археолог та етнограф Павло Захарович Рябков (1848-1926). За його ініціативи відновленням музею та його колекції у 1913 році займалося «Товариство розповсюдження писемності та ремесел», якому передали рештки зібрання реального училища. Але реалізації цих планів завадила Перша світова війна [12].

Наступний етап відновлення музейного колекціонування як і розвитку музейної справи припадає на радянський час. У 1922 році на основі наявних колекцій було відкрито історико-археологічний музей, який очолював П.З. Рябков. У 1929 році округовому історико-археологічному музею було виділено приміщення на вулиці Леніна, 40, де він знаходиться і нині, а у 1939 році музею надано статус обласного краєзнавчого, колекція якого включала й нумізматичну складову. До ІІ світової війни у більшості обласних музеїв не велися книги надходжень та паспортизація предметів колекцій, що не дозволяє встановити ні довоєнний склад їх колекцій, ні втрати які вони зазнали під час війни. Кіровоградський обласний краєзнавчий музей не був винятком із цього правила. Постанови Кіровоградського бюро обкому партії від 01.05.1946 року констатує: «До Великої Вітчизняної війни фонди краєзнавчого музею мали у своєму розпорядженні велику кількість предметів історії, археології, етнографії, нумізматики, флори і фауни, рукописи Саксаганського, Кропивницького, картини російських, голландських, французьких, українських художників, бібліотеку з великою кількістю книг XV-XVIII ст. У період окупації експозицію було розібрано і експонати звалено у підвал музею. Картини, вишивки, килими, книги, порцеляну, цінні вази окупанти вивезли до Німеччини. Музейну документацію знищили. Загалом музей втратив більше 10 000 експонатів». Після визволення міста і відновлення діяльності музею,

його фонди істотно поповнилися новими колекціями [5]. Вже у вересні 1946 року музей було відкрито для відвідувачів.

У 1994 році музей успадкував колекцію збирача предметів старовини і мистецтва Олександра Ільїна. На початок XXI ст. у фондах музею налічувалося близько 80 тисяч пам'яток з історії, археології, нумізматики, етнографії, історії та природи краю від найдавніших часів до сучасності.

У 2019 р. до фондів музею жителькою м. Кропивницький Єгурновою М.А. було передано невелику нумізматичну колекцію монет іноземного походження к. XIX-XX ст. Вона включає 5 дрібних монет: 2 Королівства Румунія, 2 Речі Посполитої та Республіки Польща, 1 Австро-Угорщини.

Найдавнішою є монета Австро-Угорщини – 20 геллерів 1894 р.

Дві монети Королівства Румунія по «20 баней» датуються 1905 та 1906 рр., тобто початком XX ст.

Монета Речі Посполитої номіналом «20 грошей» датується 1923 р. а монета Республіки Польща також номіналом «20 грошей» 1949 р.

Усі монети дрібного номіналу мають круглу форму, виготовлені з легких металів або їх сплавів (цинк, нікель, мідно-нікеливий сплав) у техніці карбування. Особливістю монет Королівства Румунія є наявність круглого отвору в центральній частині монети. Іконографія монет відповідає традиційним зображенням та текстам країн грошову систему яких вони представляють.

Отже, можна зробити висновок, що невелике поповнення нумізматичної колекції Кіровоградського обласного краєзнавчого музею 2019 р. репрезентує обігові монети дрібного номіналу трьох європейських країн к. XIX – трет. чв. XX. Зазначені монети відображають традиції монетного карбування Австро-Угорщини, Польщі та Королівства Румунія. Вони виступають у ролі державного документа, що репрезентує особливості грошового обігу в зазначених країнах, культуру та технологію їх виготовлення, мистецтво епіграфічного оформлення, що відповідають часу їх використання.

Додаток.

1.Монета обігова «20 бань», Королівство Румунія (1867 – 1924 рр.). Автор: Антон Шорфф. Час і місце створення: 1905 рік, місто Гамбург, Німеччина. Розміри (см/мм): d – 2,5 см. Матеріал: мідно-нікелевий сплав. Техніка: карбування. Має форму кола з отвором всередині. На аверсі монети зображено текст ROMANIA та викарбувано зображення корони у верхній частині. На реверсі зображено текст 20 BANI 1905, рік карбування відокремлено з двох сторін п’ятикутною фігурою, всередині якої викарбувана п’ятикутна зірка..

2. Монета обігова «20 бань», Королівство Румунія (1867 – 1924 рр.)

Автор: Антон Шорфф. Час і місце створення: 1906 рік, місто Гамбург, Німеччина. Розміри (см/мм): d – 2,5 см. Матеріал: мідно-нікелевий сплав. Техніка: карбування. Має форму кола з отвором всередині. Аверс: текст ROMANIA та зображення корони у верхній частині. Реверс: текст 20 BANI 1906, рік карбування відокремлено з двох сторін п’ятикутною фігурою, всередині якої викарбувана п’ятикутна зірка.

3. Монета обігова «20 грошей», Республіка Польща (1919 – 1939 рр.). Час і місце створення: 1923 рік, місто Варшава, Республіка Польща. Розміри (см/мм): d – 2 см. Матеріал: цинк. Техніка: карбування. Аверс: рік карбування 1923, текст RZECZPOLITA POLSKA та державний герб у верхній частині. Реверс: текст 20 GROSZY обрамлений орнаментом дубового листя.

4. Монета обігова «20 грошей», Республіка Польща (1949 р.). Час і місце створення: 1949 рік, місто Варшава, Республіка Польща. Розміри (см/мм): d – 2 см. Матеріал: мідно-нікелевий сплав. Техніка: карбування. Аверс: рік карбування 1949, у центрі державний герб з текстом навколо нього RZECZPOLITA POLSKA. Реверс: текст 20 GROSZY, а під ним сплетіння колосків пшениці.

5. Монета обігова «20 геллерів», Австро-Угорська імперія. Час і місце створення: 1911 рік, місто Відень, Австро-Угорська імперія. Розміри (см/мм): d – 2,1 см. Матеріал: нікель.

Техніка: карбування. Аверс: малий імператорсько-королівський герб (1867-1915 рр.). Реверс: текст 20 та рік карбування 1911 в обрамлені геральдичним щитом.

Список літератури

1. Адаменко В.М. Розвиток музейної справи на Кіровоградщині // Міжвузівська наукова конференція з історичного краєзнавства. — Кіровоград. 1990. — С. 69 - 71.
2. Григор'єва Т. Кіровоградщина музейна // Культура і життя. — 2003. — 2 липня. — С.2.
3. Здір Л. Музеї Кіровоградщини — у літописі української культури // Народне слово. — 2005. — 15 лютого. —С.4.
4. Кіровоградський краєзнавчий музей. Путівник. — Дніпропетровськ, 1969. — 104с.
5. Колесник Л. Пізнаючи старовину — пізнаємо себе: про Кіровоградський обласний краєзнавчий музей // Вечірня газета. — 2002. — 17 травня. — С.9.
6. Левочко В. Музеї України. Кіровоградщина // Ведомости. — 2005. — 18 лютого. — С.4.
7. Матівос Ю. Землемір, просвітитель, культурний діяч //Кіровоградська правда. — 1998. — 30 липня. — С.3.
8. Пархомчук В. Краєзнавчий музей в Кіровограді // Вечірня газета. — 1995. — 21 травня. — С.2.
9. Печериця Т. Особовий фонд П.З. Рябкова. // Вісник Київського національного університету ім.. Т. Шевченка. —2001. — вип.57 — С.51.
10. Послужной список 2 апреля 1894 года. — ДАКО. Ф.60.Оп.1.Арх.106.
11. Рябков П.З. Музейное дело в Елисаветграде: прежде и теперь// Фонд рукописів Кіровоградського обласного краєзнавчого музею. — С.1.
12. Технічна освіта на Кіровоградщині: історичний нарис. – Кіровоград: «Імекс-ЛТД», 2009. – 240 с.
13. Тупчієнко М.П. Музеєзнавчі аспекти археологічної спадщини В.М. Ястребова. // Український музей при навчальному закладі: історія і сучасність. Матеріали науково-методичної конференції. Кіровоград. Вид-во КОП. ім.. В. Сухомлинського. 2008 р. – С. 109-118.
14. Хоменко І. Наш музей: вісті з Кіровоградщини // Літературна Україна. — 2004. — 22 липня. —С.2.
15. Черновые отчеты о состоянии земского реального училища в 1883 - 1886 годах. ДАКО. Ф. 50. Оп.1. Арх. 39.
16. Ястребов В.М. Дані про археологічну колекцію при Єлисаветградському земському реальному училищі // Єлисавет. — 1992. — 30 вересня. —С.2.
17. Яцук М. Обласний художній музей — візитна картка міста Кіровограда // Коммивояжер. — 2002. — №7. — С.21.

УДК 336.14

В. Мудренко, магістр гр.ФС-18МЗ
Центральноукраїнський національний технічний університет

ПРОБЛЕМИ ФОРМУВАННЯ ФІНАНСОВИХ РЕСУРСІВ МІСЦЕВИХ БЮДЖЕТІВ В УКРАЇНІ

У статті досліджено теоретичні аспекти сутності категорії «місцевий бюджет» та «фінансові ресурси», особливості формування та використання фінансових ресурсів місцевих бюджетів в Україні. Розглянуті проблеми управління доходами та видатками місцевих бюджетів, а також запропоновані напрями ефективного їх використання в Україні.

фінансові ресурси місцевого бюджету, місцеві бюджети, місцеві фінанси, принципи управління місцевих фінансів, фінанси територіальних громад, система місцевого самоврядування

Основне завдання розвитку України як демократичної держави полягає у задоволенні потреб людини та забезпеченні необхідних умов для зростання її добробуту. Такі умови створюються, насамперед, на місцевому рівні і залежать від забезпечення місцевого бюджету фінансовими ресурсами.

Фінансові ресурси місцевого бюджету – це створені в результаті розподілу і перерозподілу валового внутрішнього продукту грошові доходи, грошові нагромадження і резерви грошових коштів (частина яких концентрується у відповідних фондах), необхідні

органам місцевого самоврядування для виконання покладених на них функцій і завдань з метою забезпечення соціально-економічного функціонування та розвитку територіальної громади і задоволення їх спільних інтересів [1].

Науково-практичного значення набуває потреба визначення та обґрунтування складових елементів фінансових ресурсів місцевого самоврядування. Проблеми місцевих фінансових ресурсів та управління ними посідають важливе місце в дослідженнях зарубіжних науковців, зокрема Дж. Аронсона, Р. Аграноффа, А. Вагнер, Р. Масґрейва, Ч.Тібу, Дж. Хіллі, та інших.

До українських науковців, які займаються проблематикою структуризації фінансових ресурсів місцевих бюджетів належать: Н.В. Васильєва, Н.М. Гринчук, Т.М.Дерун, В.С. Куйбіда, А.Ф. Ткачук та ін.[2]. Хоча вони мають різні точки зору щодо її вирішення проблем формування та розподілу фінансових ресурсів. Тому, у фінансовій системі потрібно в подальшому проводити теоретичні дослідження, пов'язані із управлінням формування використання фінансових ресурсів місцевих бюджетів в Україні, враховуючи вітчизняних і зарубіжний досвід.

Метою статті є поглиблення теоретичних положень, обґрунтування проблем та практичних заходів щодо вдосконалення управління формуванням і використанням фінансових ресурсів місцевих бюджетів в Україні.

Місцеві бюджети – це план формування та використання фінансових ресурсів територіальних одиниць чи територіальної громади протягом бюджетного періоду, а також є складовою частиною бюджетної системи України. Місцевими бюджетами є бюджет Автономної Республіки Крим, обласні, районні, міські, селищні, сільські бюджети та бюджети об'єднаних територіальних громад, що створюються згідно із законом та перспективним планом формування територій громад. Нині налічується 8331 місцевий бюджет (без місцевих бюджетів Автономної Республіки Крим та м. Севастополя) (див. рис. 1.) [5].

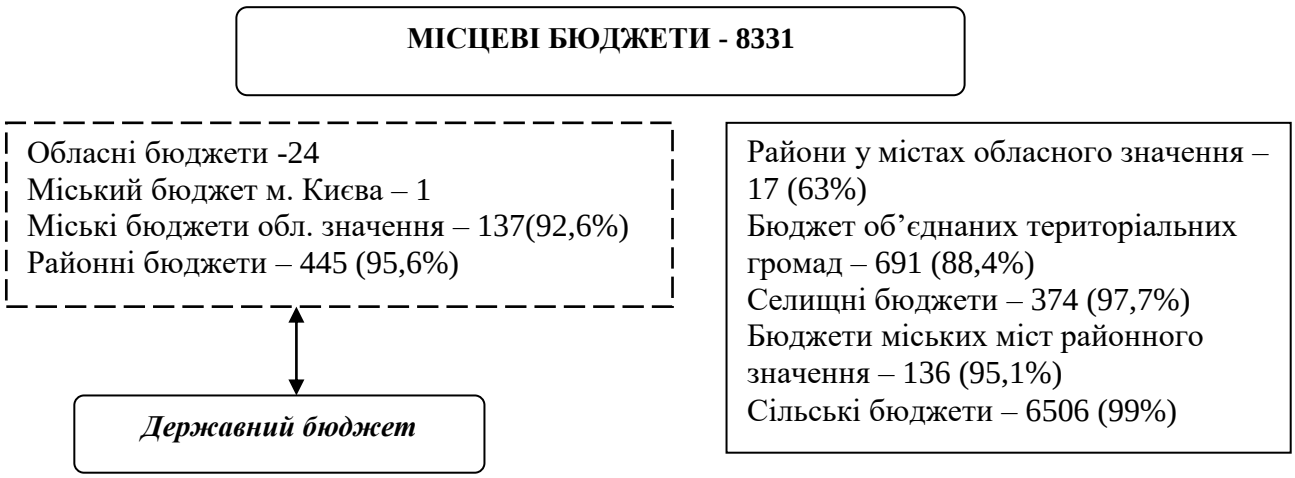


Рисунок 1- Структура і склад місцевих бюджетів в Україні станом на 2019 рік[5]

Вивести точну цифру місцевих бюджетів доволі складно, оскільки не кожне село має окремий бюджет. Якщо в селі є органи місцевого самоврядування (сільрада), то останні формують окремий бюджет. Якщо ж сільради нема, то й окремого бюджету не буде (в такому разі фінансування здійснюватимуть з районного бюджету). Тобто, кількість місцевих бюджетів в Україні не відповідає кількості адміністративно-територіальних одиниць.

Сутність місцевого бюджету, як економічної категорії, реалізується через його функції, які показані на рисунку 2.

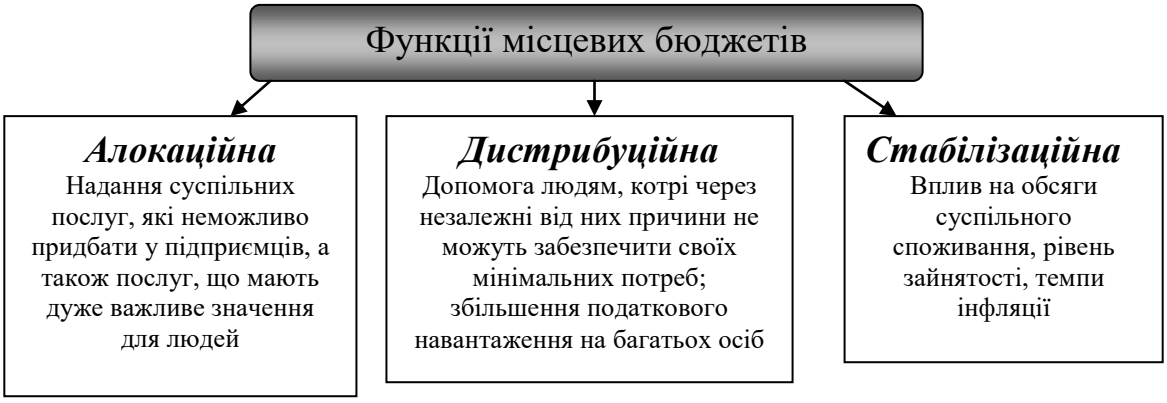


Рисунок 2 - Функції місцевих бюджетів[6]

Функції місцевих фінансів визначають їхню роль та значення у фінансовій системі держави. Головне завдання під час формування місцевих фінансів – це розмежування завдань, які має вирішувати центральна влада, і тих, що покладають на місцеві органи.

Роль місцевих бюджетів у соціально-економічному розвитку регіону проявляється в тому, що у місцевих бюджетах акумулюється частина фінансових ресурсів, яка створюється на визначеній території і забезпечує фінансову базу місцевим органам влади для реалізації своїх повноважень. З іншого боку, створення середовища для формування фінансової бази є головним для місцевих органів влади. Зазвичай, у різних адміністративно-територіальних одиницях фінансова база різна. Інколи вона обмежена. Через це наповненість місцевих бюджетів залежить, з одного боку, від рівня економічного розвитку регіону, зокрема від повноти використання його економічного потенціалу, а з іншого – від цільового, раціонального та ефективного використання бюджетних ресурсів.

Місцеві фінансові ресурси – це сукупність фондів коштів, що формуються в процесі розподілу ВВП і направляються на економічний і соціальний розвиток адміністративно-територіальних одиниць.

Державна бюджетна політика щодо місцевих бюджетів та міжбюджетних відносин у 2019-2021 роках спрямована на розбудову спроможної, ефективної, прозорої та підзвітної системи управління місцевими фінансами, орієнтованої на досягнення цілей сталого економічного та соціального розвитку.

Бюджет на 2019 рік формується на підставі чинного бюджетного та податкового законодавства з урахуванням окремих законодавчих змін, а також виходячи з параметрів, визначених основними напрямками бюджетної політики на 2019-2021 роки.

Для формування місцевих бюджетів слід враховані основні прогнозні макропоказники економічного і соціального розвитку України на 2019 рік, а саме:

- номінальний ВВП – 3946,9 млрд грн;
- темп зростання реального ВВП – 103,0 %;
- індекс споживчих цін – 107,4%;
- фонд оплати праці найманих працівників і грошове забезпечення військовослужбовців – 1142,7 млрд грн.[6]

При плануванні місцевих бюджетів важливими параметрами є розміри державних соціальних стандартів, що безпосередньо впливає на дохідну і на видаткову частини місцевих бюджетів. На 2019 рік встановлені наступні розміри:

- розмір мінімальної заробітної плати – 4173 грн;
- розмір посадового окладу працівника І-го тарифного розряду ЄТС – 1921 грн;
- прожитковий мінімум на одну особу в розрахунку на місяць: з 1 січня 2019 року – 1853 грн, з 1 липня – 1936 грн, з 1 грудня – 2027 грн.

На обсяги фінансових ресурсів, які органи місцевого самоврядування можуть залучати та використовувати, впливають такі чинники:

- розподіл повноважень між органами державної влади і місцевим самоврядуванням;
- розподіл дохідних джерел державного та місцевого бюджетів;
- чинна система оподаткування, перелік податків і внесків, їх ставки, пільги;
- специфіка міжбюджетних відносин і порядок надання трансфертів місцевими бюджетами із державного бюджету;
- стан фінансового ринку країни та реальні можливості органів місцевого самоврядування у сфері використання запозичених (кредитів) і залучених коштів (місцевих позик);
- склад і фінансовий стан підприємств та інших суб'єктів господарювання, які належать до місцевого господарства.

Доходи місцевого бюджету є однією з ключових складових частин фінансових ресурсів органів місцевого самоврядування. Саме дохідна частина місцевих бюджетів виступає фінансовою основою органів місцевого самоврядування, яка формується за рахунок власних та закріплених джерел, загальнодержавних податків і зборів, трансфертних платежів.

Згідно із Законом «Про місцеве самоврядування в Україні», органи місцевого самоврядування самостійно розробляють, затверджують і виконують відповідні місцеві бюджети.

У складі доходів місцевих бюджетів слід вирізняти:

– доходи, отримані на певній території (власні доходи);

– мобілізовані доходи на інших територіях і спрямовані до певного бюджету через механізм вирівнювання;

– передані доходи з бюджету вищого рівня (бюджетні трансферти);

– загальнодержавні доходи, законодавчо закріплені за місцевими бюджетами;

– інші доходи [4].

Передбачено істотне збільшення надходжень до місцевих бюджетів, основними джерелами котрих є: податок на доходи фізичних осіб (ПДФО) (60 %), рентна плата за використання лісових ресурсів (50 %), використання води (50 %), користування надрами (25 %), державне мито, податок на майно, єдиний податок, туристичний збір, плата за ліцензії, плата за державну реєстрацію, надходження від орендної плати, штрафні санкції і штрафи, та за рахунок інших джерел (ст. 64 Бюджетного кодексу України).

Збільшити надходження планувалось також до спеціального фонду місцевих бюджетів за рахунок коштів до бюджету розвитку, від відшкодування втрат виробництва, стягнень за шкоду, заподіяну довкіллю (70 %), екологічного податку (80 %), цільових і спеціальних внесків та інших джерел (ст. 69 Бюджетного кодексу України)[3].

Варто зазначити, що значною проблемою функціонування місцевих бюджетів є недотримання принципу податкової еквівалентності. Так, основною статтею надходжень до місцевих бюджетів, як було показано вище, є податок на доходи фізичних осіб (надходження цього податку повністю зараховуються до місцевих бюджетів). Проте місцеві органи влади позбавлені можливості приймати рішення щодо податкового регулювання (встановлення ставки податку, встановлення нормативів розмежування надходжень між місцевими бюджетами різного рівня, надання відстрочок і розстрочок тощо). Надходження податку на доходи фізичних осіб зараховуються до місцевого бюджету за місцем роботи платника податку (як правило, це міста), хоча найважливіші неринкові послуги (дошкільна та шкільна освіта, охорона здоров'я, соціальне забезпечення) платники отримують за місцем проживання [1].

Крім того існують інші гострі проблеми, що становлять перешкоди для досягнення місцевим бюджетам фінансової самодостатності та потребують вирішення і постійного контролю з боку держави:

1. Підприємства комунальної власності у містах змінюють місце реєстрації підприємств, установ, організацій, як правило – перереєструються у селищах і селах, що спричинює недоотримання сум ПДФО місцевими бюджетами міст[10].

Причинами таких дій є різниця у ставках орендної плати та комунальних послуг між містом та селом (у сільській місцевості тарифи нижчі).

За результатами такої перереєстрації керівники підприємств сплачують податок на доходи фізичних осіб до іншого бюджету, в тому числі і посеред бюджетного року. Це негативно впливає на ефективність виконання бюджетного процесу, адже виникає необхідність вносити зміни до місцевого бюджету в частині зменшення дохідної частини та перегляду обсягів і напрямків видатків. Також виникає дисбаланс у питанні утримання осіб, що працюють за місцем реєстрації даної установи і на місці мають отримувати відповідні послуги.

2. Місцеві бюджети недоотримують суми земельного податку внаслідок того, що 70 % дрібних аграріїв (із 43 тисяч одиниць) отримують і не декларують доходи[11].

Причини існування нелегального агроринку наступні: часті зміни у податковому законодавстві (відсутність стабільності в категоріях, до яких відносять платників єдиного податку, що веде до ігнорування необхідності зміни категорії); загрози ринку від дій трейдерів (аграрії не знаються на особливостях експорту зерна, тому продають його трейдерам, які отримують 10 % загального доходу від зернового експорту у $ 15 млрд.); недосконаліть оподаткування обігу ріллі (оподаткування здійснюється на основі нормативної грошової оцінки землі, а для земель сільськогосподарського призначення, що знаходяться за межами населених пунктів, наразі ще не проведено таку оцінку, для них затверджено тільки ставки податку на землю, що діють з 01.01.19 р., і це дає можливість проводити недостовірну оцінку, внаслідок чого відбувається недоотримання коштів до бюджетів)[12], обмеження НБУ на готівкові розрахунки у валюті. У результаті недекларування доходів місцеві бюджети недоотримують щороку 10 млрд грн.[13]

3. На територіях громад наявні об’єкти безхазяйного, нерентабельного майна, та відумерлої спадщини (майно, власник якого помер, а спадкоємці за заповітом і за законом відсутні, усунуті від права спадкування або не прийняли спадщину чи відмовилися від її прийняття). В Україні відсутній реєстр такого виду майна. Натомість існує Єдиний реєстр суб’єктів господарювання, які можуть здійснювати реалізацію безхазяйного майна та майна, що переходить у власність держави, на 2019 рік, наданий ДФС. За цим реєстром станом на 13.03.19 р., таких суб’єктів 28[14].

Реалізація такого майна на аукціонах дала б змогу отримувати додаткові кошти до місцевих бюджетів. Органи місцевого самоврядування можуть звертатись до Єдиного реєстру суб’єктів господарювання, які зможуть посприяти в питаннях реалізації безхазяйного, нерентабельного майна та відумерлої спадщини.

Окремі громади вже здійснюють процес виявлення такого майна, проведення його обліку, реєстрації та починають реалізовувати його на аукціонах, а кошти направляють на розвиток громад.

4. Ще одна серйозна проблема сьогоднішнього дня – державні повноваження, делеговані органам місцевого самоврядування. В Україні делеговані повноваження тільки на 70 % забезпечуються державою. Решту коштів місцевий бюджет має вишукувати самостійно.

Притому, що вага місцевих податків і зборів у надходженнях до місцевого бюджету дуже незначна. Як наслідок існування таких проблем в першу чергу зумовлюють виникнення дисбалансу в самих місцевих бюджетах, а саме виникає дефіцит бюджетних коштів, по-друге не вирішуються важливі життєві проблеми людей, відбувається занепад всього місцевого господарства.

Для збільшення в місцевих бюджетах частки власних доходів, зменшення залежності від фінансової допомоги, досягнення збалансованості бюджетів, підвищення ефективності управління місцевими фінансами необхідно здійснити поступовий перехід до децентралізації

управління місцевими бюджетами, що надасть можливість місцевим фінансам стати більш самостійним інститутом.

Для вирішення проблем, що виникають при формуванні місцевого бюджету доцільно запропонувати такі заходи:

1) залучення інвестицій, в тому числі іноземних інвесторів;

2) підтримка розвитку малого та середнього бізнесу;

3) сприяння розширенню внутрішніх і зовнішніх ринків збуту продукції місцевих виробників;

4) ініціювання реформування податкового законодавства у напрямку зниження податкового тиску на місцеві підприємства;

5) проведення частини видатків за рахунок власних надходжень бюджетних установ, що дасть змогу направляти кошти загального фонду на розвиток бюджетних галузей.

Отже, ресурси – «інструменти» органів місцевого самоврядування для виконання їх головної функції – розвитку території, а головна задача органів місцевого самоврядування – обрати серед наявних такі ресурси, використання яких приведе до розвитку.

Враховуючи існуючи проблеми формування дохідної частини місцевих фінансів, ми повинні докорінно змінити пріоритети їх побудови, а саме: поставити інтереси місцевих бюджетів на перше місце. Це повинно здійснюватися шляхом зміцнення дохідної бази місцевих бюджетів, які є фінансовою основою місцевого самоврядування і всієї бюджетної системи України. Для того, щоб місцеві бюджети стали основою фінансової самостійності місцевої влади, потрібно здійснити ряд заходів. У першу чергу необхідно чітко розподілити компетенції між органами центральної влади, регіонального та місцевого самоврядування і поступово переходити до децентралізації державних фінансів.

На державному рівні повинні фінансуватися лише ті видатки, що пов’язані із забезпеченням загальнодержавних потреб. Фінансові проблеми місцевого рівня ефективніше вирішують місцеві органи влади за рахунок коштів власних бюджетів. Крім того, для наповнення дохідної частини місцевих бюджетів потрібно: змінити базу оподаткування податку на нерухоме майно, дозволити місцевим органам встановлювати нові економічно обґрунтовані неподаткові платежі, проводити переоблік та індексацію земельних ділянок, ліквідувати заборгованість із заробітної плати та збільшити розмір заробітної плати, здійснювати обов’язкове середньострокове планування доходів місцевих бюджетів.

Список літератури

1. Алєксєєв І. В., Лопушняк Г. С., Ливдар М. В. Бюджетний механізм і соціально-економічний розвиток регіонів : монографія. Львів : Ліга-Прес, 2014. 248 с.
2. Васильєва Н. В., Гринчук Н. М., Дерун Т. М., Куйбіда В. С., Ткачук А. Ф. Місцевий бюджет і фінансове забезпечення об’єднаної територіальної громади: навч. посіб. / [Н. В. Васильєва, Н. М. Гринчук, Т. М. Дерун, В. С. Куйбіда, А. Ф. Ткачук] – К.: – 2017. – 119 с.
3. Бюджетний кодекс України від 08.07.2010 № 2456-VI [електронний ресурс]. – режим доступу : http://zakon2.rada.gov.ua/laws/show/2456-17
4. Децентралізація. Місцеві бюджети 159 об’єднаних територіальних громад : фін.-аналіт. матеріали / Каб. Міністрів України, М-во регіон. розвитку, буд-ва та ЖКГ України ; підгот. Я. М. Казюк ; консультац. підтримка Я. Джийкіч. – [Київ : б. в.], 2016. – 190 с.
5. Офіційний веб-сайт Міністерства фінансів України [електронний ресурс]. – режим доступу : http://minfin.gov.ua
6. Полинюк Н.І. Механізм формування фінансових ресурсів місцевих органів управління в умовах демократизації суспільства / Н.І. Полинюк // економічний аналіз. – 2016. – № 1. – т. 26. – с. 65–72
7. Податковий кодекс України від 02.12.2010 р. № 2755-VI [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/2755-17
8. Ползікова Г.В. Механізми регіонального податкового менеджменту в умовах децентралізації влади в Україні // Інвестиції: практика та досвід. – 2016. – № 22. – С. 49-53.
9. Разумова Г.В. Аналіз сфери міжбюджетних відносин в Україні (на прикладі м. Дніпро) // Економічний простір. – № 112. – Дніпропетровськ: ПДАБА, 2016. – С. 112-121.

10. Асоціація міст України [Електронний ресурс]. – Режим доступу: http://www.auc.org.ua/novyna/asociaciya-mist-ukrayiny-peredala-do-dfs-perelik-pidpryyemstv-shcho-ne-splachuyut-pdfo
11. Українське агентство "Українські національні новини"[Електронний ресурс]. – Режим доступу: http:// unn.com.ua
12. Земельний податок: зміни з 1 січня 2019 року [Електронний ресурс]. – Режим доступу: www.medoc.ua/uk/blog/zemelnij-podatok-zmini-z-1-sichnja-2019
13. Інструменти забезпечення фінансової самодостатності громад [Електронний ресурс]. – Режим доступу: http:// niss.gov.ua/en/node/183
14. Офіційний сайт ДФС [Електронний ресурс]. - Режим доступу: http://sfs.gov.ua/dovidniki--reestri--perelik/reestri/363146.html

УДК 338.58

І. Орехова, магістр гр. ФС-18МЗ
Центральноукраїнський національний технічний університет

НАПРЯМИ ПІДВИЩЕННЯ ПРИБУТКОВОСТІ ПІДПРИЄМСТВА

Розглянуто підходи щодо категорії прибуток, прибутковість.
прибуток, прибутковість, рентабельність

На підприємстві прибуток є потужним важелем динамічного розвитку виробництва, і тому головним завданням розвитку підприємств є вироблення ефективних методів управління підприємством у процесі здійснення підприємницької діяльності, а саме у застосуванні методів управління прибутком та збільшенні прибутковості підприємства.

Одержаний підприємством прибуток дає можливість виконувати свої функції і спрямовувати кошти на власний розвиток, на соціальні потреби своїх працівників, створювати фонди матеріального заохочування та на інші потеби передбачені чинним законодавством. Тому у сучасних умовах прибуток стає не тільки важливим показником, а й метою роботи кожного підприємства незалежно від роду діяльності.

Дослідженню питання забезпечення управління прибутком та рентабельністю суб'єктів господарювання приділяється значна увага як серед вітчизняних, так і серед зарубіжних науковців, таких як: Р.Р.Антонюк, О.І. Бала, О.В. Богоявленський, Л.М. Борщ, А.В. Буряк, Л.М. Волощенко, О.І. Гуторов, О.А. Коваль, М.І. Савлук, В.В. Зимовець, І.Ю. Крамаренко, О.Л. Лаврик, А.М. Поддерьогін та інші.

Перед сучасними підприємствами дуже гостро постає питання отримання прибутку і підвищення ефективності виробництва. Формування, використання та зростання прибутку підприємства мають свої особливості в умовах ринкової економіки, що зумовлює необхідність поглибленого дослідження теоретичних засад зростання прибутковості підприємства, її впливу на темпи та обсяги суспільного відтворення. На сучасному етапі необхідний якісно новий підхід до теоретичного висвітлення і практичного обґрунтування рекомендацій щодо збільшення шляхів та напрямів прибутковості підприємства.

Безумовно, сучасні науковці категорію «Прибуток» трактують по різному, але ми схиляємось до думки, що прибуток – це кінцевий фінансовий результат діяльності підприємств і в загальному вигляді є різницею між виручкою від реалізації продукції і собівартістю реалізованої продукції. Між поняттям прибуток та прибутковість є тісний діалектичний взаємозв'язок. Так, прибуток – це показник для зображення економічного ефекту в абсолютних показниках, а прибутковість – показник для зображення економічної ефективності діяльності суб'єкта господарювання [2].

Р.Р. Антонюк [1] визначає прибутковість як здатність підприємства генерувати позитивний фінансовий результат від здійснення господарської діяльності, який полягає в перевищенні доходу над здійсненими витратами, при чому в розмірі достатньому для ефективного подальшого функціонування. Так, основою прибутковості є сам прибуток, який у цілому й визначає результат фінансово-господарської діяльності підприємств. Отже, прибутковість – це показник, який характеризує ефективність діяльності підприємства з точки зору здатності його приносити прибуток та забезпечувати ефективне відтворення використаних ресурсів.

Процес управління прибутковістю на підприємстві має відбуватися у певній послідовності і забезпечувати реалізацію головної мети і основних завдань цього управління. Управління прибутком являє собою цілеспрямований, систематичний процес підготовки, оцінки, відбору та реалізації альтернативних управлінських рішень з усіх питань його формування, розподілу та використання на конкретному підприємстві. Система управління прибутком може функціонувати тільки за наявності відповідних даних, на основі яких можна налагодити постійний моніторинг процесу формування прибутку; оцінювати рівень операційного та валового прибутку; аналізувати чинники впливу на обсяг прибутку. Джерелами інформації у даному разі виступають дані маркетингового аналізу, бухгалтерського та управлінського обліку [3]. Головною метою управління прибутком є визначення шляхів найбільш ефективного його формування та оптимального розподілу, що спрямовані на забезпечення розвитку діяльності підприємства та зростання його ринкової вартості

Основною метою політики управління прибутковості підприємства є максимізація прибутку підприємства. В даний час в умовах ринкової економіки для аналізу фінансових результатів необхідно загальноприйняту класифікацію факторів зростання прибутку розширити та деталізувати. Це дозволить більш докладно підійти до питань формування, розподілу і використання прибутку, наступної його максимізації. Можна запропонувати наступну класифікацію резервів підвищення прибутку підприємства, а також факторів і шляхів реалізації цих резервів.

Політика управлінням прибутку на підприємстві повинна бути спрямована на максимізацію розміру позитивного фінансового результату після виконання комплексу завдань що сприяють зростанню обсягів його діяльності, ефективного управління витратами, підвищення ефективності використання матеріально-технічної бази, оптимізації складу та структури обігових коштів, підвищення продуктивності праці та системи управління суб’єктом господарювання.

Отже, система управління прибутком дає змогу вирішувати такі завдання:

− сприяти максимізації розміру прибутку, що сформований відповідно до ресурсного потенціалу підприємства;

− забезпечувати оптимальну пропорційністьі між рівнем прибутку і допустимим рівнем ризику;

− сприяти забезпеченню високої якості прибутку, що формується;

− забезпечувати виплати необхідного рівня доходу на інвестований капітал власникам підприємства;

− забезпечення формування відповідного обсягу фінансових ресурсів за рахунок прибутку відповідно до завдань розвитку підприємства на майбутній період;

− сприяти постійному зростанню ринкової вартості підприємства;

− стимулювати персонал, щодо участі у розробці ефективних програм, які сприятимуть покращенню прибутковості.

Для забезпечення чіткої дії механізму управління прибутком підприємства необхідно проаналізувати чинники впливу на прибуток підприємства. Прибуток формується під впливом великої кількості взаємозалежних чинників, що впливають на результати діяльності підприємства по-різному: одні – позитивно, інші – негативно. Серед зовнішніх чинників можна виділити такі: економічні умови господарювання, місткість ринку, платоспроможний

попит споживачів, державне регулювання діяльності підприємств та інше. Особливе значення має рівень, динаміка і коливання платоспроможного попиту, тому що він визначає стабільність одержання прибутку.

Основними задачами управлінням прибутковістю підприємства є такі: забезпечення максимізації розміру прибутку, що формується, і який відповідає ресурсному потенціалу суб'єкта господарювання та ринковій кон'юнктурі; забезпечення оптимальної пропорційності між рівнем прибутку, що формується, та допустимим рівнем ризику; забезпечення високої якості прибутку, що формується; забезпечення постійного збільшення ринкової вартості підприємства; підтримка конкурентоспроможності у довгостроковому періоді; забезпечення ліквідності підприємства та його платоспроможності; підтримка інвестиційної привабливості.

Механізм управління рентабельністю підприємства є частиною загальної системи управління підприємством, що забезпечує вплив на чинники, від яких залежить загальний результат діяльності суб'єкта. Процес формування механізму управління необхідно розпочати з характеристики його складників, проведення детального аналізу рентабельності, визначення факторів, що мали вплив на зміну показників, розроблення шляхів їхнього зростання.

Розроблення якісного механізму управління рентабельністю підприємства дає змогу виявити велику кількість тенденцій розвитку, вказати керівництву підприємства шляхи подальшого успішного функціонування, вказати на помилки в господарській діяльності, а також виявити резерви зростання прибутку, що в кінцевому підсумку дає змогу підприємству більш успішно здійснювати свою діяльність. Під час формування механізму управління рентабельністю підприємства важливо визначитися з типом стратегії підвищення його показників. Це складний і багатогранний процес, який включає у себе глибокий економічний аналіз виробничих і фінансових показників за період, що передував плановому періоду, досягнення максимальної узгодженості з кількісними й якісними показниками плану випуску продукції (виконання робіт, послуг), її реалізації, собівартості, врахування наявних резервів збільшення випуску продукції, зниження витрат на виробництво, особливо непродуктивних і позареалізаційних витрат і збитків [3].

Для підвищення рівня прибутку на підприємстві доцільно проводити заходи в такій послідовності: організаційні (удосконалення виробничої структури, удосконалення організаційної структури управління, диверсифікація виробництва, реструктуризація виробництва тощо) – технічні (оновлення техніко-технологічної бази, переозброєння виробництва, вдосконалення виробів) – економічні важелі та стимули (удосконалення тарифної системи, форми і системи оплати праці, прискорення обігу оборотних коштів тощо). Якщо почати проводити зміни не в такому порядку, то позитивні зрушення в ефективності діяльності будуть малопомітними або відсутніми взагалі [3].

Внутрішні фактори збільшення рентабельності є суб'єктивними, адже на них підприємство може впливати безпосередньо. До цих факторів можна віднести сукупність дій та заходів, що сприятимуть підвищенню ефективності діяльності підприємства, а саме:

- збільшення обсягів реалізації продукції;
- підвищення продуктивності працівників;
- зростання ефективності використання основних фондів;
- оптимізація складу і структури оборотних коштів;
- введення ефективної маркетингової політики;
- підвищення якості продукції та її конкурентоспроможності.

Одним із резервів росту рентабельності підприємства є збільшення обсягів реалізації товарної продукції, адже чим більше продукції реалізується, при інших рівних умовах, тим більшою є сума прибутку, що має позитивний вплив на рентабельність.

При цьому підвищення рентабельності підприємства за рахунок збільшення обсягів реалізації товарів можливе за допомогою:

- здійснення ефективної маркетингової політики в галузі збуту товарів;

- диверсифікації асортименту шляхом внесення до переліку взаємодоповнюючих та взаємозамінних товарів;
- регіональної диверсифікації діяльності (розширення регіону збуту);
- надання споживчого кредиту при реалізації товарів тривалого користування;
- розширення системи додаткових торгових послуг, пов'язаних із реалізацією товарів;
- вироблення високорентабельної продукції та зняття з виробництва низькорентабельної.

Необхідними умовами для ефективного управління прибутковістю є:

1) розробка стратегії діяльності підприємства та стратегічного управління в довгостроковому періоді;

2) прийняття рішень з урахуванням стратегії діяльності підприємства;

3) наявність сформульованих конкретних цілей діяльності підприємства;

4) аналіз та оцінка умов, за яких здійснюється діяльність підприємства, а також чинників, які впливають на остаточні результати діяльності;

5) формування ефективної політики з урахуванням правильної оцінки поточної та майбутньої ситуації з точки зору прояву критичних чинників, які її лімітують. Під час розроблення стратегії управління прибутком необхідно враховувати період його життєвого циклу, поточні та перспективні ключові фактори успіху.

Для підвищення рівня прибутковості підприємства можуть упроваджувати заходи в такому порядку:

– організаційні (вдосконалення виробничої структури й організаційної структури управління, диверсифікація виробництва, реструктуризація виробництва тощо);

– техніко-технологічні (оновлення техніко-технологічної бази, переозброєння виробництва, вдосконалення виробів, що виробляються);

– економічні важелі та стимули (вдосконалення тарифної системи, форми і системи оплати праці, прискорення оборотності оборотних коштів тощо).

Список літератури

1. Антонюк О.О. Оцінка рівня прибутковості як важлива складова діагностики кризових явищ підприємства //Вісник «ХНУ». Економічні науки. – 2013. – № 5. – Т. 2. – С. 20–24.
2. Гуторов О. І. Економічні засади формування прибутковості виробництва молока в аграрних підприємствах : теоретико-прикладний аспект : моногр. / О. І. Гуторов, Л. Ю. Кучер, А. В. Кучер. – Х. : Точка, 2013. – 490 с.
3. Коваль О.А. Рентабельність як показник економічної ефективності діяльності сільськогосподарських підприємств / О.А. Коваль // Економіка. Управління. Інновації. – 2014. – № 1. – С. 225–227.

УДК 338.439

Т. Підлубний, магістр гр. ЕО-18М
Л. Коломієць, доц.
Центральноукраїнський національний технічний університет

НЕОБХІДНІСТЬ РОЗВИТКУ ОРГАНІЧНОГО АГРОВИРОБНИЦТВА В УКРАЇНІ

Проаналізовано питання необхідності розвитку органічного агровиробництва, яке дозволяє отримувати якісну продукцію та зберегти природні властивості грунтів
грунти, органічна система, біодинамічне землеробство, добрива, сидерати, врожайність

В умовах погіршення природних властивостей грунтів культурні рослини стають більш вразливими до несприятливих умов довкілля, хвороб та шкідників. Запобігти посиленню цього явища може органічна система землеробства, яка дотримується принципу виключення або мінімізація використання хімічних засобів у рослинництві, органічне удобрення, використання природних процесів.

Актуальність. Актуальним на сьогодні є якомога ширше впровадження елементів органічного землеробства, найбільш доступних сільгоспвиробникам, в першу чергу використання добрив біогенного походження. Одним з найвигідніших місцевих добрив є сидерати, які виправдали себе в багатьох господарствах України та за кордоном. Але необхідне подальше вивчення особливостей їх застосування в кожних окремих грунтово-кліматичних умовах.

Мета дослідження. Визначити вплив «зелених добрив» як одного з найважливіших елементів біодинамічного землеробства на властивості грунту та врожайність культурних рослин.

Завдання: - вивчити стан грунтів в умовах сучасного виснажливого природокористування

- проаналізувати принципи органічного землеробства та його розвиток
- визначити можливі зміни властивостей грунтів за використання біодинамічних принципів догляду
- провести визначення врожайності цукрового буряка за традиційного та органічного удобрення

Об'єкт дослідження: стан грунтів в умовах інтенсивного сільського господарювання та їх родючість.

Предмет дослідження: вплив на врожайність с/г культур біодинамічної технології удобрення.

Результати досліджень.

Природно-ресурсною базою розвитку сільського господарства залишається грунт – найбільш цінне і незамінне багатство країни. В Україні налічується багато різновидів ґрунтів, які відрізняються між собою мінералогічним складом, вмістом гумусу та поживних елементів, фізичними та хімічними властивостями, а отже, і родючістю, придатністю до лісо- та сільськогосподарського використання.

Серед усіх типів ґрунтів України найбільш поширеними є чорноземи. Вони найбільш родючі, з високим вмістом гумусу. Моноліт чорнозему з Воронезької області, як еталон найбільш родючого ґрунту у світі, розміщено поряд з еталонами метра та інших мір в міжнародному інституті метрології в Парижі. В.В. Докучаєв в праці «Русский чернозем»

писав, що російський чорнозем - це цар ґрунтів, він дорожчий за вугілля, дорожчий за золото.

В Україні розорано біля 58 % території - більше, ніж у будь-якій іншій країні Європи. У США, наприклад, цей показник також менший - втричі.

На угіддях фермерських господарств та агрохолдингів переважно вирощуються зернові, кормові та технічні культури. Але їх надто мало для вирішення продовольчої проблеми країни. Не вистачає кормів, насамперед, кормового зерна (кукурудзи, вівса, бобових, коренеплодів) для тваринництва. І причина цього - не низька віддача землі, яка все ж має значний потенціал родючості, а неправильне і недбале господарювання людей на ній, що призводить до виснаження ґрунтів, тобто втрати родючості [1-3].

Найбільшим багатством ґрунту є його гумус – органічна складова. Його роль в біосфері величезна. В українських чорноземах вміст гумусу становить сьогодні 4-6 % , а ще в кінці XIX ст. його вміст становив 8-12 і навіть 16 %. Щорічно ґрунти України втрачають за рахунок мінералізації 14 млн.т гумусу, за рахунок ерозії - 19 млн т.

У природних умовах для того, аби утворити шар гумусу завтовшки 1 сантиметр, потрібно не менше 250-400 років. Зменшення вмісту цієї речовини на 1% зменшує врожайність зернових на кілька центнерів.

За визначенням академіка В.І. Вернадського, - грунт є основою організації біосфери. Географи називають ґрунт дзеркалом, фокусом ландшафту. У ґрунті поєднуються всі компоненти біосфери, формуючи складну полігенетичну систему. Без ґрунту неможливе життя рослин і тварин на суші, бо він є основою цього життя. Вирішальне значення у формуванні ґрунту відіграє жива речовина. Ґрунтотворення почалося з появою життя на Землі. Будь-яка гірська порода, як би вона глибоко не була розкладена та вивітрена, ще не ґрунт. Тільки тривала взаємодія материнських порід з живою речовиною за певних кліматичних умов створює специфічні якості, котрі відрізняють ґрунт від гірських порід. Ґрунт є акумулятором тепла і опадів. Найбільш родючим є ґрунт, здатний утримувати найбільшу кількість води [4,5].

Шкідливий антропогенний вплив, а ще розгул стихій, природних та посилених людиною, завдають ґрунтам величезної, інколи непоправної шкоди. Це, насамперед, водна і вітрова ерозія, погіршення ґрунтової структури, механічне руйнування та ущільнення ґрунту, постійне збіднення на гумус та поживні речовини, забруднення ґрунту мінеральними добривами, отрутохімікатами, мастилами та пальним, перезволоження та засоленість земель.

Деякі види антропогенних впливів на ґрунти, котрі зумовлюють зміну їхньої родючості, наводяться в табл.1.

Таблиця 1. - Наслідки антропогенних впливів на грунти

Вид впливу	Основні зміни грунтів
Щорічне розорювання	Посилена взаємодія з атмосферою, вітрова та водна ерозія, зміна чисельності ґрунтових організмів
Сінокоси, збирання врожаю	Вилучення деяких хімічних елементів, підвищення випаровування
Випас худоби	Ущільнення грунту, знищення рослинності, котра скріплює грунт, ерозія, збіднення грунтів рядом хімічних елементів, висушування, удобрення гноєм, біологічне забруднення
Випалювання старої трави	Знищення грунтових організмів в поверхневих шарах, підсилення випаровування
Зрошення	При неправильному поливанні відбувається заболочення та засолювання грунтів
Застосування отрутохімікатів та гербіцидів	Зниження вологості, виникнення вітрової ерозії Загибель ряду ґрунтових організмів, зміни ґрунтових процесів, накопичення небезпечних для живих організмів отрут

Створення промислових та побутових звалищ	Зниження площі землі, придатної для сільського господарства, отруєння ґрунтових організмів на прилеглих ділянках
Робота наземного транспорту	Ущільнення грунту при русі поза дорогами, отруєння Грунтів відпрацьованими газами та сипкими матеріалами
Стічні води	Зволоження грунтів, отруєння ґрунтових організмів, забруднення органічними та хімічними речовинами, зміна складу грунтів
Викиди в атмосферу	Забруднення грунтів хімічними речовинами, зміна їхньої кислотності та складу
Знищення лісів	Посилення вітрової та водної ерозії, посилення випаровування
Вивезення органічних відходів виробництва та фекалій на поля	Забруднення грунтів небезпечними організмами, зміна їхнього складу
Шум та вібрація	Сповільнення росту рослин, загибель живих організмів
Енергетичні винромінювання	Сповільнення росту рослин, забруднення грунтів

Втрата ґрунтами грудкуватої структури у верхньому горизонті відбувається внаслідок постійного зменшення вмісту органічних речовин, механічного руйнування структури різноманітними знаряддями обробітку, а також під впливом опадів, вітру, перепаду температур тощо.

За рахунок ведення інтенсивного вирощування сільськогосподарських культур та недотримання сівозміни спостерігається активне винесення з грунту поживних речовин і як наслідок погіршення його агроекологічних властивостей (табл. 2), зокрема родючості.

Таблиця 2 - Винесення з грунту елементів живлення урожаєм основних сільськогосподарських культур, кг/т продукції

Культура	Продукція								
	Основна			Побічна			Основна з урахуванням побічної		
	N	P_2O_5	K_2O	N	P_2O_5	K_2O	N	P_2O_5	K_2O
Озима пшениця	20,7	7,4	4,9	5,1	1,6	9,9	28,9	10,0	20,7
Озиме жито	17,4	7,5	5,4	5,6	2,2	11,0	27,8	11,7	26,4
Ячмінь:									
озимий	17,0	8,3	4,9	6,0	2,0	13,6	24,7	10,9	22,6
Ярий	18,4	7,6	5,3	6,6	2,3	13,9	26,2	10,4	22,0
Овес	18,9	8,3	5,1	5,2	2,8	17,9	27,2	12,7	33,7
Кукурудза:									
на зерно	15,3	5,9	4,2	6,9	2,1	14,2	24,1	8,6	22,4
на силос	3,15	1,14	4,23	-	-	-	-	-	-
Просо	19,4	4,9	4,1	9,1	2,0	25,9	33,9	8,1	45,5
Гречка	17,7	5,9	7,1	9,7	4,1	16,4	36,1	13,7	38,3
Горох	33,4	8,4	13,0	10,0	2,3	13,6	44,4	12,5	28,0

Соняшник	23,7	10,4	8,4	8,7	3,1	43,6	42,8	17,2	104,3
Льон	5,4	2,01	10,1	38,9	15,0	11,6	61,6	19,9	63,3
Картопля	3,7	1,1	5,5	3,7	0,9	4,6	5,6	1,6	7,8
Трави (сіно)									
однорічні	20,0	6,0	20,7	-	-	-	-	-	-
багаторічні	23,3	5,3	20,1	-	-	-	-	-	-

Основний критерій родючості – врожай культур. Родючість ґрунту характеризується вмістом органічних і поживних речовин, товщиною гумусового горизонту, будовою, водно-повітряним режимом, вбирним комплексом, структурою та реакцією ґрунту [3,6].

До біологічних показників родючості ґрунту належить:

− вміст органічної речовини;

− мікрофлора;

− чистота від насіння та вегетативних органів бур'янів, шкідників, збудників хвороб сільськогосподарських культур.

Найбільше рослинних решток у ґрунті залишають: багаторічні трави, однорічні сумішки на зелений корм, кукурудза, озимі зернові, ярі зернові, коренеплоди, картопля, льон. Для підтримання бездефіцитного балансу гумусу в ґрунті необхідно вносити перегною: на Поліссі 13-14 т/га; в Лісостепу 11-13 т/га; у Степу 8-9 т/га; при зрошенні 11-13 т/га. Вважається, що з 1 т перегною в процесі гуміфікації утворюється 40 кг гумусу [4,5].

Мікроорганізми беруть участь в процесах нітрифікації, розкладенні клітковини, амоніфікації, диханні ґрунту тощо.

Для збереження властивостей грунтів необхідно використання добрив біогенного походження, що є одним з основних принципів біодинамічного землеробства, яке забезпечує розвиток органічного агровиробництва. В усьому світі даний напрямок впроваджується вже тривалий час. Використання природних процесів забезпечує відновлення грунтів та достатній рівень врожаю сільгоспкультур. Адже мінеральні добрива дають врожай, але не можуть підтримувати потенціал родючості. Як і природніх екосистемах, у агрофітоценозах має відбуватися повернення органіки.

Інтенсифікація біологічних процесів в посівах та насадженнях культурних рослин відбувається із залучення у них мікроорганізмів, грунтової флори і фауни, природного потенціалу рослин, тварин і ландшафтів [11].

Зважаючи на природну потенційну родючість українських грунтів, впровадження принципів органічного агровиробництва є можливим і необхідним. Адже вирощена якісна продукція має значний попит на споживчому ринку і високо ціниться. З усіх країн Європи у нас найбільша площа угідь, придатних для вирощування культур – біля 41 млн.га. Прийнятий в 2014 р. Закон «Про виробництво та обіг органічної продукції» закладає правову основу для розвитку галузі. Починаючи з 2003 року, обсяг площ органічного виробництва зростає, і до 2016 р. вже становив більше 380 тис. га [7-10].

Оскільки у виробників не завжди є можливість придбати готові органічні добрива високої якості, то їх можна вдало замінити на сидерати - так звані «зелені добрива».

У землеробстві сидерати застосовуються вже багато століть, ще з початку нової ери. З тих пір, як з'явилися мінеральні добрива, сидерати втратили свою величезну популярність серед садівників і сільських жителів, але в останні роки відроджуються традиції вносити в ґрунт деякі види зелених добрив як в приватних домоволодіннях, так і в крупних фермерських господарствах.

Найбільш ефективне внесення сидеральних добрив, за результатами досліджень українських вчених, спостерігається при вирощуванні картоплі, кормових і цукрових буряків, кукурудзи, озимих зернових, овочевих і плодово-ягідних культур.

Завдяки сильно розвинутій кореневій системі сидерати підвищують родючість не тільки верхнього орного шару, а й більш глибоких підорних горизонтів ґрунту і підґрунту: покращується азотний режим, збільшується вміст доступних для рослин фосфору і калію, мікроелементи; відбуваються позитивні зміни фізико-хімічного стану ґрунту, збільшується кількість шпаринок, в яких є повітря, поліпшуються умови мікрофлори, - в той час як удобрювальна дія гною обмежується верхнім орним шаром ґрунту [7,8].

В наших дослідженнях було використано в якості сидеральних культур гірчицю білу, редьку олійну, та люпин вузьколистий. Крім привносу поживних речовин у грунт ці рослини діють ще й таким чином, що шкідникам стає «некомфортно» і вони залишають удобрені ділянки, - внаслідок виділення в грунт після розкладання біомаси зелених добрив специфічних біологічно активних речовин. Сидерати на час заорювання в грунт формували врожайність зеленої маси 239-280 ц/га зеленої маси, в залежності від виду (табл.3).

Таблиця 3 - Показники урожайності зеленої маси сидеральних культур, 2017-2018рр.

Сидеральна культура	Урожайність, ц/га		
	2017р.	2018р.	Середнє за 2017-2018 рр.
Люпин вузьколистий	283	277	280
Гречка	277	281	279
гірчиця біла	234	244	239
Редька олійна	329	331	330

Для наших досліджень біодинаміки врожаю висівали сидерати у 2017-2018 рр., а культурою-послідовником кожного наступного року був цукровий буряк. Щороку дослідження проводилися на різних полях, оскільки згідно принципу сівозміни така культура як цукровий буряк категорично не може висіватися повторно, оскільки забирає вологу з деяких глибоких шарів грунту, тому на наступний рік необхідного рівня врожайності досягнуто бути не може.

Найбільший урожай коренеплодів був зібраний по варіанту, який підживлювався заорюванням зеленої гречки - 37,0 т/га, що означає приріст до контролю – 9,4 т/га (табл.4).

Таблиця 4 - Врожайність цукрових буряків, в залежності від виду підживлення, 2018-2019 рр.

Варіанти	Збір коренеплодів, т/га			Приріст, т/га	
	2018 р.	2019 р.	середнє за 2018-2019 рр.	до контролю	до мінерального підживлення
Контроль - без підживлення(чорний пар)	27,8	28,2	28,0	-	-
Внесення мінерального підживлення	36,0	36,6	36,3	8,3	-
Посів на сидерат люпину вузьколистого	36,3	38,3	37,8	9,8	1,5
Посів на сидерат гречки	37,0	37,8	37,4	9,4	1,1
Посів на сидерат гірчиці білої	34,8	35,8	35,3	7,3	-1,0
Сівба на сидерат	35,6	37,0	36,8	8,8	0,5

редьки олійної					

Порівняно з контрольним варіантом – чорним паром без будь-якого удобрення, по всіх сидератах було збільшення врожайності цукрового буряку – від 0,5 до 1,5 ц/га. Порівняно з мінеральним удобренням лише варіант з гірчицею білою знизив врожай на 1 ц/га.

Отже, якщо навіть за одноразового використання сидерації умови росту і розвитку культури покращуються, то логічно передбачити значне поліпшення умов вирощування за систематичного застосування «зеленого» добрива. систематичне впровадження хоча б окремих елементів біодинамічного землеробства поліпшує грунтові умови, потенціює родючість, запобігає розвитку хвороб та шкідників.

Висновок. Зважаючи на необхідність впровадження систем землеробства, які є невиснажливими для грунтів та можуть стабільно забезпечувати населення рослинницькою продукцією високої якості, необхідно якомога більше вивчати та впроваджувати таких прийомів господарювання, як біодинамічне землеробство. Головний принцип – заміна хімічних засобів боротьби за врожай такими, що мають біогенне походження. Це дозволяє повернути грунтам родючість, а культурним рослинам надати природної стійкості до несприятливих факторів довкілля, що забезпечує повноцінний ріст і розвиток рослин та реалізацію їх генетичного потенціалу.

Вивчення умов росту і розвитку цукрового буряка за сидерального удобрення, рекомендованого біодинамічною системою землеробства, забезпечило прибавку врожаю. Та в першу чергу це доводить екологічну доцільність органічного агровиробництва.

Список літератури

1. Стан родючості ґрунтів України та прогноз його змін за умов сучасного землеробства / За ред.. В.В. Медведева і М.В. Лісового. – Харків, 2001. – 98с.
2. Грабак Н.Х. Основи ведення сільського господарства та охорона земель: навч.посіб./ Н.Х. Грабак, І.Н. Топіха, В.М. Давиденко, І.В. Шевель; М-во освіти і науки України. – [2-ге вид.]. - К.: Професіонал, 2006. – 396с.
3. Мазур Г.А. Гумус і родючість ґрунтів / Г.А. Мазур // Агрохімія і ґрунтознавство. - Київ-Харків, 2002. – 396с.
4. Пістун М.Д. Географія агропромислових комплексів: Навч. посіб. для студентів/ М.Д. Пістун, В.О. Гуцал, Н.І. Проватор. – К.: Лебідь, 1997. – 198с.
5. Ґудзь В.П., Примак І.Д., Будьонний Ю.В., Танчик С.П. Землеробство: Підручник. 2-ге вид. перероб. та доп./За ред. В.П. Гудзя.-К.:Центр учбової літератури, 2010.-464с.
6. Панас Р.М. Раціональне використання та охорона земель: Навч. посібник. - Львів:Новий світ.-2000,2008.-352с.
7. Бородачова Н.В. Органічне виробництво: як прискорити доступ споживачів до органічних продуктів в Україні /Н.В.Бородачова// Наук.вісн.НАУ. – 2005. - № 81. – С. 293-301.
8. Зінчук Т.О. Витоки та підходи до формування категоріального апарату «органічне виробництво»: європейський і світовий досвід/ Т.О.Зінчук//Органічне виробництво і продовольча безпека. – Житомир: Полісся, 2013. – 492 с.
9. Прадун В.П. Формування екологічно збалансованого аграрного виробництва: теоретико-методологічні та прикладні аспекти/ В.П. Прадун// Агроінком. – 2004. - №5-6. – С.59-64.
10. http://www.agroecology.in.ua/organicmovement
11. Біодинамічне землеробство як метод збільшення врожайності [Електронний ресурс] http://agro-yug.com.ua/archives/22395

УДК 658.567.1

Х. Поніч, магістр гр. ЕО-18М
Л. Коломієць, доц.
Центральноукраїнський національний технічний університет

ОБСЯГ ВІДСОРТОВАНИХ РЕСУРСНО-ЦІННИХ СИРОВИННИХ КОМПОНЕНТІВ, ЩО ВХОДЯТЬ ДО СКЛАДУ ТВЕРДИХ ПОБУТОВИХ ВІДХОДІВ

У статті розглядається технологія сортування селективно зібраних відходів; оптимальна схема управління ТПВ; розрахунок обсягів відсортованих ресурсно-цінних сировинних компонентів, що входять до складу відходів.
ресурсно-цінні сировинні компоненти, сортування, тверді побутові відходи, вторинна сировина.

Актуальність теми. У ТПВ попадає багато цінних компонентів, потенційно придатних для вторинного використання таких як папір, картон, харчові відходи, дерево, метал чорний, метал кольоровий, текстиль, кістки, скло, шкіра, гума, взуття, каміння, фаянс, пластмаса.

Актуальними є розробки заходів з раціонального залучання відходів в господарський оберт на основі їх селективного по компонентного збору в місцях утворення, не допускаючи попадання цінних компонентів у загальну масу ТПВ. У цьому випадку в переробку може використовуватися незабруднена вторинна сировина. Роздільно зібрані в контейнери відходи практично не містять домішки інших компонентів.

Аналіз останніх досліджень і публікацій. Усі види відходів виробництва та споживання по можливості використання можна поділити на вторинні матеріальні ресурси, які вже використовуються або переробка яких планується, та потенційні ресурси, які на даному етапі економічного розвитку переробляти недоцільно на думку Балацького О.Ф.

У західних країнах, де проблема одержання з ТПВ вторинної сировини багато в чому вирішується за рахунок масштабної організації роздільного по компонентного збору відходів у місцях їхнього утворення, доведення селективно зібраних відходів здійснюються на спеціальних сортувальних комплексах, в основному, методами ручного сортування. При цьому проводиться як пряме сортування (добування цінних компонентів), так і зворотне (видалення забруднюючих компонентів, у тому числі небезпечних). В якості компонентів практикується виділення макулатури (у тому числі за сортами), пластмаси, скла та металів (метали часто вилучають в автоматичному режимі за допомогою магнітної та аеродинамічної сепарації).

Реймерс Н.Ф. під вторинними матеріальними ресурсами розуміє – відходи виробництва та вжитку, які виникають у народному господарстві та можуть бути повторно використані у ньому [1].

Згідно словника, ресурси вторинні матеріальні – це відходи виробництва та споживання (включаючи побутові відходи), які використовуються у народному господарстві на даному етапі розвитку науки і техніки [2].

З останнього визначення витікає, що рівень використання відходів визначається науково-технічним рівнем суспільного розвитку. Однак, зазначені вище та інші тлумачення поняття вторинного матеріального ресурсу (Данилова та Данильяна В.И. [3], Мусієнко М.М. [4]) не враховують його якісних характеристик та ціни, що, по суті, визначає конкурентоздатність вторинного ресурсу у порівнянні з первинним.

Всі вторинні ресурси можна класифікувати за наступними ознаками:

- за сферою виникнення: промислові, сільськогосподарські, комунальні;

- за стадіям життєвого циклу продукту: виробництва, споживання та утилізації;
- за стадіям життєвого циклу первинного ресурсу: видобутку, збагачення, переробки;
- за можливостями використання у виробництві: реальні, потенційні ;
- за морфологічним складом: промислові (доменний та сталеплавильний шлак), побутові (скло, папір, металобрухт, полімери та ін.);
- за кратністю використання: однократного та багатократного використання (капрон повторно переробляється до 10 разів, поліформальдегід і його полімери - до 7 разів);
- за належністю до регіону: вторинні ресурси, що використовуються у регіоні
- за місцем виникнення та ті, що використовуються в інших регіонах;
- за напрямком використання: зі зміною та без зміни першочергового спрямування використання (без зміни: скляна тара; зі зміною: використання склобою для виробництва облицювальної плитки).

Як вже відмічалося вище, відходи становлять небезпеку для навколишнього середовища, а також містять ресурсно-цінні компоненти (РЦК), що обумовлює необхідність управління ними.

Управління – це діяльність, пов'язана з впливом керуючого суб'єкта на керований об'єкт з метою досягнення певних результатів [5].

Більш повне визначення надає Скібіцька Л.І., розуміючи під «управлінням» - складний процес, який включає цілеспрямований вплив на об'єкти, системи з метою збереження їхньої сталості або переведення з одного стану в інший з метою досягнення певних цілей [6].

Постановка завдання. Завданням дослідження є аналіз зарубіжного досвіду у сортування відходів, аналіз технологічної схеми сортування твердих побутових відходів, розрахунках обсягів відсортованих ресурсно-цінних сировинних компонентів, що входять до складу ТПВ в м. Кропивницький.

Виклад основного матеріалу. Технологія сортування селективно зібраних відходів у більшості випадків ідентична і являє собою ручну вибірку тих або інших компонентів зі стрічки тихохідного конвеєра (ширина стрічки – не більше 1200 мм, швидкість – не більше 0,5 м/с, переважно 0,1-0,2 м/с) у сполученні з механізованим сортуванням металів. У ряді випадків ручному сортуванню передує операція просівання вихідного матеріалу з метою видалення дрібної фракції та розпушування маси відходів; при необхідності, у технологічну схему можливе включення операції дроблення (розкриття упакування). Устаткування механізованого сортування встановлюється на подіумі в спеціальному приміщенні-кабіні, обладнаному припливно-витяжною вентиляцією та знезаражуючим пристроєм сепарованих відходів.

Технологічна схема сортування твердих побутових відходів, основні операції якої відпрацьовані на потоці ТПВ при продуктивності 15 т/год., представлена на рисунку 1.1.

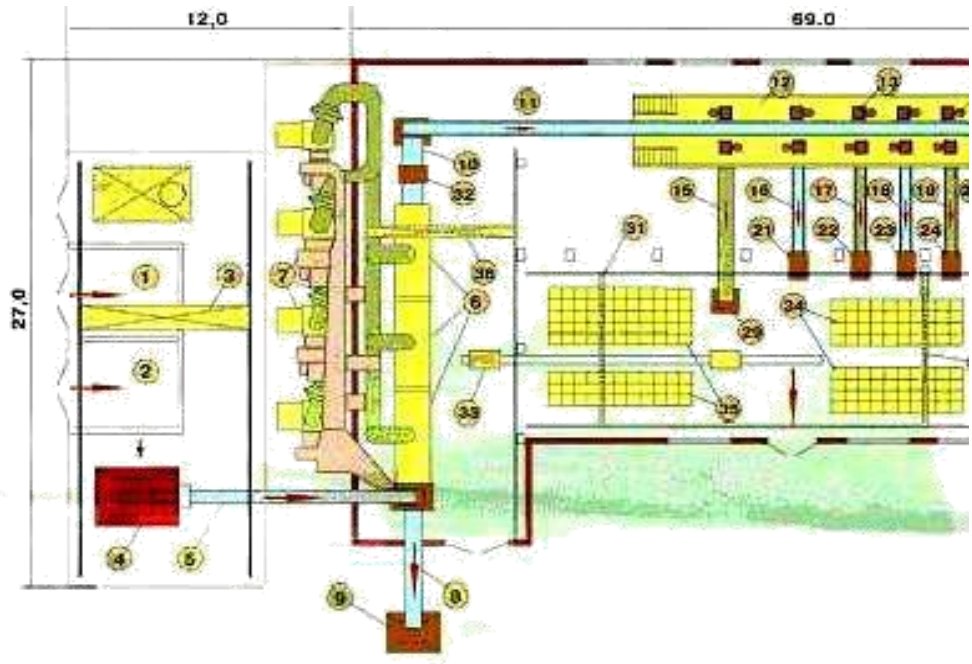


Рисунок 1.1 – Технологічна схема сортування твердих побутових відходів з використанням сортувальної лінії

Джерело: (методичні вказівки, з дисципліни «управління та поводження з відходами» Харків: ХНАМГ, 2010).

1.	Засік прийому ТПВ валового збору	21,22,23,24. Комплекси для пак	
2.	Засік прийому	текстилю	
3.	Кран мостовий грейферний в/п 3,2 т	28.	Пресс для металобрухту
4.	Прийомний бункер з пластинчастим живильником	29.	Контейнер збору в/с
5,8,10,11,15,16,17,18,19,20,25,27. Стрічковий конвеєр		30.	Бункер збору відходів
6.	Сушильно-знезаражуюча камера	31 Підвісний електричний кран	
7.	Повітряно-циркуляційна система	32	Установка для знезаражування
9.	Бункер прийому відходів, які не переробляють	33.	Вагонетка
12. Технологічна площадка з металоконструкцій		34,35.	Площадки тимчасового збору
13. Ринва для подачі вторинної сировини на конвеєр		36. Кран-балка в/п 3 т	
14. Робоче місце сортувальника			
26. Електромагнітний відділювач		.	

Сміттєвози, що доставляють відходи на сортування, проходять радіометричний контроль, зважуються та розвантажуються на рівну бетонну площадку (мінімальні розміри 30х30 м). За допомогою фронтальних завантажувачів відходи подаються у хвостову частину заглибленого стрічкового конвеєра або пластинчастого живильника легкого типу (оптимальний варіант – використання горизонтально-похилого живильника, до пластин якого кріпиться гумова стрічка, що запобігає просип матеріалу). Верхня вітка живильника-конвеєра, що подає матеріал на сортувальний конвеєр, заглиблена на 0,4 м. Продуктивність однієї лінії сортування, залежно від складу збагачуваної сировини, коливається від 3 до 10 т/година. Відібрані в якості вторинної сировини компоненти скидаються в люки та попадають або у контейнери, які стоять на нижній відмітці, або в накопичувальні ємності (бункера), розташовані на нижній відмітці (під сортувальною кабіною). Дном цих ємностей може служити горизонтальна конвеєрна стрічка, що полегшує подачу на пакетування макулатури, пластмаси й текстилю (автоматична подача матеріалів на горизонтально-похилий конвеєр, що живить пакетувальний прес).

Найбільш повний і селективний поділ твердих побутових відходів на компоненти досягається при моно шаровій подачі їх до сортувальних апаратів та пристроїв, коли окремі компоненти не перекривають один одного й перебувають у роз'єднаному стані. Моно шаровою подачею відходів у процес сепарації забезпечують їхній поділ на легку й важку фракції та східчасте збільшення швидкості потоку ТПВ перед кожною наступною операцією збагачення по ходу технологічного процесу (від 0,2 до 1,5 м/с).

Таким чином, на стадії збору та видалення накопичених побутових відходів багато в чому визначається ефективність і безпека їхньої подальшої переробки та захоронення при поетапній реалізації системи управління комплексної переробки ТПВ.

Зарубіжний досвід показує: сортуванню на спеціальних об'єктах повинні піддаватися відходи нежилого сектора міста (торгівельні та комерційні підприємства, адміністративні установи, навчальні заклади й т.п.), що характеризуються підвищеним вмістом незабрудненої макулатури, металів, полімерних відходів і низьким вмістом харчових та рослинних залишків. Отже, для України оптимальний склад ТПВ, що залучають у масштабну переробку для одержання цінних продуктів, повинен підбиратися за рахунок централізованої організації в регіонах не змішуваних потоків муніципальних відходів, частина яких, збагачена цінними компонентами, направляється на комплекси по сортуванню та переробці твердих побутових відходів.

При розрахунках обсягів відсортованих ресурсно-цінних сировинних компонентів, що входять до складу ТПВ, виходять з обсягів розміщення відходів по нормах накопичення, адміністративного району міста та планованого добування відходів (фізико-хімічні втрати).

Загальна кількість накопичення відходів за рік ($V_{заг.}$) визначається за формулою:

$$V_{заг} = k \times N, тис.м^3 \quad (1.1)$$

де k – коефіцієнт норми накопичення, приймається рівним 1,4;

N – чисельність жителів районів міста.

Загальна кількість відходів від житлового сектора визначається за формулою:

$$V_{ж.с} = \frac{V_{заг} \times W}{100\%}, м^3/рік \quad (1.2)$$

де *W* – обсяг ТПВ загального обсягу накопичення (для житлового сектора = 60 %, для нежилого – 40 %).

Для визначення кількості відходів, накопичених від житлового та не житлового сектору ($V_{S\,1,2}$, ,$V_{M\,1,2}$), використовуємо формули (2.3,2.4)

$$VS_{1,2} = \frac{V_{ж.с} \times S_{1,2}}{100\%}, м^3/рік \quad (1.3)$$

$$V_{M_{1,2}} = \frac{V_{ж.с} \times M_{1,2}}{100\%}, м^3/рік \quad (1.4)$$

де S , M – зміст обсягів ресурсних відходів до загального обсягу ТПВ, % ;

1,2 – компоненти, що входять до складу ТПВ.

При цьому варто враховувати фактичний відбір відходів (фізико-хімічні втрати), плановані добування відходів із загальної маси ТПВ, виходячи з яких у формули (1.3, 1.4) вводяться фактичні виправлення:

$$V_{факт_{S_{1,2}(M_{1,2})}} = \frac{V_{S_{1,2}(M_{1,2})} \times F}{100\%}, м^3/рік \quad (1.5)$$

де F – фактичний відбір відходів, %.

З розрахунку відібраних обсягів і тарифів закупівельних цін, визначеного Постановою КМ України № 1084 від 26.06.02 визначений додатковий резерв природно-ресурсного потенціалу міста в обсязі:

$$V_{заг_{1,2}} = V_{S_{1,2}} + V_{M_{1,2}}, \ м^3/рік \quad (1.6)$$

Перехід від (м3) до (т) здійснюється за допомогою коефіцієнта ущільнення:

$$G = V_{заг_{1,2}} + k_y, \ т/рік \quad (1.7)$$

де k_y – коефіцієнт ущільнення.

У загальній сумі (тис. грн.) від реалізації доход складе:

$$R_{1.2} = G_{1.2} + B_{1,2}, \ грн \quad (1.8)$$

де В – сума від реалізації відсортованих вторинних ресурсних сировинних відходів, грн.

Загальна сума (∑) складе:

$$\sum = R_{1.2} + R_{1.2}\ ,\ \text{грн} \qquad (1.9)$$

Визначити кількість вторинної сировини та суму від їхньої реалізації:

- полімерних відходів, т/рік;
- макулатури (т/рік)

від житлового упорядженого та нежилого (комерційного) сектора м. Кропивницький.

Вихідні дані:

- чисельність населення м. Кропивницький 226,5 тис. чол.;
- норма накопичення n = 1,4 м^3/чол. рік;
- коефіцієнт ущільнення k_y = 0,25 т/м^3;

вміст до загальної маси ТПВ:

а) у житловому секторі (макулатура – 22 %; полімерні відходи – 7,87 %);

б) у нежилому (комерційні відходи) секторі (макулатура – 53 %; полімерні відходи – 8,5 %).

Плановане (фактичне) добування:

- від житлового сектора відбір полімерних відходів 100 %, макулатури –90 %;
- від нежилого сектора відбір полімерних відходів 100 %, макулатури – 95 %.

1. Визначаємо загальну кількість накопичення відходів у Кропивницькому за рік

$$1{,}4 \times 226{,}5\ \text{тис.чол.} = 151{,}34 = 317{,}1\ \text{тис. м3}$$

2. Визначаємо кількість твердих побутових відходів (м3/рік), що накопичилися від житлового сектора (60 %):

$$V_{\text{ж.с}} = \frac{V\text{заг} \times 60}{100} = \frac{317100 \times 60}{100} = 190260\text{м}^3/\text{рік}$$

3. Визначаємо кількість відходів (м3/рік) від нежилого (комерційні відходи) сектора :

$$V_{\text{ком}} = \frac{V\text{заг} \times 40}{100} = \frac{317100 \times 40}{100} = 126840\ \text{м}^3/\text{рік}$$

4. Визначаємо кількість полімерних відходів, накопичених від житлового сектора, з розрахунку 7,87 % до загальної маси ТПВ та фактичного відбору 100 %

$$V\text{полім} = \frac{190260 \times 7{,}87}{100} = 149743{,}5\ \text{м}^3/\text{рік}$$

5. Визначаємо кількість відсортованої макулатури (м3/рік) з розрахунку 22 % до загальної маси ТБО та фактичного відбору 90 % (фізико-хімічні втрати).

$$V\text{макул.} = \frac{190260 \times 22}{100} = 41857{,}2\ \text{м}^3/\text{рік}$$

$$V_{\text{факт.мак.}} = 41857{,}2 \times 0{,}9 = 37671{,}48\ \text{м}^3/\text{рік}$$

6. Визначаємо кількість полімерних відходів, накопичених від нежилого сектора (комерційні відходи), з розрахунку 8,5 % до загальної маси ТПВ та фактичного відбору 100%.

$$V\text{полім} = \frac{126840 \times 8{,}5}{100} = 10781{,}4\ \text{м}^3/\text{рік}$$

7. Визначаємо кількість (т/рік) відсортованої макулатури від нежилого (комерційного) сектора з розрахунку 53 % та фактичного відбору 95 %.

$$V\text{макул.} = \frac{126840 \times 53}{100} = 67225{,}2\ \text{м}^3/\text{рік}$$

$$V_{\text{факт.мак.}} = 32084{,}1 \times 0{,}95 = 63863{,}94\ \text{м}^3/\text{рік}$$

Додатковий резерв природно-ресурсного потенціалу м. Кропивницький в обсязі:

- полімерних відходів від житлового та нежилого секторів району (т/рік)

$$V_{\text{п.заг.}} = V\text{п.ж.} + V\text{п.к.} = 149743{,}5 + 10781{,}4 = 160524{,}9\ \text{м3/рік}$$

$$G_{\text{т/рік}} = 160524{,}9 \times 0{,}25 = 40131{,}23\text{т/рік}$$

- макулатури від житлового та нежилого секторів району

$V_{м.заг.} = Vм.ж. + Vм.к. = 37671,48 + 63863,94 = 101535.42м^3$ /рік

$G_{т/рік} = 101535.42 \times 0,25т/ м^3 = 25383,85т/рік$

У загальній сумі (тис. грн.) доход від реалізації ресурсно-цінних сировинних компонентів складе:

- від реалізації полімерних відходів:

$R_{полім.} = 40131,23 т \times 850 грн. = 34111545,5 грн$

- від реалізації макулатури:

$R_{макул.} = 25383,85 \times 350грн. = 8884347,5 грн$

Усього: Σ = 2,612 млн. грн. + 4,2 млн. грн. = 6,812 (млн. грн./рік).

Відповідь: у загальній сумі доход від реалізації складе: 6,812 (млн. грн./рік).

Висновки. Стан оточуючого середовища – одна з найважливіших характеристик якості життя, науково-технічного та економічного розвитку регіону держави, яку необхідно враховувати при оцінці економічної доцільності впровадження установок для очистки повітря від пилу. Заміна старого очисного обладнання більш високоефективним забезпечує поліпшення екологічної ситуації, сприяє збереженню здоров´я населення.

Список літератури

1. Реймерс Н.Ф. Природопользование: Словарь-справочник / Н.Ф. Реймерс. М.: «Мысль», 1990. – 637 с.
2. Білявський Г.О. Основи загальної екології: Підручник – 2-е видання зі змінами / Г.О. Білявський, М.М. Падун, Р.С. Фурдуй. – К.: Либідь, 1995. – 368 с.
3. Метлова Л.П. Теорія та практика поводження з відходами (на прикладі Донецької області): Монографія / НАН України. Інститут економіки промисловості. – Донецьк, 2004. – 168 с.
4. Шершнев Е.С. Масштабы, структура и проблемы утилизации городских мусорных свалок / Е.С. Шершнев, В.Г. Ларионов, П.Ю. Куркин // Экология и промышленность России. – 1999. – №2. – С. 29-32.
5. Закон України «Про відходи» №187/98-ВР від 5 березня 1998 р. [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua
6. Сытник К.М. Словарь-справочник по экологии / [К.М Сытник, А.В. Брайон, А.В. Гордецкий и др.]. – К.: «Наукова думка», 1994. – 664 с.

УДК 930.25

В. Попов, магістр гр. ІС-18М
Центральноукраїнський національний технічний університет

СТАНОВЛЕННЯ ТА ДІЯЛЬНІСТЬ ДЕРЖАВНОГО АРХІВУ КІРОВОГРАДСЬКОЇ ОБЛАСТІ В 1920-і рр.

У статті розглядається створення та перші роки діяльності Державного архіву Кіровоградської області. Висвітлено історію становлення архівної установи, визначено напрямки її функціонування.
архів, архівні установи, Державний архів Кіровоградської області, архівний фонд

Актуальність теми. Архівні установи України є невід'ємною частиною національної історичної спадщини. Їхня діяльність сприяє збереженню національної пам'яті, поширенню національної свідомості та самоідентифікації української нації. Архіви є унікальними хранителями «пам'яті людства», центрами зосередження різноманітних документальних пам'яток історії, науки та культури. Досвід минулих поколінь важливий не тільки для історичної пам'яті, а й для розв'язання сучасних практичних питань повсякдення. Наявність архівних матеріалів сприяє розвитку чималої групи наукових дисциплін, предметом вивчення яких є суспільство – як системи загалом, так і окремих його частин, функцій та

елементів, а також людини – соціальної особи, особистості, як суб'єкта і об'єкта суспільних зв'язків та відносин.

Чільне місце серед архівних установ України займає Державний архів Кіровоградської області (далі – ДАКО), що є центром системи архівної справи регіону.

Аналіз останніх досліджень і публікацій.

Проблема становлення та діяльності Державного архіву Кіровоградської області не знайшла широкого висвітлення. Наукових розвідок, присвячених цій темі загалом небагато. Однак, тією чи іншою мірою її торкалися автори статей та розділів путівників, присвячених історії архівної системи України. Серед них І.Матяш [2], К. Климова [10] С. Абросимова, В. Бездрабко, В. Болдирєв [1]

Безпосередньо до питання історії архівної справи на Кіровоградщині зверталися Є. Горбунова [9], О. Трибуцька (колишній начальник відділу інформації та використання документів Державного архіву Кіровоградської області) [11], С. Шевченко (у 1983-1991 рр. директор ДАКО) [12], О. Бабенко – нинішній директор архіву [3].

Постановка завдання. Проголошення незалежності української держави зумовило широкі можливості розвитку української національної культури, яка була і є важливим чинником державотворення та консолідації української нації. Важливе значення під цим кутом зору має Національний архівний фонд як складник інформаційних ресурсів України щодо консолідації суспільства й державотворчих процесів. Все це викликало зростання інтересу до актуальних проблем розвитку архівної справи в українській науці. Саме через це метою цієї статті є з'ясування ролі та місця Державного архіву Кіровоградської області у сфері громадського та інтелектуального життя міста і області, головних тенденцій розвитку архівної справи, зокрема і в попередні періоди.

Виклад основного матеріалу. 1920-і в історії розвитку архівної справи в Україні були складними і неоднозначними. Після більшовицького державного перевороту постало питання щодо впровадження реформи архівної справи в Україні.

У квітні 1920 р. Рада Народних Комісарів України ухвалила постанову, згідно з якою усі архіви на території УСРР, а також приватні зібрання документів, оголошувалися загальнонародною власністю. Усім установам заборонялося знищувати, продавати, передавати документальні матеріали на власний розсуд. Саме так було покладено початок формування централізованого архівного фонду в УСРР. У вересні 1921 р. було створено Головне управління архівами, що діяло при Народному комісаріаті освіти УСРР. Крім того, у Києві та Харкові були створені центральні історичні архіви. В губернських центрах створювалися губернські архівні управління та губернські історичні архіви. У цьому ж контексті розпочалося налагодження централізованої архівної справи й у м. Єлисаветграді. 5 липня 1920 року наказом Єлисаветградського повітового виконкому була створена комісія, що мала обстежити наявні у місті архіви. До складу комісії увійшли представники поліграфічного відділу Раднаргоспу, робітничо-селянської інспекції та відділу управління повітвиконкому.

Всеукраїнський центральний виконавчий комітет у січні 1923 р. затвердив положення про Центральне архівне управління, на яке покладалося керівництво архівною справою у республіці. З огляду на адміністративну реформу структура архівних органів в України була відповідно скорегована: в 1925 р. було ліквідовано 9 губернських архівних управлінь й натомість утворено 40 окружних.

Президія Зінов'євського (м. Єлисаветград в 1923 р. перейменовано на Зінов'євськ) окружного виконавчого комітету в листопаді 1925 р. створила окружне архівне управління, завідувачем якого призначила Г.М. Павлюченка, який у 1925-26 рр. був єдиним співробітником установи. У користування архівного управління було передано приміщення будинку, що раніше належав купцю Остроухову [4, арк.177].

Саме з цього моменту розпочалася діяльність Зінов'євського окружного архівного управління зі збирання та каталогізації документів. Слід відзначити, що сам принцип радянської реформи архівної справи за своїми головними чинниками фактично збігався з

тим, що планував започаткувати у цій сфері уряд гетьмана Скоропадського. Пояснювалося це, напевне тим, що обидві політичні сили були прибічниками жорсткої централізованої державної структури, а також тим, що участь у формуванні загальних принципів реформи брали, швидше за все, одні й ті самі спеціалісти, зокрема академік Д.І. Багалій.

Отже, у 1925 р. завершився перший період у становленні архівної справи в нашій області. Попередні спроби створити архів та упорядкувати документи не мали успіху через громадянську війну та економічну кризу. Внаслідок цього було втрачено чимало цінних документів з історії міста та повіту, серед них зокрема архіви жандармського управління, поліцейських частин міста, повітового суду, земських суддів.

З огляду на це, архівне управління розпочало створювати документальну базу фактично на порожньому місці. Впродовж кількох років були укомплектовані фонди повітової земської управи, поштово-телеграфної контори, заводу швейних машин, комерційного та реального училищ, а також особовий фонд міського землеміра, історика, археолога і громадського діяча П.З. Рябкова [6, арк.15].

Окружний виконком спільно з окружним архівом у листопаді 1927 р. звернулися до громадськості, насамперед до вчителів, з проханням відшукувати та зберігати історичні документи. В тому ж році в архіві почали систематично видавати документи користувачам у читальному залі [5, арк. 67-68].

Постановою Раднаркому УСРР у 1928 р. Зінов'ївське окружне архівне управління було віднесено до другої категорії архівних управлінь. Відповідно перед ним були визначені певні завдання:

- нагляд за архівами на території округу, їхній облік та реєстрація;
- розробка заходів щодо охорони архівних матеріалів у відповідності до чинного законодавства;
- нагляд за веденням архівної справи в архівних частинах державних і громадських установ, організацій та підприємств на території округи;
- концентрація архівних матеріалів, що їх здавали установи, організації, підприємства до архівосховищ окружного архівного управління;
- попередня розробка архівних матеріалів, що надходять до архівосховищ окружного архівного управління і видача довідок установам, організаціям і приватним особам. [7, арк. 24].

Окружне архівне управління в кінці 1930 року було ліквідоване, а замість нього було утворено Зінов'євське місцеве архівне управління. Утримувалося архівне управління за рахунок місцевого бюджету за загальним кошторисом окружного виконкому. У своїй діяльності управління керувалося основними нормативними документами Центрального архівного управління.

Висновки. Отже, період 1920-х рр. в історії розвитку архівної справи в Україні був визначальним. Упродовж цього періоду було здійснено архівну реформу, створено правову базу діяльності архівних установ, проведено її централізацію, створено мережу архівних установ, сформовано державний архівний фонд, завершено концентрацію архівних документів в державних архівах, впроваджено нормативне й методичне забезпечення ключових напрямів роботи архівів.

На території Зінов'ївського округу до кінця 1920-х рр. завершився етап становлення архівної справи. На цьому етапі були визначені головні принципи архівного будівництва, створені місцеві органи архівного управління, розпочато створення централізованої структури архівних установ.

Список літератури

1. Абросимова С., Бездрабко В., Болдирєв В. Нариси історії архівної справи в Україні /ДКА України, Український науково-дослідний інститут Архівної справи та документознавства. К., 2012. 612 с.
2. Архівні установи України: довідник / Держкомархів України. УНДІАСД; Редкол.: Г.В. Боряк, І.Б. Матяш, Г.В. Папакін. 2-е вид., доп. К.: ДЦЗД НАФ, 2005. Т. 1. Державні архіви. 692 с.

3. Бабенко О.О. Скарбниця історичної пам'яті краю. // Між Бугом і Дніпром. Науково-краєзнавчий вісник Центральної України / Випуск IV. Кіровоград: Центрально-Українське видавництво, 2015. С. 7-12.).
4. ДАКО, ф. Р-833, оп. 1, спр. 1.
5. ДАКО, ф. Р-833, оп.1, спр. 11.
6. ДАКО, ф. Р-833, оп.1, спр. 13.
7. ДАКО, ф. Р-833, оп.1, спр. 18.
8. Державний архів Кіровоградської області. Анотований реєстр описів. Том ІІ. Фонди періоду після 1917 р. Книга 1/ Державний архів Кіровоградської області; Упор.: Тетяна Базишена, Олена Жук, Лілія Маринець та ін. Кіровоград, 2010. 655 с.
9. Кіровоградський обласний державний архів: путівник. /упоряд: Є.Й. Горбунова та ін. Кіровоград, 1966. 255 с.
10. Нариси історії архівної справи в Україні: Посібник / За загальною редакцією І.Б. Матяш та К.І. Климової. К., 2002. 612 с.
11. Трибуцька О.А. Державному архіву Кіровоградської області – 85 років // Архіви України № 5. 2010. С. 91-103
12. Шевченко С.І. Центральноукраїнський архів. Кіровоград, 2013. 131 с.

УДК 631.15

Ю. Постолатій, магістр гр. АДМ-18-1,4
Центральноукраїнський національний технічний університет

ТЕОРЕТИЧНІ ЗАСАДИ АНТИКРИЗОВОГО УПРАВЛІННЯ СІЛЬСЬКОГОСПОДАРСЬКИМИ ПІДПРИЄМСТВАМИ

У статті здійснено дослідження теоретичних засад антикризового управління. Доведено, що антикризове управління актуальне та особливо важливо за сучасних темпів науково-технічного та глобального економічного прогресу. Обґрунтовано, що у сучасних умовах невизначеності і високої ймовірності кризових явищ управління сільськогосподарськими суб'єктами господарювання потребує конструктивного менеджменту, який повинен бути заснованим на стратегічних підходах і попереджувальних заходах.
антикризове управління, кризи, суб'єкти господарювання, сільськогосподарські підприємства, теорія циклів

Кризові явища ускладнюють діяльність суб'єктів господарювання. Результати функціонування підприємств залежать від багатьох чинників як макроекономічного, так і мікроекономічного характеру, вплив яких обумовлює коливання господарських та фінансових показників діяльності і відхилення їх від запланованих. Особливо потерпають від різноманітних кризових явищ сільськогосподарські підприємства. Це пов'язано з тим, що їх діяльність відбувається у тісній залежності від природно-кліматичних факторів, характеризується обмеженістю власного капіталу, значними борговими зобов'язаннями, циклічністю виробництва. Все це актуалізує проблему своєчасного розпізнавання, оцінки та усунення причин кризи, що потребує формування системи антикризового управління.

Науковим підгрунтям для розробки антикризових заходів і формування системи попередження та реагування на кризу підприємств є праці вчених-економістів: М. Дем'яненка [3], Лігоненко Л. О. [6], О. Собкевич [7], Я.Гринчишина [2], І. Брижань [1], Стецюка П.А. [8], Короткова Е.М. [5], Кондратьєва М.Д. [4] та ін.

Кризи об'єктивно характерні для економіки будь-якого рівня і супроводжують життєдіяльність будь-якого підприємства, тому що знаходяться у самій природі існування господарюючих суб'єктів. Тому для суб'єкта господарювання з метою запобігання криз є необхідним здійснювати регулярний моніторинг ознак кризи і на підставі отриманих даних своєчасно реалізувати антикризові стратегії, вживати відповідні організаційно-

управлінські заходи.

Зміст і методологія антикризового управління на підприємстві актуальні та особливо важливі за сучасних темпів науково-технічного та глобального економічного прогресу. Діяльність підприємств є основою економічного розвитку як кожної країни, так і світової економіки, і саме для цього економічного рівня найбільш небезпечні кризові явища, що обумовлює нагальну необхідність спеціального антикризового управління для суб'єктів господарювання. Конкурентоздатність підприємств, як передумова успішного стабільного функціонування, вимагає організації виробництва таких товарів та послуг, які задовольнятимуть мінливий споживчий попит за якістю і ціною, а це, своєю чергою, вимагає регулярного техніко-технологічного оновлення, тобто потрібна відповідна інвестиційна стратегія в рамках антикризового управління діяльністю підприємства.

Так, Е.М. Коротков вказує, що соціально-економічна система в будь-якому вигляді та будь-якій формі, чи то суспільна формація, фірма або підприємство, має дві тенденції свого існування: функціонування і розвиток.

Функціонування – це підтримка життєздатності, збереження функцій, які визначають її цілісність, якісну визначеність, сутнісні характеристики. Розвиток – це набуття нової якості, що зміцнює життєдіяльність в умовах мінливого середовища. Функціонування стримує розвиток хоча й виступає його поживним середовищем. Розвиток руйнує функціонування, проте, водночас, створює умови для більш стійкого функціонування у майбутньому. Ці протиріччя й призводять до кризи [5].

Так як розвиток є обов'язковою умовою життєдіяльності будь – якого підприємства у ринкових умовах, то виникнення криз (чи то в цілому по підприємству, чи то по окремих товарах) є нормальним, а іноді й необхідним, явищем в умовах нормального функціонування ринкової економіки.

Теорія циклів, як важлива складова розвитку антикризового управління, досліджувалась багатьма вченими, зокрема, була сформована у роботах М.Д.Кондратьєва [4]. Основою теорії криз М.Д.Кондратьєва є:

1) взаємозв'язок закономірностей економічної статики, циклічної динаміки і соціогенетики у динаміці суспільства;

2) великі цикли кон'юнктури, їх основи і взаємозв'язок із середньостроковими циклами;

3) неможливість кризових фаз у динаміці циклів;

4) роль винаходів та інновацій у зміні великих циклів.

В загальному розумінні криза це різкий злам чого-небудь; скрутне, важке становище. В перекладі з грецької криза (гр. Krisis) означає рішення, поворотний пункт, результат, різкий, крутий перелом, важкий перехідний стан, крайня точка падіння, гостра нестача, невідповідність.

Кризи притаманні не лише підприємницькій діяльності, а й усім сферам життя суспільства: політичній, соціальній, екологічній тощо. Крім того кризи вирізняються за причинами виникнення, характером протікання, наслідком, масштабами, можливостями впливу на них тощо. У зв'язку з цим типологія криз надзвичайно розгалужена й по різному характеризується в наукових джерелах.

Найбільш вдала типологія криз, наведена на рис. 1, запропонована Е.М. Коротковим [5].

На наш погляд у зв'язку з вступом України до СОТ доцільно розрізняти й вивчати глобальну світову кризу. Загалом вирізняють кризи на макро- і мікроекономічному рівні. На макроекономічному рівні виділяють загальну економічну кризу, галузеві, регіональні, кризи фінансово-кредитної системи, фінансового ринку, платіжні тощо. На сучасному етапі розвитку сільського господарства має місце загальногалузева криза, наслідком якої є масова збитковість і фінансова нестабільність більшості підприємств.

Діяльність сільськогосподарських підприємств є ризиковою у наслідок специфіки технологічного процесу, його залежності від природно – кліматичного фактору, а також

впливу економічного та соціального середовища. Незважаючи на наявність в Україні системи заходів (на законодавчому та галузевому рівнях) підтримки сільськогосподарських підприємств, спостерігаються ознаки кризи прибутковості, рентабельності платоспроможності, а також деякі сільськогосподарські підприємства працюють в умовах системної кризи, що охоплює як виробничу так і інвестиційну та фінансову діяльність, що потребує розробки системи антикризового управління, спрямованого у першу чергу на фінансове оздоровлення - санацію.

Результативність будь-якого процесу істотнім чином залежить від ефективності управління ним. Це стосується й процесу фінансової санації підприємства.

Менеджмент санації – антикризове управління - це сукупність принципів, методів та заходів управління процесом оздоровлення фінансово-господарського стану підприємства. Головна мета управління у даному випадку полягає у досягненні високої ефективності цього процесу.

Вагомим важелем управління виступає планування як щодо визначення загальних підходів до здійснення процесу антикризового управління і розробки й узгодження окремих дій у даному процесі.

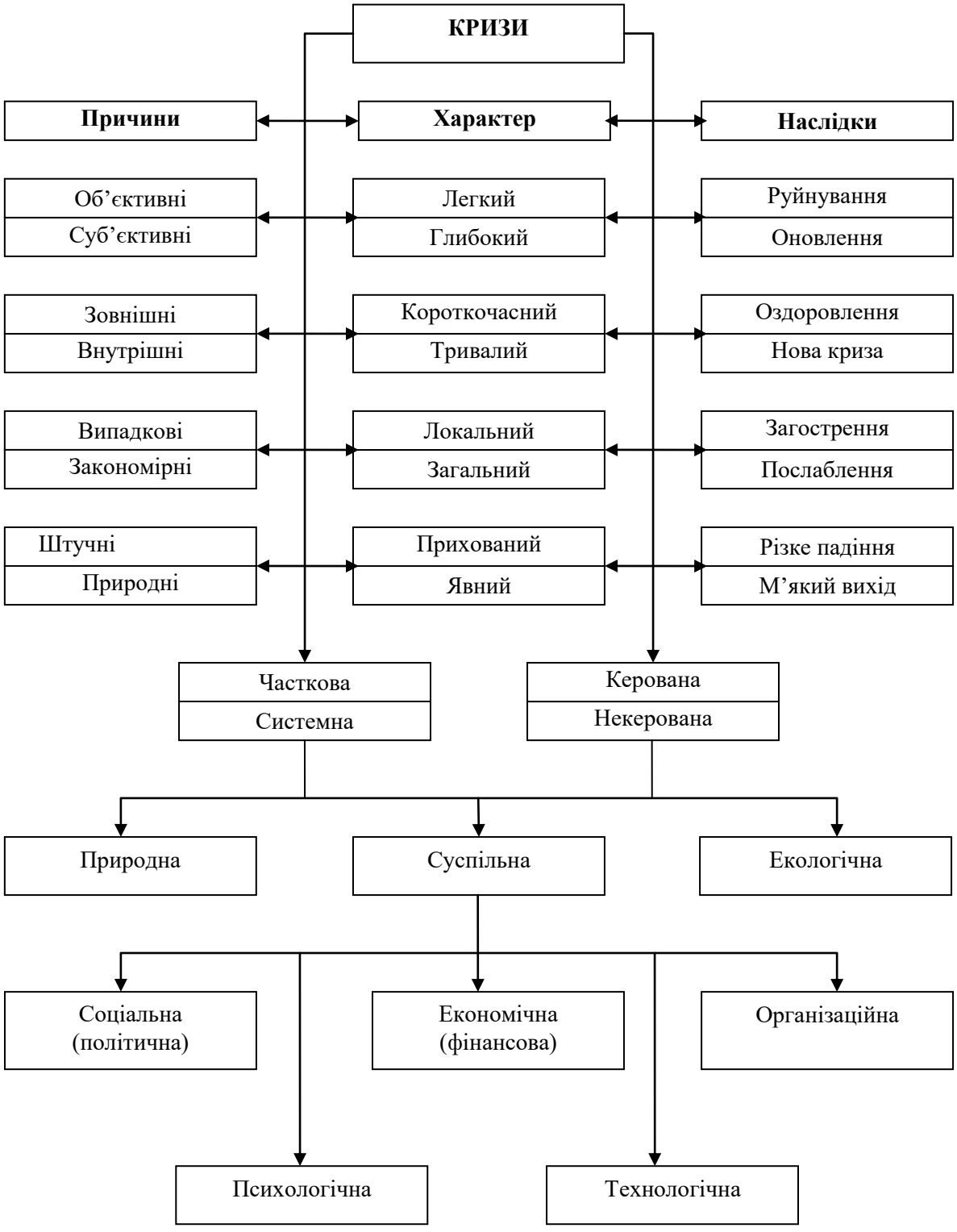


Рисунок 1 – Класифікація кризи як об'єкту антикризового управління

Джерело: [5].

Визначення загальних підходів передбачає формування антикризової концепції (програми санації), обґрунтування конкретних заходів – підготовку плану санації.

Розробку концепції антикризового управління окремого підприємства являє собою так звана „класична модель управління фінансовим оздоровленням", яка широко використовується в якості основи для визначення механізму антикризового управління суб'єктів господарювання у країнах з розвинутою ринковою економікою [5].

Класична модель включає аналіз причин виникнення кризової ситуації (причинно-

наслідковий аналіз), прийняття рішення про оздоровлення чи ліквідацію підприємства, визначення цілей управління, формування стратегії антикризового управління, розробку санаційних заходів, формування програми і плану санації, реалізацію плану санації, координацію та контроль тощо.

Цілковите розкриття та осягнення сутності антикризового менеджменту, на нашу думку, вимагає вивчення управління із двох точок зору:

по-перше, як специфічної діяльності менеджера (менеджерів) – фізичних осіб щодо безпосереднього керівництва, алміністрування підприємства;

по-друге, як економічної системи методів, принципів, моделей і заходів впливу на діяльність підприємства. Оскільки антикризове управління може здійснюватися як до, так і під час провадження справи про неплатоспроможність підприємства, то й управління згідно першої точки зору як діяльність менеджерів суттєво відрізняється.

При досудовій санації керівництво нею здійснює, як правило, керівник підприємства або антикризовий менеджер (у деяких джерелах кризис-менеджер). Проте антикризовий менеджер цілком підпорядковується керівництву підприємства і таким чином його діяльність підпорядковується діяльності топ-менеджерів підприємства.

При здійсненні антикризового управління у судовому порядку застосовується абсолютно інший підхід. Безпосереднє управління здійснює залучена стороння особа – арбітражний керуючий, при цьому він бере на себе й функції керівника підприємства, а не підпорядковується йому. Керівник підприємства при цьому згідно законодавства звільняється або, як свідчить практичний досвід, переводиться на іншу посаду. Таким чином, при судовій санації топ-менеджмент підпорядковується арбітражному керуючому.

При погодженні із комітетом кредиторів керуючим санацією може ставати керівник підприємства. Проте, у такому випадку він працює паралельно із арбітражним керуючим – розпорядником майна, звітується комітету кредиторів та господарському суду, що цілком забезпечує зовнішній нагляд і контроль за його діяльністю.

Згідно законодавства арбітражний керуючий (розпорядник майна, керуючий санацією, ліквідатор) – це фізична особа, яка має ліцензію, видану в установленому законодавством порядку, та діє на підставі ухвали господарського суду. Одна і та ж особа може виконувати функції арбітражного керуючого (розпорядника майна, керуючого санацією, ліквідатора) на всіх стадіях провадження у справі про банкрутство. Особу, що претендує на посаду арбітражного керуючого можуть пропонувати: позивач, комітет кредиторів, боржник (як правило при погодженні із комітетом кредиторів). Затвердження арбітражного керуючого на посаді в обов’язковому порядку здійснюється господарським судом. У разі коли господарському суду не запропоновано кандидатуру арбітражного керуючого у встановленому порядку господарський суд має право призначити арбітражним керуючим працівника державного органу з питань банкрутства за поданням останнього. Таким чином, робота арбітражного керуючого при проваджені справи є обов’язковою.

Арбітражний керуючий працює упродовж усього терміну судового провадження й виконує на кожній його стадії окремі функції. Так в процедурі розпорядження майном боржника арбітражний керуючий виконує функції розпорядника майном, в процедурі санації – керуючого санацією, а в ліквідаційній процедурі – ліквідатора.

Отже, керуючий санацією – це фізична особа, яка відповідно до рішення господарського суду організовує здійснення санації боржника. Керуючий санацією має право самостійно розпоряджатися майном боржника (з урахуванням певних обмежень, передбачених законодавством); укладати від імені боржника мирову угоду та інші цивільно-правові угоди; відмовлятися від виконання договорів боржника у певних випадках.

У процесах досудової санації управлінська діяльність антикризового менеджера подібна, проте вона підпорядковується керівнику підприємства та не регламентується ні комітетом кредиторів, ні господарським судом, ні законодавством щодо функцій і обов’язків.

Інша сторона менеджменту санації, як зазначалося вище, - управління санацією як система методів, принципів, моделей тощо. Такий менеджмент у науковій літературі

висвітлюється в двох основних аспектах: як антикризовий менеджмент і як контролінг.

Антикризове управління на відміну від регулювання здійснюється на мікроекономічному рівні. В літературі не існує єдиного підходу щодо визначення даного поняття.

Ми дотримуємося позиції дослідників, які вважають, що „антикризове управління підприємством – це система управління підприємством, яка має комплексний системний характер і спрямована на запобігання та усунення несприятливих для діяльності підприємства явищ за допомогою розробки і реалізації на підприємстві спеціальних заходів, які мають стратегічний характер і дозволяють усунути тимчасові перешкоди, зберегти і примножити ринкові позиції".

Головною метою антикризового управління є швидке відновлення платоспроможності та поновлення достатнього рівня фінансової стійкості підприємства, забезпечення міцного положення на ринку й стабільно стійких фінансів компанії при будь-яких економічних, політичних й соціальних метаморфозах в країни. Водночас мета і задачі антикризового управління істотно залежать від стадії кризи в якій воно вводиться.

Методи й технології антикризового управління надзвичайно різноманітні.

При впровадженні системи антикризового фінансового управління плануються усі передбачувані заходи у вигляді плану (програми). Антикризова програма підприємства являє собою спеціально підготовлений внутрішній документ, в якому систематизовано перелік основних заходів, що планується здійснити в межах підприємства, його структурних підрозділів та функціональних служб для досягнення поставленої мети – виведення підприємства з кризового стану.

Другим механізмом, крім антикризового менеджменту, управління підприємством у кризові та, особливо, передкризові періоди є контролінг. Побудові системи контролінгу присвячені чисельні дослідження.

Слово контролінг походить від англійського to control - контролювати, управляти, яке, в свою чергу, є похідним від французького слова, що означає „реєстр, список перевірки".

Контролінг дає можливість поліпшити управлінську діяльність шляхом впровадження бюджетування. Також контролінг поліпшує координацію, контроль й інші функції менеджменту.

Тим не менш, найважливіше місце як в системі контролінгу, так і в антикризовому управлінні займає аналіз причин кризи, стану підприємства, здатності його до відновлення нормального функціонування тощо.

Таким чином, у сучасних умовах невизначеності і високої ймовірності кризових явищ управління сільськогосподарськими суб'єктами господарювання потребує конструктивного менеджменту, заснованого на стратегічних підходах і попереджувальних заходах.

Список літератури

1. Брижань І., Григор'єва О. Концептуальні основи антикризової політики екологічно орієнтованого розвитку України. Економічний часопис XXI. 2015. №5-6. С. 41-44.
2. Гринчишин Я. Еволюція європейського підходу до використання фінансової реструктуризації в системі антикризового управління підприємств. Економічний часопис XXI. 2016. №156 (1-2). С. 63-66.
3. Дем'яненко М.Я., Малік М.Й. Фінансова криза в аграрному секторі АПК / М.Я. Дем'яненко, // Економічні науки. Сер.: Облік і фінанси. Вип. 7 (1). С. 408-414.
4. Кондратьев Н. Д. Большие циклы конъюнктуры и теория предвидения. Избранные труды. 2002. М.: Экономика. 767 с.
5. Коротков Э.М. Антикризисное управление: учебник. Москва: ИНФРА, 2000. 432 с.
6. Лігоненко Л.О. Антикризове управління підприємством: Теоретико-методологічні засади та практичний інструментарій: монографія. К.: КНТЕУ, 2001. 580 с.
7. Собкевич О. Напрями антикризової політики для інноваційної модернізації промисловості і забезпечення економічної безпеки України. Економічний часопис XXI. 2015. №5-6. С. 28-32.
8. Стецюк П.А. Модернізація механізмів фінансового забезпечення аграрного виробництва. Облік і фінанси. 2016. № 1(71). С. 132-136.

УДК 930.25(477)

Г. Почтарук, магістр гр. ІС-18 М
Центральноукраїнський національний технічний університет

ІСТОРІЯ АРХІВНОЇ СПРАВИ В УКРАЇНІ: СТАН ДОСЛІДЖЕННЯ

У статті проаналізувати ступінь дослідження історії архівної справи в Україні. Визначено основні напрямки досліджень радянських і сучасних істориків. Окреслено здобутки та прогалини в проведених наукових пошуках.
архів, державний архів, архівні установи, архівознавство, історіографія

Актуальність теми. Архівні документи допомагають реконструкції минулого країни, виявленню основних напрямів діяльності органів державної та виконавчої влади, захисту соціальних прав населення тощо. З огляду на затребуваність архівних документів у розв'язанні важливих політичних і соціально-економічних проблем в умовах радикальних змін у житті сучасної Української держави, дослідження історії діяльності держаних архівів набуває все більшої актуальності.

Аналіз останніх досліджень і публікацій. Історія та організація архівної справи в Україні знайшла певне відображення в історіографії. Декілька загальних праць О. Водолажченко та В. Барвінського, В. Романовського, Ф. Герасименка, А. Грінберга, С. Пількевича, Д. Щедриної з історії архівної справи в Україні, що побачили світ за радянської доби, досліджували зазначену тему, хоч висвітлювали проблеми архівістики здебільшого заангажовано [1]. Тією ж заангажованістю позначена й фундаментальна праця О. Г. Мітюкова [2]. Питання історії архівної справи в Україні та діяльності архівних установ розглянуто в працях Г. Боряка, К. Климової, І. Матяш, Н. Московченко, Г. Папакіна, Н. Павловської, Ю. Прилепішевої, Н. Христової, присвячених розвитку архівної науки, освіти, періодики, довідкового апарату архівів і рукописних відділів бібліотек; роботі Археографічної комісії ЦАУ; археографічній діяльності архівних установ [3].

Постановка завдання. Дослідження історії архівної справи сприяє осмисленню їхнього місця і ролі у житті суспільства, пізнанню закономірностей еволюції різних типів архівів, що дає змогу простежити процес збирання документальних матеріалів та формування архівних фондів. Вивчення історії архівів допомогає розв'язанню різноманітних завдань: отримати відомості про склад і зміст архівів, про особливості формування їх у різні історичні періоди, про причини та обсяги втрат документальних матеріалів, що сприятиме пошуку документів і окремих частин архівних фондів, реконструкції національної архівної спадщини.

Історія архівної справи й до сьогодні не отримала достатнього дослідження у вітчизняній історіографії. Саме тому метою нашого дослідження є виявлення публікацій з питань історії розвитку архівної справи та діяльності архівних установ, визначення хронологічних меж таких публікацій, виявлення найвагоміших наукових концепцій, з'ясування внеску авторів у вивчення проблем розвитку та організації архівної справи.

Виклад основного матеріалу. Архівна справа в Українській РСР знаходилась у скрутному становищі, адже рішення приймались і нав'язувались загальносоюзними органами, які практично не враховували специфіку архівів окремих республік. Тоді під жорстким партійним і цензурним контролем перебувала діяльність органів архівної служби, профільних кафедр вищих навчальних закладів, редколегій «Архівів України», «Українського історичного журналу», наукових збірників та інших видань.

Українські радянські історики-архівісти у своїх наукових розвідках головну увагу зосередили на питаннях та перспективах архівного будівництва в роки радянської влади. Це відобразилося у низці праць С. Д. Пількевича, Л. І. Лозенко і А. В. Кентія, О. Г. Мітюкова [4, 5]. Незважаючи на заідеологізованість цих публікацій, все ж ними введено в науковий обіг деякі важливі історичні джерела.

У 1970–1980-ті рр. в українській радянській історіографії з'явилися наукові дослідження, присвячені історії виникнення і розвитку в Україні партійних архівів. Діяльність партійного архіву Інституту історії партії при ЦК Компартії України та обласних партійних архівів висвітлено в публікаціях Д. С. Щедріної [6].

Особливий інтерес становлять праці про діяльність окремих державних архівів, написані здебільшого їхніми співробітниками на основі відповідних джерел. У них висвітлено історію архіву протягом певного періоду чи якийсь окремий вид архівної роботи. У розвідці О. М. Бунькової та О. О. Кривошеєвої «До історії Центрального державного архіву Жовтневої революції і соціалістичного будівництва УРСР» було розглянуто діяльність архіву з часу створення, тобто з листопада 1943 р., і до другої половини 1960-х рр. [7]. Значну увагу автори приділили відновленню роботи цього архіву в Києві і його філіалу в Харкові, зміцненню його матеріальної бази та функціонуванню установи після об'єднання.

Нова ситуація в історичній науці почала складатися у другій половині 1980-х рр. під впливом процесів перебудови в УРСР. З одного боку, вона ще через ідеологічний тиск переживала кризу, з іншого – тоді вже робились спроби формування нової хвилі історіографічних досліджень. Зокрема, було збільшено доступ до архівних джерел і вітчизняні дослідники архівної справи знову повернулись до вивчення історії окремих архівів.

Проголошення у серпні 1991 р. державної незалежності України, нова хвиля національно-культурного відродження, демократизація країни, її входження у світове співтовариство започаткували новий, сучасний етап розвитку архівознавства. Він пов'язаний з потребою суспільства і держави в новому осмисленні долі архівів, значення історико-архівознавчих, джерелознавчих та археографічних досліджень, з прийняттям Закону України «Про національний архівний фонд і архівні установи» (1993 р.), з реформуванням архівної системи в Україні, її демократизацією. Важливою віхою в розвитку архівознавства є заснування Українського науково-дослідного інституту архівної справи та документознавства (1994 р.), координуючого центру архівознавчих досліджень.

Одним із нових напрямків досліджень, до якого активно залучилися науковці, було питання діяльності архівних установ в умовах складних періодів української історії. Вивченню подібних тем сприяло поступове розсекречення архівних документів, що значно розширювало джерельну базу досліджень. На основі нових документальних свідчень історики-архівісти розпочали видавати праці, в яких намагались об'єктивно висвітлювати історію архівної справи раніше замовчуваного або свідомо фальсифікованого періоду. Так, збірник «Архівна та бібліотечна справа в Україні доби визвольних змагань (1917–1921 рр.)» [8] містив студії українських дослідників історії архівної справи доби УНР та Української Держави.

Для поширення наукових ідей, публікації та обговорення результатів наукових досліджень архівознавства, документознавства, спеціальних історичних дисциплін, публікації архівних документів у 1990-х рр. було засновано низку спеціальних видань: «Український археографічний щорічник» (1994), «Рукописна та книжкова спадщина України: археографічні дослідження унікальних архівних та бібліотечних фондів» (1994), в УНДІАСД – науковий щорічник «Студії з архівної справи та документознавства» (1996), археографічний щорічник «Пам'ятки» (1998), серійні видання «Історія архівної справи: спогади, дослідження, джерела», «Архівні та бібліографічні джерела української історичної думки» (1998), міжвідомчий науковий збірник «Архівознавство. Археографія. Джерелознавство» (1999).

У 1998 р. був виданий підручник «Архівознавство», автори якого під керівництвом Я. С. Калакури, виклали новітні підходи до історії, теорії і методики архівної справи. У 2002 р.

авторський колектив суттєво доповнив перше видання підручника і підготував новий узагальнюючий посібник [9].

З появою цього підручника започатковано видання серії навчальних посібників «Нариси історії архівної справи в Україні», «Хрестоматія з архівознавства», орієнтованих на те, щоб надати молодому поколінню фахівців не лише теоретичні знання, а й націлити на практичну діяльність, наповнити її новим змістом, сприяти оволодінню новітніми технологіями архівної справи, піднести соціальне і духовне значення професії.

У процесі відродження та становлення вітчизняної архівної термінології поступово відбулося впорядкування архівного понятійного апарату та професійної мови українських архівістів. Так, у 1999 р. вперше в Україні видано національний архівний термінологічний тлумачний словник «Архівістика», підготовлений авторським колективом за керівництвом К. Є. Новохатського та К. Т. Селіверстової [10]. Значення цієї праці визначається тим, що в ній проведено комплексний аналіз сучасної термінологічної ситуації та розкрито основну проблематику саме української архівістики з її особливостями та відмінностями.

У 1990-х – на початку 2000-х рр., поряд із розширенням тематики наукових досліджень, поліпшився зміст наукових праць. Одним із нових напрямків, започаткованих в архівознавстві в цей час, є вивчення історії архівної справи через особу архівіста. Так, у 1992 р. в журналі «Архіви України» з'явилася рубрика «Матеріали до словника архівних діячів», мета якої полягала у висвітленні біографій і творчої діяльності українських архівістів. На основі розвідок, що публікувались у рубриці, передбачалося розширити поле наукових праць. Водночас було започатковано серію видань «Історія архівної справи: спогади, дослідження, джерела», в яких знайшли відображення науково-професійні здобутки С. Д. Пількевича, М. Я. Варшавчика, М. А. Рубача, О. Г. Мітюкова, С. Г. Кулешова.

Найпомітнішими результатами історико-архівознавчих досліджень слід вважати колективну працю «Нариси історії архівної справи в Україні» (2002) [11], монографії І. Б. Матяш «Архівна наука і освіта в Україні 1920 – 1930-х рр.» (2000) [12] та «Українська архівна періодика 1920 – 1930-х рр.: історія, бібліографія, бібліометрія» (1999) [13], дисертаційні дослідження Г. В. Папакіна «Археографічна комісія Центрального архівного управління УСРР: історія створення і науковий доробок (1928 – 1934)» (1995) [14], Н. М. Христової «Науково-довідковий апарат архівів та рукописних підрозділів бібліотек в Україні у 1920 – 1990 рр.» (1999) [15] та ін., започаткування видавничих серій «Історія архівної справи: спогади, дослідження, джерела», «Історіографічні та бібліографічні джерела української історичної думки», спеціальної рубрики «Архівна справа: історія та сучасність» у «Студіях з архівної справи та документознавства». У процесі досліджень викристалізовувалися й перспективні напрями.

Підсумки. Отже, аналіз наукової літератури з історії архівної справи в Україні в другій половині XX – на початку XX дозволяє стверджувати, що характерною її рисою був перехід від заідеологізованої науково-дослідницької діяльності в галузі архівознавства до національного і духовного відродження, що помітно вплинуло на хід розвитку архівної системи в цілому. Характерними рисами нового етапу в розвитку історіографії історії архівної справи стали: розширення джерельної бази та проблематики досліджень, методологічна переорієнтація істориків, поява нових методологічних підходів до вивчення вітчизняної історії через відмову від ідеологічних стереотипів та значне розширення доступу до архівних документів.Крім того зауважимо, що далеко не всі аспекти історії розвитку архівної справи висвітлені достатньою мірою, особливо враховуючи те, що коло джерел впродовж останнього часу значно збільшилось, а це дає змогу доповнити і, певною мірою переглянути вже зроблені висновки. Історія архівної справи ще потребує детального дослідження, зокрема регіональних аспектів, що сприятиме створенню цілісної картини української архівної науки.

Список літератури

1. О. Водолажченко, В. Барвінський Короткий нарис історії архівної справи та діяльності Укцентрархіву за 1924 р.// АС. – 1925. – Кн. 1. – С. 45 – 72; Романовський В. О. Нариси з архівознавства: Історія архівної справи на Україні та принципи порядкування в архівах. – Харків: Черв. друк, 1927. – 170 с.; Герасименко Ф. А. До історії архівної справи на Полтавщині // АС. – 1928. – Кн. 5/6. – С. 64–73; Грінберг А. Й. Архівне будівництво на Україні в період іноземної інтервенції і громадянської війни (1918 – 1920) // Наук. записки КДУ. – 1956. – Т. XV. – Вип. VI. – С. 47 – 57; Пількевич С. Д. 40 років радянського архівного будівництва на Україні // З історії архівного будівництва на Україні. – Харків, 1958. – 115 с.; Щедрина Д. З історії становленні і розвитку партійних архівів на Україні //УІЖ. – 1978. – № 5. – С.45-52
2. Мітюков О. Г. Радянське архівне будівництво на Україні 1917 – 1973. – К.: Наук. думка, 1975. – 270 с.
3. Боряк Г.В. Національна архівна спадщина України та державний реєстр "Археографічна україніка": Архівні документальні ресурси та науково-інформаційні системи. – К., 1995. – 347 с.; Папакін Г. В. Археографічна комісія ЦАУ УСРР: історія створення і науковий доробок. (1928 – 1934 рр.): Дис.... канд. іст. наук. – К., 1995. – 223 с.; Христова Н.М. Науково-довідковий апарат архіві та рукописних відділів бібліотек в Україні у 1920 – 1990-х рр.: Автореф. дис.... канд. іст. наук. – К., 1999. – 19 с.; Московченко Н. П. Розвиток архівної справи і Україні (1919 – 1932 рр.): Автореф. дис.... канд. іст. наук. – К., 2003. – 20 с.; Павловська Н.П. В.І. Веретенников як архівознавець та архівіст.: Автореф. дис.... канд. іст. наук. – К., 2003. – 19 с. та ін
4. Пількевич С. Архівне будівництво на Україні за роки радянської влади // Архіви України. – 1968. – № 6. – С. 13–20.
5. Лозенко Л. І. Архівне будівництво в УРСР (1919-1974) / Л.І. Лозенко, А.В. Кентій // Архіви України. 1978. №3. С. 5 – 15.
6. Щедрина Д. С. Источники опыта борьбы и создания (История создания и деятельности партийных архивов Украины) / Д.С. Щедрина. – К.: Политиздат Украины, 1987. 152 с.
7. Бунькова О. М. До історії Центрального державного архіву Жовтневої революції і соціалістичного будівництва УРСР / О.М. Бунькова, О.О. Кривошеєва // Третя республіканська конференція з архівознавства. – К., 1968. – Т. 1. – С. 5 – 21.
8. Архівна та бібліотечна справа в Україні доби визвольних змагань (1917-1921 РР.) : зб. наук. пр. / Укр. держ. НДІ арх. справи та документознавства, Нац. парлам. б-ка України ; ред. В. С. Лозицький. К. : [б. и.], 1998. – 275 с.
9. Архівознавство: Підручник для студентів вищих навчальних закладів України /Авт.: Я.С. Калакура, Г.В. Боряк, Л.А. Дубровіна, К.І. Климова, та ін. – К., 1998. – 316 с.
10. Архівістика: Термінологічний словник /Авт.-упорядн.: К. Є. Новохатський, К. Т. Селіверстова та ін. – К., 1998. – 106 с.
11. Нариси історії архівної справи в Україні: Посібник / За загальною редакцією І.Б. Матяш та К.І. Климової. – К., 2002. – 612 с.
12. Матяш І. Б. Архівна наука і освіта в Україні 1920-1930-х років / Держкомархів України. УДНДІАСД. – К., 2000. –591 с.
13. Матяш, І. Б. НАН України. Нац. б-ка України ім. В.І.Вернадського. Українська архівна періодика 1920-1930-Х рр..: історія, бібліографія, бібліометрія / І. Б. Матяш ; .ред. О. С. Онищеннко ; НАН України. Нац. б-ка України ім. В.І.Вернадського. – К. : [б. и.], 1999. – 480 с.
14. Папакін Г.В. Археографічна комісія центрального архівного управління УСРР: історія створення і науковий доробок (1928-1934) : дис...канд. іст. наук: 07.00.06. НАН України, Ін-т укр. археографії та джерелознавства ім. М. С. Грушевського. – К., 1995. – 224 л.
15. Христова Н.М. Науково-довідковий апарат архівів та рукописних підрозділів бібліотек в Україні у 1920-1990 рр. [Текст] : дис... канд. іст. наук: 07.00.08. Український держ. НДІ архівної справи та документознавства Головного архівного управління України. – К., 1999. – 193 л. –л. 158-193.

УДК 658.15

М. Продан, магістр гр. АДМ-18М-1,4
Центральноукраїнський національний технічний університет

ОСОБЛИВОСТІ АНТИКРИЗОВОГО УПРАВЛІННЯ ДІЯЛЬНІСТЮ ПІДПРИЄМСТВ

Стаття присвячена дослідженню особливостей антикризового управління діяльністю підприємств у сучасних умовах. Проаналізовано підходи науковців щодо розуміння сутності антикризового управління. Наведено сутність організаційно-економічного механізму антикризового управління, причини виникнення кризових явищ, інструменти антикризового управління. Сформоване авторське визначення сутності антикризового управління з урахуванням особливостей його здійснення.
антикризове управління, криза, загроза, ризик, ефективність

Виникнення і розгортання системної кризи вражає основні складові елементи підприємницької діяльності, призводить до нездатності відновлення стану самоокупності та загрози банкрутства внаслідок зростання заборгованості на підприємстві. За таких умов потрібне швидке реагування керівників підприємства, ефективне антикризове управління та мобілізація внутрішніх ресурсів підприємства. Найефективнішим засобом виходу з кризового стану є застосування процедури антикризового управління, яка передбачає впровадження в систему підприємницької діяльності виробничо-технічних заходів, використання зовнішніх і внутрішніх резервів для відновлення прибутковості та уникнення банкрутства [1].

Підходи до трактування сутності антикризового управління наведено в табл. 1.

Таблиця 1 – Підходи до трактування сутності антикризового управління

Автор, джерело	**Підхід до визначення**
1	2
Бровко Л.І., Сірко А.Ю., Крюкова Г.В. [1]	Антикризове управління підприємства – це управління, яке орієнтується на передбачення небезпеки кризи, аналіз її симптомів і усунення загроз появи кризових ситуацій, а в разі їх появи – аналіз та прийняття швидких заходів ліквідаційного характеру з найменшими втратами та негативними наслідками.
Фокіна-Мезенцева К.В., Байда І.В. [10]	Антикризове управління – це система економічних відносин, які виникають у процесі розроблення, затвердження, реалізації та контролю над реалізацією заходів, що спрямовані на запобігання або усунення несприятливих для бізнесу явищ за допомогою використання всього потенціалу менеджменту, який дає змогу усунути тимчасові труднощі, зберегти і примножити ринкові позиції за будь-яких обставин, спираючись на різні види ресурсів.
Мостенська Т.Л., Юрій Е.О. [7]	Антикризове управління – це діяльність менеджменту, що є складовою управління економічною безпекою підприємства і полягає у передбаченні можливості настання кризової ситуації, реалізується через підготовку та впровадження відповідних управлінських рішень, взяття на себе відповідальності та контролю за реалізацією запланованих заходів, швидкому реагуванні у випадку кризової ситуації для виведення підприємства із кризового стану.

Мартинець В.В. [5]	Антикризове управління підприємством – це спеціально організована система управління, яка має комплексний системний характер, спрямована на оперативну діагностику кризи, своєчасне її подолання, недопущення банкрутства підприємства та забезпечення подальшого розвитку і підвищення конкурентоспроможності підприємства.
Тимошенко О.В., Буцька О.Ю., Сафарі Ф.Х. [9]	Антикризове управління підприємством – це система заходів передкризового (превентивного) характеру, спрямованих на проведення діагностики загрози банкрутства; реактивного характеру – пошук шляхів виходу підприємства з кризового стану; післякризового характеру, що містять оцінку посткризового стану підприємства та розробку і реалізацію дій щодо усунення підприємством негативних наслідків фінансової кризи.
Мельниченко О.О. [6]	Антикризове управління – система управління, що спрямована насамперед на раннє виявлення протиріч підприємства з зовнішнім середовищем або у його внутрішньому середовищі з огляду на окремі бізнес-процеси підприємства з метою запобігання кризовим явищам на підприємстві; при виникненні імовірності настання кризового стану – на переорганізацію виконання окремих бізнес-процесів відповідно до поточних умов господарювання; при виникненні кризового стану – на розробку механізму виходу з кризи, що передбачатиме здійснення відповідних інструментів та процедур.

Джерело: узагальнено автором

Основні причини виникнення кризових ситуацій на підприємстві розподіляють на об'єктивні та суб'єктивні. До об'єктивних причин можуть бути віднесені: економічна нестабільність; недосконаліть фінансової та законодавчої системи; інфляція, низька платоспроможність населення; велика конкурентоспроможність на ринку. До суб'єктивних причин належать: внутрішні фактори діяльності підприємства; зниження продажу через низький рівень маркетингу; високі витрати на виробництво; низька рентабельність [3].

Організаційно-економічний механізм антикризового управління підприємством являє собою систему заходів по реформуванню механізму антикризового управління у відповідності до вимог, які формуються внутрішнім та зовнішнім середовищем підприємства на сучасному етапі економічного розвитку. Кінцевою задачею формування організаційно-економічного механізму антикризового управління має стати його ефективна модель, яка б дозволяла коректувати діяльність підприємства у відповідності з метою стійкого і прогресивного розвитку [4].

Механізм антикризового управління може мати типову побудову, але не може носити універсальний характер і визначається: глибиною кризових явищ; визначеними цілями (банкрутство чи оздоровлення); внутрішнім потенціалом підприємства; силою впливу зовнішніх факторів; обмеженістю у часі і засобах (насамперед фінансових) [2].

Залежно від особливостей та глибини прояву кризи у діяльності підприємницьких структур антикризове управління використовує відповідні інструменти, такі як реструктуризація підприємства, фінансова реструктуризація (заборгованості, власності на активи), оптимізація та реінжиніринг бізнес-процесів, реорганізація, санація [8].

За іншим підходом, інструменти антикризового управління на підприємстві можуть бути класифіковані на три групи (рис. 1).

Рисунок 1 – Класифікація інструментів антикризового управління на підприємстві

Джерело: [10]

Функціональна підсистема антикризового управління підприємницької структури складається з таких етапів, як: 1) моніторинг внутрішнього та зовнішнього середовища; 2) діагностика стану бізнес-структури; 3) планування – вироблення антикризової політики підприємницької структури, що включає в себе розроблення плану та програми його фінансового оздоровлення за необхідності; 4) прийняття антикризових управлінських рішень; 5) організація виконання антикризових управлінських рішень; 6) мотивація виконання рішень; 7) облік результатів; 8) контроль виконання розроблених рішень з антикризового управління бізнес-структури [8].

Таким чином, антикризове управління являє собою управління, спрямоване на своєчасне виявлення і розпізнавання ознак появи кризових явищ на підприємстві, запобігання їх виникненню (за можливості), мінімізацію негативних наслідків впливу на підприємство та організацію заходів щодо виведення підприємства із кризового стану та нормалізації його основної діяльності.

Список літератури

1. Бровко Л.І., Сірко А.Ю., Крюкова Г.В. Економічна сутність антикризового управління підприємством. Modern economics. 2019. №15. С. 36-40.
2. Бурбело Н.О. Формування комплексу заходів антикризового управління підприємством. Інноваційна економіка. 2017. №1-2. С. 65-70.
3. Кравченко М.С., Митюк М.С. Антикризове управління в сучасних економічних умовах. Теоретичні і практичні аспекти економіки та інтелектуальної власності. 2018. Вип. 18. С. 190-198.
4. Мажаренко К.П., Бражнікова Т.М. Визначення механізму антикризового управління на вітчизняних підприємствах машинобудівної галузі. Економічний форум. 2019. №3. С. 143-149.

5. Мартинець В.В. Особливості антикризового управління промисловим підприємством. Науковий вісник Херсонського державного університету. Серія: Економічні науки. 2015. Вип. 11(4). С. 48-51.
6. Мельниченко О.О. Сутність антикризового управління підприємством у сучасних умовах господарювання. Економічний аналіз. 2015. Т. 21(2). С. 157-162.
7. Мостенська Т.Л., Юрій Е.О. Інструменти антикризового управління. Український журнал прикладної економіки. 2019. Т. 4, №1. С. 64-72.
8. Овсак О.П., Кривицька Н.Ю., Савицька І.А. Складники антикризового управління підприємницькою структурою. Проблеми системного підходу в економіці. 2019. Вип. 5(1). С. 99-103.
9. Тимошенко О.В., Буцька О.Ю., Сафарі Ф.Х. Антикризове управління як передумова підвищення ефективності діяльності підприємства. Економічний аналіз. 2016. Т. 23(2). С. 187-192.
10. Фокіна-Мезенцева К.В., Байда І.В. Удосконалення інструментів антикризового управління на підприємстві. Бізнес-навігатор. 2019. Вип. 5-1. С. 143-148.

УДК 338.47

Д. Рибалка, магістр гр. ОКД-18М-1,4
Центральноукраїнський національний технічний університет

НАПРЯМКИ ПІДВИЩЕННЯ КОНКУРЕНТОСПРОМОЖНОСТІ ПІДПРИЄМСТВА

В статті розглянуті актуальні питання теоретичного характеру щодо визначення поняття «конкурентоспроможність підприємства» стосовно підприємств дорожньо-будівельної галузі. Обґрунтовано, що розвиток інноваційного потенціалу, активізація управлінських зусиль щодо збільшення виробничої потужності за рахунок впровадження науково-технічних досягнень і успішного міжнародного досвіду є важливою умовою підвищення конкурентоспроможності дорожньо-будівельного підприємства.
підприємство, конкурентоспроможність, дорожньо-будівельна галузь, управління

Постановка проблеми. В сучасних економічних умовах проблема підвищення конкурентоспроможності є актуальною для підприємств усіх галузей економіки. Особливо це питання важливе для підприємств дорожньо-будівельного господарства. Це пов’язано з багатьма причинами. Насамперед, розвиток дорожньої мережі і транспортної інфраструктури визначає інтенсивність економічних зв’язків і є одним з найважливіших умов розвитку економіки країни. Активне зростання економіки країни може суттєво гальмуватися інфраструктурними обмеженнями, в основі яких лежить низька якість доріг та низька пропускна здатність інфраструктурних об’єктів дорожньої мережі, зокрема мості та тунелів. Отже, на сучасному етапі становлення та розвитку ринкової економіки в Україні особливо важливим стає питання забезпечення високого рівня конкурентоспроможності українських підприємств дорожньо-будівельної галузі.

Аналіз останніх досліджень і публікацій. Існує значна кількість опублікованих робіт, присвячених вивченню окремих аспектів процесу управління конкурентоспроможністю підприємств. Зокрема, забезпеченню підвищення конкурентоспроможності вітчизняних підприємств присвячено праці наступних вітчизняних науковців: І. Багрова. О. Нефедова, А. Воронкова, І. Должанський, Р. Лупак, А. Дідич, С. Клименко, Т. Омельяненко, Д. Барабась, О. Дуброва, А. Вакуленко, С. Хамініч та інші. Проте недостатньо дослідженими є питання підвищення конкурентоспроможності підприємств саме дорожньо-будівельного господарства.

Мета статті. Метою написання даної статті є дослідження теоретичних засад підвищення конкурентоспроможності підприємств дорожньо-будівельного господарства України в сучасних економічних умовах.

Виклад основного матеріалу. Дослідження літературних джерел показало, що є чимало дискусійних питань, пов’язаних із визначенням місця і ролі дорожньо-будівельного

комплексу в сучасній економічній системі України. Так, недостатньо розроблені питання розвитку системи управління підприємствами дорожньо-будівельного комплексу для піднесення їх інноваційної складової і підвищення конкурентоспроможності, що загалом негативно відображається на практичних аспектах вирішення проблем галузі. Не повною мірою також вивчені можливості адаптації успішного зарубіжного досвіду управління конкурентоспроможністю підприємств дорожньо-будівельної галузі в сучасних українських умовах.

Національна транспортна стратегія України на період до 2030 року «Drive Ukraine 2030» передбачає комплексний розвиток автомобільних доріг, будівництво національної мережі автомагістралей з 10 автобанів на умовах концесії, а також розвиток міжнародних транспортних коридорів (як-от міжнародний інфраструктурний проект GO Highway) [8]. В згаданому документі зазначається, що збільшення ефективності та конкурентоспроможності транспортної галузі, а також вдосконалення правового механізму державно-приватного партнерства є вкрай необхідним для нашої держави. Також в Стратегії запланований ремонт близько 24 000 км доріг загальнодержавного значення за п’ять років, а до розбудови Транс'європейської транспортної мережі включено 39 інфраструктурних проєктів з України.

В цьому зв’язку збільшення ефективності та конкурентоспроможності підприємств дорожньо-будівельної галузі України набуває особливого значення.

Слід підкреслити, що підвищення ефективності загального управління підприємством є важливою умовою забезпечення конкурентоспроможності дорожньо-будівельних підприємств. Так, можливість швидкої передачі управлінського рішення до виконання, його контрольованість, а також професіоналізм та авторитетність керівництва формують загальну ефективність управління підприємством. Підвищення ефективності діяльності підприємства, яку можна оцінити за показниками витрат на будівництво об’єкту, фондовіддачі, рентабельності, продуктивності праці тощо свідчить про загальну ефективність менеджменту і рівень конкурентоспроможності дорожнього підприємства.

Відмітимо, що конкурентоспроможність дорожнього підприємства і конкурентоспроможність дорожньо-будівельної продукції, виконаних робіт або послуги є різними поняттями Конкурентоспроможність дорожньо-будівельної продукції, виконаних робіт або послуги – це їх властивість бути на ринку нарівні з аналогічними про, що виконуються іншими підприємствами галузі.

Вагомим напрямом підвищення конкурентоспроможності підприємств дорожньо-будівельної галузі, з нашої точки зору, є розвиток їх інноваційного потенціалу. В свою чергу, управління інноваційним розвитком підприємств дорожньо-будівельної галузі полягає у переході на більш сучасну, високопродуктивну техніку при будівництві та ремонті доріг; у використанні передових технологій та матеріалів для збільшення довговічності та надійності автодорожнього покриття; розвитку транспортних розв’язок для збільшення пропускної здатності доріг.

Крім того, інноваційна діяльність в дорожньому господарстві має високу соціально-економічну значущість. Застосування нових технологій, техніки, конструкцій і матеріалів сприяє суттєвому покращенню споживчих властивостей автомобільних доріг, до яких можна віднести безперервність, безпеку, швидкість і зручність руху; високу пропускну здатність і низький рівень завантаження доріг; екологічну безпеку тощо.

Висновки. У сучасних економічних умовах для досягнення ефективних результатів своєї роботи дорожньо-будівельним підприємствам необхідно пристосовуватися до мінливих умов, які, в свою чергу, вимагають розробки інноваційних концепцій розвитку підприємств і підвищення їх конкурентоспроможності. На сьогодні існує невідповідність стану дорожнього господарства України цілям і задачам економіки, що викликає необхідність вирішення теоретичних і практичних проблем підвищення конкурентоспроможності підприємств дорожньо-будівельної галузі. Одним із способів набуття конкурентних переваг є розвиток інноваційного потенціалу дорожньо-будівельних підприємств, але разом із тим, забезпечення

бажаного рівня конкурентоспроможності дорожньо-будівельних підприємств неможливе без системного підходу до вирішення цього питання.

Список літератури

1. Багрова І. В., Нефедова О. Г. Складові та фактори конкурентоспроможності // Вісник економічної науки України. 2007. №1(11). С. 11–16.
2. Воронкова А.Е. Конкурентоспроможність підприємства: механізм управління та діагностика / А.Е. Воронкова. Економіка промисловості. 2009. № 3. С. 133-137.
3. Должанський І.З. Конкурентоспроможність підприємства: навчальний посібник [Текст] / І.З. Должанський, Т.О. Загорна. – Київ: Центр навчальної літератури, 2006. – 384 с.
4. Друкер П. Ф. Эпоха разрыва: ориентиры для нашего меняющегося общества: Пер. с англ. М.: ООО «И.Д. Вильямс», 2007. 336 с.: ил.
5. Інноваційний менеджмент: Навч. посібник. Краснокутська Н. В. Київ: КНЕУ, 2003. 504 с.
6. Литвиненко, О.Г. Оцінка конкурентоспроможності підприємства: кваліметричний підхід [Текст]. Бюлетень міжнародного Нобелівського економічного форуму. 2011. № 1 (4). С. 235- 240.
7. Лупак Р. Л., Дідич А. М. Економічні основи забезпечення конкурентоспроможності підприємства в умовах ринкових відносин // Науковий вісник НЛТУ України. 2010. – Вип. 20.6. – С. 248–252.
8. Національна транспортна стратегія України на період до 2030 року. / [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/430-2018-%D1%80#n13
9. Овсюк М.О. Удосконалення методів конкурентоспроможності будівельного підприємства в умовах кризи .Науковий журнал «Бізнес Інформ». 2011. № 6. С. 65-67.
10. Павлова В. А. Конкурентоспроможність підприємства: оцінка та стратегія забезпечення. – Д.: Вид-во ДУЕП, 2006. – 276 с.
11. Пєтєшова Т.А. Методичні підходи до оцінки рівня конкурентних переваг і конкурентоздатності підприємства / Т.А. Пєтєшова // Економіка: проблеми теорії та практики : збірник наукових праць. – Випуск 261: В 7 т. – Т. IV. – Дніпропетровськ: ДНУ, 2010. – С. 908-918.
12. Портер М. Конкурентная стратегия: Методика анализа отраслей и конкурентов. М. Альпина Бизнес Букс, 2006. 454 с.
13. Рогатинський, Р.М., Ковальчик О.А. Чинники впливу на ефективність функціонування підприємств дорожньо-будівельного комплексу України / Матеріали IX Міжнародної науково-методичної інтернет-конференції форумі молодих економістів-кібернетиків «Моделювання економіки: проблеми, тенденції, досвід» (30 жовтня 2018 р., м. Львів).
14. Скрипко Т. О. Інноваційний менеджмент: підручник / Т. О. Скрипко. – К. : Знання, 2011. – 423 с.
15. Управління конкурентоспроможністю підприємства : навч. посіб. / С.М. Клименко, Т.В. Омельяненко, Д.О. Барабась, О.С. Дуброва, А.В. Вакуленко. – К.: КНЕУ, 2008. – 520 с.
16. Хамініч С. Методика інтегральної оцінки рівня конкурентоспроможності промислового підприємства. Економіст. 2006. № 10 (240). С. 59-61.

УДК 65.012

С. Ритов, магістр гр. УФЕБ-18М-1,4
Центральноукраїнський національний технічний університет

МЕХАНІЗМИ ПІДВИЩЕННЯ ФІНАНСОВО-ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВ

У процесі дослідження проведено аналіз теоретичних та практично-прикладних підходів щодо функціонування механізму підвищення фінансово-економічної безпеки вітчизняних підприємств. Відзначено, що даний механізм включає основну мету, завдання, принципи, функції та методи управлінського впливу. Ключовою умовою ефективності функціонування механізму забезпечення фінансово-економічної безпеки підприємств є комплексний характер застосування його основних складових залежно від ситуації, що склалася у внутрішньому та зовнішньому середовищі суб'єкта господарювання.
фінансово-економічна безпека, управління, механізм, принцип, функція, метод

У сучасних умовах господарювання багато українських підприємств перебувають у нестабільному економічному та суспільно-політичному середовищі, переживають спад виробництва і знаходяться в критичному стані закриття або банкрутства. Тому фінансово-економічна безпека, фінансово-економічна стійкість суб'єктів господарювання має бути у постійній увазі менеджменту з метою прийняття оптимальних управлінських рішень щодо розвитку або збереження підприємницької діяльності [8].

Забезпечення фінансово-економічної безпеки являє собою процес зміцнення фінансового стану господарюючого суб'єкту, запобігання негативних впливів потенційних внутрішніх та зовнішніх загроз, в умовах динамічного розвитку глобальної і національної економік. Факторами негативного впливу є зменшення власного капіталу, промисловий шпіонаж, розголошення комерційної таємниці, неефективна стратегія підприємства, неграмотна дивідендна політика, форс-мажорні обставини, стан світової фінансової кон'юнктури, стагнація економіки держави, спекулятивні дії з цінними паперами, лобіювання фінансово-економічних інтересів конкурентів, агресивна купівля акцій підприємства конкурентами [10].

Фінансово-економічна безпека може бути визначена як стан та динаміка найбільш ефективного використання корпоративних ресурсів, виражені в оптимальних значеннях фінансових показників прибутковості і рентабельності бізнесу, якості управління та використання основних і оборотних коштів, структури капіталу [8].

В цілому, розрізняють такі підходи до розуміння сутності фінансово-економічної безпеки підприємства: ресурсний, системний, потоковий, виробничий підхід, конкурентний, гармонійний, захисний, функціональний [4].

Основними завданнями формування системи фінансово-економічної безпеки підприємства є: 1) виявлення та ідентифікація реальних і потенційних загроз ефективній діяльності підприємства; 2) вжиття необхідних заходів для нейтралізації виявлених загроз; 3) ознайомлення колективу підприємства з необхідністю функціонування та основними проблемами фінансово-економічної безпеки підприємства; 4) систематичний моніторинг стану фінансово-економічної безпеки підприємства на основі комплексу фінансово-економічних критеріїв [9].

Під час організації, побудови та функціонування системи економічної безпеки підприємств необхідно дотримуватися таких принципів:

– комплексність (системність) та доцільність – необхідність створення такої системи безпеки, що забезпечила б захищеність всіх об'єктів захисту підприємства;

– пріоритет заходів запобігання (своєчасність) та наступність – раннє виявлення чинників невизначеності, ризиків і загроз та запобігання їх шкідливому впливу;

– безперервність та послідовність – постійна дія системи;

– регламентованість, нормативність та законність – робота повинна здійснюватися на основі чинного законодавства, інструкцій і нормативів;

– плановість, узгодженість – діяльність із забезпечення безпеки організується на основі єдиного задуму, викладеного в комплексній програмі та конкретних планах з окремих напрямів безпеки;

– оптимальність – досягнення максимальної функціональної ефективності (віддачі) системи економічної безпеки за більш-менш фіксованих витрат виділених для неї ресурсів;

– взаємодія – погодженість у діяльності всіх учасників системи, включаючи тісні ділові контакти й узгодження дій із зовнішніми організаціями, які забезпечують безпеку підприємств;

– поєднання гласності та конфіденційності – з одного боку, система основних заходів безпеки повинна бути відома всім працівникам підприємства, а з другого – цілий ряд способів, сил, засобів, методів забезпечення безпеки повинні бути відомі дуже вузькому колу фахівців;

– компетентність та фаховість – професійність всіх учасників системи [1].

Фінансово-економічна безпека відіграє значну роль у функціонуванні будь-якого господарюючого суб'єкта, особливо в нестійких умовах їх функціонування, яка виражається у проведенні наступних заходів: виконання цілей і досягнення поставлених завдань підприємства; доступ до економічних ресурсів і ринків; забезпечення достатнього рівня ефективності фінансово-економічної діяльності; створення передумов до стійкого розвитку; захищеність від зовнішніх та внутрішніх загроз та небезпек [2].

На думку фахівців, механізм формування системи фінансово-економічної безпеки підприємства являє собою сукупність всіх його основних принципів, функцій, методів, прийомів, інструментів та стимулів [3].

З точки зору Чаленко Н.В., Діденко А.В., механізм її забезпечення фінансово-економічної безпеки підприємства являє собою сукупність законодавчих актів, правових норм, спонукальних мотивів і стимулів, методів, заходів, сил і засобів, за допомогою яких суб'єкт впливає на об'єкт для досягнення цілей безпеки і розв'язання завдань, які стоять перед нею. При цьому, для визначення кількісного рівня фінансово-економічної безпеки підприємства використовується декілька підходів: індикаторний (пороговий), ресурсно-функціональний, програмно-цільовий (комплексний), підхід на основі теорії економічних ризиків [11].

Логіко-структурна модель формування механізмів управління безпекою підприємства, як відзначає Мойсеєнко І.П., повинна складатися з таких механізмів: організаційно-синергетична інтеграція; вертикальна інтеграція, що використовує організаційно-адміністративний ресурс; горизонтальна інтеграція, яка використовує функціональний ресурс, котрий забезпечує ефект мультиплікації; синергетичної орієнтації використання інтелектуальних ресурсів [5].

До функціональної структури механізму управління фінансово-економічною безпекою можна віднести такі основні функції управління:

– планування, включаючи програмування і прогнозування (розробка оперативних та стратегічних планів, концепцій та програм розвитку, прогнозів);

– організацію і регулювання (вироблення і реалізація управлінських рішень;

– розробка і використання фінансових інструментів);

– стимулювання (використання економічних та соціально-психологічних методів управління; зростання ефективності праці);

– контроль у складі обліку, аналізу і аудиту (формування контрольно-аналітичної інформації виконання планів, програм; аудит стану фінансової безпеки підприємства) [6].

Орлик О.В. констатує, що механізм забезпечення фінансово-економічно безпеки включає такі методи управління, як: інституційно-правові, адміністративні (організаційно-розпорядчі), економічні, організаційно-технологічні, інформаційні, соціально-психологічні. Автор наголошує, що механізм забезпечення фінансово-економічної безпеки підприємства є невід'ємною частиною системи його економічної безпеки, що: базується на певних завданнях, функціях і принципах; передбачає використання системної сукупності методів, інструментів та конкретних заходів їх реалізації, які необхідно використовувати не розрізнено, а у поєднанні, комплексно і оперативно [7].

На підставі вищевикладеного можна зробити висновок, що механізм забезпечення і підвищення фінансово-економічної безпеки підприємств за сучасних умов є поняттям надзвичайно комплексним. Даний механізм має свою чітко визначену мету, його функціонування відбувається на основі відповідних принципів (комплексності, системності, доцільності, оптимальності, взаємодії, безперервності, плановості, послідовності, узгодженості та ін.). Функції механізму підвищення фінансово-економічної безпеки підприємств у загальному вираженні є такими ж, як і для будь-якого управлінського механізму, і включають планування, організацію, мотивацію і контроль, проте сам процес реалізації цих функцій має свою специфіку. Методи механізму підвищення фінансово-економічної безпеки підприємств можуть бути об'єднані у три великі крупи: організаційно-розпорядчі, економічні та соціально-психологічні.

Список літератури

1. Антошкін В.К. Шляхи та принципи удосконалення фінансово-економічної безпеки аграрних підприємств на засадах системного підходу. Молодий вчений. 2018. №9(2). С. 457-460.
2. Бондарчук Н.В., Педько А.С. Фінансово-економічна безпека як запорука розвитку алого підприємства. Молодий вчений. 2018. №10(1). С. 296-299.
3. Городиський Т.І., Паласевич М.Б., Семак Б.Б. Механізм формування системи фінансово-економічної безпеки підприємства. Інноваційна економіка. 2017. №9-10. С. 48-51.
4. Круглянко А.В. Особливості управління фінансово-економічною безпекою підприємства. Вісник Чернівецького торговельно-економічного інституту. Економічні науки. 2018. Вип. 3. С. 108-118.
5. Мойсеєнко І.П. Системний механізм управління фінансово-економічною безпекою підприємства. Науковий вісник Львівського державного університету внутрішніх справ. Серія: економічна. 2013. Вип. 1. С. 284-291.
6. Одношевна О.О., Малоок Н.Р. Теоретичні аспекти управління фінансово-економічною безпекою підприємства: стратегія та механізми забезпечення. Молодий вчений. 2016. №12. С. 805-808.
7. Орлик О.В. Механізм управління фінансово-економічною безпекою підприємства та його основні складові. Фінансово-кредитна діяльність: проблеми теорії та практики. 2015. Вип. 2. С. 222-232.
8. Рогатіна Л.П. Формування та управління розвитком фінансово-економічної безпеки підприємств. Науковий вісник Херсонського державного університету. Серія: Економічні науки. 2015. Вип. 15(3). С. 86-88.
9. Сабецька Т.І. Формування організаційно-економічного механізму забезпечення фінансово-економічної безпеки підприємства. Науковий вісник Херсонського державного університету. Сер.: Економічні науки. 2017. Вип. 24(1). С. 140-144.
10. Хаджинова О.В., Куртяник М.С. Теоретичні аспекти забезпечення фінансово-економічної безпеки підприємств України. Теоретичні і практичні аспекти економіки та інтелектуальної власності. 2018. Вип. 18. С. 120-126.
11. Чаленко Н.В., Діденко А.В. Механізм забезпечення фінансово-економічної безпеки підприємства. International scientific journal. 2015. №9. С. 164-167.

УДК 336:658.1

Я. Самарська, магістр гр. АДМ-18М-1,4
О. Сторожук, доц., канд. екон. наук
Центральноукраїнський національний технічний університет

АКТУАЛЬНІ ПИТАННЯ ІННОВАЦІЙНОГО РОЗВИТКУ ПІДПРИЄМСТВА

В статті розглянуті актуальні питання стратегічного розвитку підприємств дорожньої галузі України в сучасних економічних умовах, визначено чинники, що гальмують інноваційний розвиток у дорожньому господарстві України. Запропоновано шляхи активізації інноваційного розвитку підприємств дорожньої галузі: вивчення та впровадження зарубіжного досвіду щодо сучасних технологій будівництва і ремонту автодоріг, створення єдиної інформаційно-аналітичної системи управління автомобільними дорогами загального користування з доступом громадськості до інформації щодо стану автомобільних доріг.
підприємство, дорожнє господарство, інноваційний розвиток, державна політика

Постановка проблеми. В сучасних економічних умовах великого значення набуває стратегічне управління інноваційним розвитком підприємств, особливо це стосується підприємств, які займаються будівництвом автомобільних доріг як головної складової будівельної галузі. Особливістю інноваційного типу розвитку підприємства галузі дорожнього господарства є перенесення акценту на застосування принципово нових прогресивних технологій, своєчасні управлінські рішення в інноваційній діяльності, проведення політики ресурсозбереження тощо. Здатність до безперервного генерування та

впровадження інновацій є однією з основних умов успіху підприємства в конкурентній боротьбі.

Тому дослідження питання інноваційного розвитку підприємств дорожньої галузі України є актуальними з теоретичної і практичної точки зору.

Аналіз останніх досліджень і публікацій. Питання діяльності підприємств дорожнього господарства досліджують у своїх працях І.А. Дмитрієв [1], І.Г. Канцур [3], Є.С. Луцкін [4], О.О. Солодовнік [511] та ін. Особливості фінансового забезпечення функціонування дорожнього господарства розглядали в своїх роботах такі вчені, як Р.М. Рогатинський [7], О.О. Святець [9], Н.В. Серьогіна [10].

Але, не дивлячись на значну кількість наукових праць, присвячених даній тематиці, питання удосконалення інноваційного розвитку підприємств дорожньої галузі України залишаються актуальними.

Мета статті. Метою написання даної статті є дослідження особливостей діяльності підприємств дорожньої галузі України в сучасних умовах та окреслення напрямків удосконалення їх інноваційного розвитку.

Виклад основного матеріалу. Структура дорожнього господарства України є досить складною. Загалом, вона містить автомобільні дороги, інженерні мережі, а також підприємства й організації усіх форм власності, що їх обслуговують. Більшість таких підприємств ще мають державну форму власності, а отже їх діяльність підпорядковується державі. В свою чергу, головним суб'єктом державного управління в сфері дорожнього господарства, який реалізує під наглядом Кабінету Міністрів України відповідну державну політику, є Державне агентство автомобільних доріг України (Укравтодор). При цьому основна діяльність підприємств дорожнього господарства проваджується у складі ПАТ «ДАК «Автомобільні дороги України», яке дотепер практично є монополістом на вітчизняному ринку дорожньо-будівельних робіт. Слід відзначити, за останні два роки спостерігається позитивна тенденція щодо збільшення обсягів фінансування дорожніх робіт, а також спостерігається нарощування обсягів робіт з будівництва та ремонту автомобільних.

Інноваційний процес в дорожньому господарстві є втіленням нововведень, як правило – результатів науково-дослідних та дослідно-конструкторських робіт. При цьому створюється принципово нова якість більш технологічної продукції і формуються нормативно-технічні вимоги до її складу, які використовуються згодом в інженерних дорожніх проєктах.

Важливим етапом стратегічного інноваційного управління підприємствами дорожнього господарства є визначення довгострокових цілей. Формулювання місії і встановлення цілей підприємства дає можливість усвідомити, для чого підприємство функціонує, і яких цілей прагне досягти. Цілі підприємства повинні встановлюватися з урахуванням: обсягів і термінів робіт; наявних і очікуваних можливостей; бажаних результатів; узгодженості на всіх рівнях управління; зростання компетентності працівників тощо.

Ефективна організація виробництва в дорожньому господарстві базується на безперервному інноваційному процесі, що здійснюється відповідно до тенденцій і динамікою науково-технічного прогресу. При розгляді динаміки технологічних інновацій можна виділити фази зародження і матеріалізації нового технічного рішення, кульмінації (активного виробничого використання), неминучого припинення життєвого циклу в результаті освоєння інновації або витіснення більш ефективною.

Можна запропонувати типові функціональні алгоритми процесів сталого розвитку інноваційної діяльності, функції відповідності "ресурс - потреба - безперервність", організації управління стійкістю процесу розвитку, формування цілей і задач процесів організації та управління. Розкривається сутність наукової категорії технологічної інновації як матеріалізується технологічного нововведення, тобто знаходиться в процесі, розвитку, в процесі впровадження в практику. Уточнено роль і значення НДДКР для інноваційного процесу. Перша - дослідно-дослідницька стадія НДДКР - є передумовою зародження

технологічної інновації, друга - дослідно-промислова - по суті, народжує технологічну інновацію. Технологічна інновація має два основні періоди еволюції життєвого циклу: розвиток (становлення) і завоювання ринку, в процесі якого вона або сприймається виробництвом товарів і послуг, або витісняється новою, більш прогресивної.

На сьогоднішній день інноваційний розвиток дорожньої галузі гальмується наступними чинниками: - нестачею фінансових ресурсів для впровадження інновацій у підприємствах транспортно-дорожнього комплексу, що зумовлено, насамперед, падінням обсягів перевезень, низьким рівнем рентабельності підприємств внаслідок застарілої матеріально-технічної бази та нераціональної структури витрат, низьким рівнем державно регульованих тарифів на перевезення, збитковістю пільгових перевезень. Великою проблемою є також відсутність фундаментальних наукових досліджень, які спрямовані на здійснення якісних змін у системі продуктивних сил, та недостатньою кількістю прикладних наукових досліджень у сфері транспортно-дорожнього комплексу.

Висновки. Створення умов для розвитку транспортно-дорожнього комплексу на інноваційній основі потребує активізації державної політики у напрямку посилення інноваційної складової державних програм розвитку транспортних підгалузей, стимулювання транспортних підприємств до впровадження інновацій, запровадження державної підтримки найважливіших інноваційних проектів та наукових досліджень у транспортній сфері.

Список літератури

1. Дмитрієв І. А., Бурмака М. М. Сучасний стан та перспективи розвитку мережі автомобільних доріг загального користування. Проблеми і перспективи розвитку підприємництва. 2013. № 1. С. 64-72.
2. Закон України «Про джерела фінансування дорожнього господарства України» № 1562-XII від 18 вересня 1991 року (чинний в редакції від 01.01.2019 р.) : сайт. URL : https://zakon.rada.gov.ua/rada/show/1562-12 (дата звернення : 18.12.2019).
3. Канцур І. Г. Сучасний стан та особливості будівництва доріг в Україні на умовах концесії. Ефективна економіка. № 3. 2017. : сайт. URL : http://www.economy.nayka.com.ua/?op=1&z=5488 (дата звернення : 18.12.2019).
4. Луцкін Є. С., Серьогіна Н. В. Основні проблеми та можливості розвитку дорожньо-транспортної інфраструктури України. Вісник ОДАБА. 2016. № 63. С. 223-229. : сайт. URL : http://mx.ogasa.org.ua/handle/123456789/2108 (дата звернення : 17.12.2019).
5. Постанова КМУ «Про затвердження Порядку спрямування коштів державного дорожнього фонду» № 1085 від 20 грудня 2017 р. (чинна в редакції
6. Реформи управління автомобільними дорогами : сайт. URL : https://mtu.gov.ua/content/reformi-v-dorozhniy-galuzi.html (дата звернення : 17.12.2019).
7. Рогатинський, Р.М., Ковальчик О.А. Чинники впливу на ефективність функціонування підприємств дорожньо-будівельного комплексу України / Матеріали IX Міжнародної науково-методичної інтернет-конференції форумі молодих економістів-кібернетиків «Моделювання економіки: проблеми, тенденції, досвід» (30 жовтня 2018 р., м. Львів). 6. Сервіс для визначення кодів видів економічної діяльності
8. Розпорядження КМУ «Про схвалення Національної транспортної стратегії України на період до 2030 року» № 430-р від 30 травня 2018 р. (чинне в редакції від 30.05.2018 р.) : сайт. URL : https://zakon.rada.gov.ua/laws/show/430-2018-%D1%80 (дата звернення : 18.12.2019).
9. Святець О. О. Аналіз фінансового стану Державного агентства автомобільних доріг України та особливості фінансового забезпечення автодорожньої галузі. Науковий вісник Херсонського державного університету. Серія «Економічні науки». 2015. Випуск 11. Частина 4. С. 138-141. : сайт. URL : http://www.ej.kherson.ua/journal/economic_11/159.pdf (дата звернення :18.12.2019).
10. Серьогіна Н. В. Джерела фінансування розвитку дорожньої інфраструктури регіонів. Економічний вісник Запорізької державної інженерної академії. 2016. Випуск 3 (03) С. 105-109. : сайт. URL : http://nbuv.gov.ua/UJRN/evzdia_2016_3_22 (дата звернення : 18.12.2019).
11. Солодовнік О. О. Розвиток дорожнього господарства України у посткризовому періоді. Причорноморські економічні студії. 2017. Випуск 23. С. 55-59. : сайт. URL : http://bses.in.ua/journals/2017/23_2017/12.pdf (дата звернення : 18.12.2019).

УДК 331.5/005.95

Т. Сидельникова, магістр гр. МЕ-18МЗ
Центральноукраїнський національний технічний університет

ВИКОРИСТАННЯ СУЧАСНИХ МЕТОДІВ ОЦІНКИ ПЕРСОНАЛУ НА ПІДПРИЄМСТВІ

Стаття присвячена сучасним методам оцінки персоналу, визначенню їх переваг та недоліків. У статті визначається сутність терміну «оцінка персоналу», характеризуються складові елементи системи оцінки персоналу, наводиться класифікація методів оцінки та визначається доцільність їх використання.
оцінка персоналу, методи оцінки, критерії оцінки, оціночна шкала, компетенції

Менеджмент персоналу передбачає широке використання результатів оцінки персоналу, адже кожна організація прагне зберегти найпродуктивніші кадри, створити їм умови для професійно-кваліфікаційного зростання і одночасно позбутися працівників інертних, малокваліфікованих, безперспективних.

Проте, перш ніж будувати систему оцінки персоналу на підприємстві та обирати ефективні методи оцінки, визначимо сутність терміну «оцінка персоналу», яка досить різниться в роботах вітчизняних вчених (табл. 1).

Інструментарій системи оцінки персоналу сформувався під впливом потреб вирішення практичних завдань виробничо-управлінської діяльності на основі певних методів. Методи оцінки персоналу мають відповідати структурі підприємства, характеру діяльності персоналу, цілям оцінки, бути простими і зрозумілими; включати 5-6 кількісних показників, поєднувати письмові та усні завдання. Методи оцінки персоналу є найголовнішою складовою оцінки персоналу та, на жаль, єдиної класифікації методів оцінки не існує.

Крушельницька О.В., Мельничук Д.П., методи оцінки персоналу ділять на традиційні і нетрадиційні. Перші сфокусовані на окремого працівника і ґрунтуються на суб'єктивній оцінці керівника або колег. Їх недоліками є те, що оцінка дається окремому працівнику без врахування цілей організації, ґрунтується на оцінці керівника, при повному ігноруванні думки колег по роботі, підлеглих, клієнтів; орієнтується на минуле (досягненні результати) і не враховуються довготермінові перспективи розвитку організації і працівника. Нетрадиційні методи - розглядають робочу групу (підрозділ, бригаду, колектив) і ставлять акцент на оцінку працівника його колегами і здатність працювати в групі; оцінка окремого працівника і робочої групи проводиться з урахуванням результатів всієї організації, і до уваги береться не тільки успішне виконання сьогоднішніх функцій, а й здібності до професійного розвитку й освоєння нових професій і знань. В цільових, планових і оперативних оцінках існуючі методи об'єднують в три групи: якісні, кількісні і комбіновані. До групи якісних методів відносять методи біографічного опису, ділової характеристики, спеціальної усної характеристики, еталону, а також метод обговорення. До групи кількісних методів відносять всі методи з кількісною оцінкою рівня якостей працівника. Комбіновані методи - це метоли експертної оцінки, тестування [7].

Данюк В. М., Петюх В. М., Цимбалюк С. О., за формою вираження кінцевого результату виділяють описові, кількісні та комбіновані методи. При описових методах оцінка подається в текстовій формі, при кількісних і комбінованих використовуються шкали оцінок, які дозволяють кількісно виміряти різні рівні виконання робіт в організації. За інструментами оцінювання розрізняють прогностичний метод, інформаційною базою якого є результат обстежень, інтерв'ю, співбесід; практичний метод, що спирається на оцінку результатів практичної діяльності працівника; імітаційний метод, коли працівник оцінюється за своєю поведінкою в умовах конкретної ситуації (в навчальному процесі – кейс-метод) [8].

Федулова Л.І. вважає, що методи оцінки персоналу необхідно поділяти на методи індивідуальної та методи групової оцінки [9].

Таблиця 1 – Визначення сутності терміну «оцінювання персоналу»

№ п/п	Автор	Визначення
1	2	3
1	Балабанова Л.В.	Оцінювання персоналу – це цілеспрямований процес встановлення відповідності якісних характеристик персоналу (здібностей, властивостей) вимогам посади або робочого місця [1].
2	Головатий М.Ф., Лукашевич М. П., Дмитренко Г. А.	Під оцінюванням персоналу розуміють процедуру, за допомогою якої виявляється ступінь відповідності якостей працівника, його трудової поведінки, результатів діяльності певним вимогам [2].
3	Завіновська Г.Т.	Оцінювання персоналу – це запланована, формалізована характеристика трудової діяльності зайнятих, ефективності роботи персоналу [3].
4	Колот А.М.	Оцінка персоналу полягає у визначенні того, якою мірою кожний працівник досягає очікуваних результатів праці й відповідає тим вимогам, які випливають з його виробничих завдань [4].
5	Савченко В. А.	Оцінювання персоналу є процедура, що здійснюється з метою виявлення ступеня відповідності професійних, ділових та особистих якостей працівника, кількісних і якісних результатів його трудової діяльності визначеним вимогам [5].
6	Скопилатов І.О., Єфремов О.Ю.	Ділова оцінка персоналу - це компонент діагностики персоналу, цілеспрямований процес встановлення відповідності кількісних і якісних професійних характеристик персоналу вимогам посади (робочого місця), підрозділи і організації в цілому [6].

На нашу думку, найпоширенішими на сьогоднішній день є наступні методи оцінки персоналу:

1. Описовий метод оцінки. Оцінювач повинен виявити і описати позитивні і негативні риси поведінки працівника, що атестується. Цей метод не передбачає чіткої фіксації результатів і тому часто використовується як доповнення до інших методів.

2. Метод оцінки нормативом роботи, тобто оцінка працівника здійснюється на основі норми на роботу, яку він виконує, в кількості, якості і часі.

3. Метод порівняльних анкет. Включає набір питань чи описів поведінки працівника. Оцінювач проставляє відмітку навпроти опису тієї риси характеру, яка, на його думку, властива працівникові, в іншому випадку залишає пусте місце. Сума позначок дає загальний рейтинг анкети даного працівника. Використовується для оцінки керівництвом, колегами та підлеглими.

4. Тестування. Для оцінки працівника можуть бути застосовані різні тести. За своїм змістом вони поділяються на три групи: кваліфікаційні, що дозволяють визначити ступінь кваліфікації працівника; психологічні, що дають можливість оцінити особистісні якості працівника; фізіологічні, виявляють фізіологічні особливості людини. Позитивні сторони тестової оцінки в тому, що вона дозволяє отримати кількісну характеристику за більшістю критеріїв оцінки, і можлива комп'ютерна обробка результатів. Однак, оцінюючи потенційні можливості працівника, тести не враховують, як ці здібності проявляються на практиці.

5. Метод алфавітно-числової шкали. Цим методом оцінюється вплив важливих факторів на трудову діяльність персоналу. Ступінь прояву кожного фактору визначається у числовому і мовному вимірі. Найчастіше даним методом вимірюються такі фактори, як цілеспрямованість, відповідальність, ініціативність, уміння працювати в колективі. Основу алфавітно-числової оцінки персоналу складає шкала. Відповідно до неї зіставляються трудові досягнення й особисті якості працівника. У даний час застосовують системи з досить щільною шкалою оцінок з різними рівнями і підрівнями. Метод алфавітно-числової шкали дозволяє глибоко проаналізувати трудову діяльність, проте має деякі недоліки: суб'єктивізм в оцінюванні особистісних якостей працівників, невизначеність змісту та числових значень критеріїв.

6. Найбільш простим і поширеним методом оцінки при прийомі на роботу є інтерв'ю. Суть інтерв'ю - претенденту дається завдання провести співбесіди з декількома кандидатами на робочі місця і самому прийняти рішення. В інтерв'ю важливо отримати інформацію про наступні компоненти і характеристики особистості: інтелектуальна сфера; мотиваційна сфера; темперамент, характер; професійний і життєвий досвід; здоров'я; ставлення до професійної діяльності; професійне навчання; служба в армії; ставлення до роботи на фірмі; захоплення; самооцінка можливостей; сімейний стан, стосунки в сім'ї; форми проведення дозвілля. Інтерв'ю має ряд недоліків: по-перше, на всіх інтерв'ю кандидату доводиться відповідати практично на одні й ті ж питання, проте ясного розуміння ключових характеристик кандидата досягти не вдається; по-друге, на проведення інтерв'ю витрачається дорогоцінний робочий час багатьох співробітників; по-третє, результативність інтерв'ю багато в чому залежить від практичного досвіду інтерв'юера. Так, наприклад, за даними дослідників, які порівнювали ефективність різних методів оцінки, "точність" неструктурованого інтерв'ю дорівнює приблизно 15%.

7. Структуроване поведінкове інтерв'ю є одним з інструментів, який використовується для аналізу компетенцій (комплексу поведінкових характеристик, необхідних працівникові для успішного виконання тієї чи іншої роботи або будь-яких функцій). За даними досліджень, прогностична цінність інтерв'ю за компетенціями вже значно вище – приблизно 63%. Цей вид інтерв'ю може проводитися не тільки для відбору зовнішніх кандидатів, а й при оцінці співробітників-претендентів на вакансії, при формуванні кадрового резерву та підведенні підсумків проведення програми розвитку та навчання. Структура поведінкового інтерв'ю – питання відносяться до минулого релевантного досвіду людини і будуються за принципом "воронки": від загальних питань про професійну ситуації до конкретних прикладів дій, які дозволили досягти заявленого результату. Даний тип інтерв'ю дуже ефективний, але його проведення вимагає навчання і практики. Ще однією перевагою такого інтерв'ювання є можливість кількісної оцінки розвитку тієї чи іншої компетенції.

8. Метод комітетів. Оцінка проводиться групою експертів і націлена на з'ясування здібностей кандидата, що дають йому право претендувати на інші посади, зокрема на висунення на підвищення. Оцінка в узагальненому вигляді укладає наступні чотири дії: вибір оцінюваних якостей, показників діяльності працівника; використання різних методів збору інформації; оціночна інформація повинна давати комплексне уявлення про людину; порівняння реальних якостей співробітника з необхідними. Досліджувані набори якостей розробляються з урахуванням завдань, які виконуються за посадою. Зазвичай таких якостей набирається від 5 до 20.

9. Метод "360 градусів". В рамках програм розвитку співробітників проводиться так звана оцінка за методом "360 градусів". Даний вид оцінки використовується і для поліпшення внутрішньої комунікації, розвитку корпоративної культури. Це погляд на працівника з різних сторін. Інформацію одержують шляхом бесіди з самим співробітником, його безпосереднім керівником, колегами, підлеглими, а в окремих випадках і клієнтами оцінюваного. На основі результатів оцінки надається розгорнута інформація, яка заснована на об'єктивних даних і носить розвиваючий характер. Інформація, отримана співробітниками, дозволяє не тільки оцінити свої сильні сторони і намітити зони розвитку, а

й покращити внутрішню комунікацію в підрозділі. Дані оцінки за методом "360 градусів" стають основою для формування програми індивідуального розвитку співробітника.

10. «Центр оцінки» – це один з методів комплексної оцінки персоналу, заснований на використанні взаємодоповнюючих методик, орієнтований на оцінку реальних якостей співробітників, їх психологічних і професійних особливостей, відповідності вимогам посадових позицій, а також виявлення потенційних можливостей фахівців. «Центр оцінки» (Ассессмент-центр) успішно вирішує наступні задачі: оцінка професійних знань і навичок персоналу; оперативне управління персоналом; навчання персоналу; розвиток навичок оцінки. Компоненти Ассессмент-центрів: інтерв'ю з експертом, в ході якого відбувається збір даних щодо знань та досвіду співробітника; тести (психологічні, професійні, загальні); коротка презентація учасника перед експертами та іншими учасниками; ділова гра; біографічне анкетування; опис професійних досягнень; індивідуальний аналіз конкретних ситуацій (case-study); експертне спостереження. Переваги «Центру оцінки»: ассессмент-центр несе в собі елементи стратегії компанії; «Центр оцінки» дозволяє отримати максимально об'єктивну оцінку в порівнянні з іншими методами; «Центр оцінки» дозволяє найбільш раціонально вкладати гроші в розвиток персоналу; забезпечується розуміння і чіткість в оцінці персоналу всіма співробітниками компанії; сама процедура «Центр оцінки» вже є сходинкою до розвитку персоналу. До недоліків можна віднести: процедура «Центру оцінки» в цілому дорожче, ніж проведення тестування або інтерв'ювання співробітників; для проведення «Центру оцінки» часто потрібно більше часу, ніж на тестування; для «Центру оцінки» потрібна підготовка спостерігачів з числа співробітників компанії, що вимагає певного часу.

11. Метод ділових ігор. Оцінка персоналу здійснюється в рамках спеціально розроблених імітаційних і розвиваючих ділових ігор. До оцінки залучаються як самі учасники ділових ігор, так і експерти-спостерігачі. Атестаційні ділові ігри орієнтовані на результат, що дозволяє оцінити готовність персоналу до вирішення поточних і майбутніх завдань, а також індивідуальний внесок кожного учасника гри. Цей метод оцінки може використовуватися для визначення ефективності командної роботи персоналу.

12. Управління досягненнями (Performance Management) являє собою концепцію управління організацією, що базується на безлічі теорій та практик управління, що передували їй. PM – це інтеграція різних методик управління організацією, що зарекомендували себе як ефективні. До основних принципів системи PM можна віднести наступні:

a) система управління орієнтована на досягнення взаємопов'язаних, взаємозалежних кількісних і якісних цілей;

b) цілі розробляються зверху вниз. В основу цілей підрозділів і персональних цілей окремих працівників покладаються цілі організації;

c) особлива увага приділяється взаємозв'язку цілей бізнесу та розвитку ключових компетенцій співробітника;

d) досягнення цілей співробітниками оцінюється за допомогою показників (Key Performance Indicators – KPI). KPI лежать в основі системи мотивації, тобто досягнення чи недосягнення персональних цілей безпосередньо впливає на матеріальну або нематеріальну винагороду. KPI використовуються не тільки для вимірювання результатів, подання звітності, диференціації досягнень, але також і для аналізу можливостей поліпшення результатів, вдосконалення і розвитку бізнесу.

13. Метод стандартних оцінок. Здійснюється керівництвом. Керівник заповнює спеціальну форму стандартних оцінок, оцінюючи окремі аспекти роботи працівника на протязі атестаційного періоду по стандартній шкалі. Однак метод стандартних оцінок страждає рядом серйозних недоліків. По-перше, атестацію проводить одна людина – керівник, що передбачає високий ступінь суб’єктивності та односторонності оцінки. Хоча він повинен приймати до уваги тільки професійні якості працівників, на оцінці можуть відобразитись особистісні взаємовідносини з підлеглими. По-друге, стандартна шкала не

враховує особливостей професійної діяльності кожного окремого працівника, що може вплинути на якість оцінки.

14. Метод вирішальних ситуацій. Для використання цього методу фахівці з оцінки готують список описів «правильної» і «неправильної» поведінки працівників у типових ситуаціях – «вирішальних ситуаціях». Ці описи розподіляються по рубриках відповідно до характеру роботи. Далі особа, що проводить оцінку, готує журнал для записів по кожному оцінюваному працівнику, в який вносить приклади поведінки по кожній рубриці. Пізніше цей журнал використовується при оцінці ділових якостей співробітника. Зазвичай даний метод використовується в оцінках, що виносяться керівником, а не колегами та підлеглими.

15. Метод заданого розподілу. Відомо, що при оцінці ефективності працівників керівники часто стикаються з труднощами, обумовленими дією помилок оцінювання. Заданий розподіл використовують для того, щоб виключити такі помилки оцінки, як помилка центральної тенденції і помилка поблажливості. Заданий розподіл є формою порівняльної оцінки, при якій керівник відносить підлеглих до певної категорії відповідно до певних (заданих наперед) правил. При цьому виходять з того, що прояв оцінюваних робочих характеристик підпорядковується закону нормального розподілу.

Отже, оцінка персоналу є однією з найважливіших складових системи управління персоналом. Проте, вітчизняній практиці оцінювання персоналу все ще бракує комплексності, систематичності та регулярності у побудові системи оцінювання. До характерних ознак чинних на підприємствах систем оцінки персоналу слід віднести орієнтацію на спрощені процедури оцінки, брак конструктивного зворотного зв’язку між об’єктом і суб’єктами оцінювання. Тому для підвищення ефективності оцінювання персоналу необхідно: поширення сучасних методів оцінки на всі категорії персоналу; розширення доступу персоналу до результатів його оцінки; активне включення персоналу в процес його оцінки через залучення до самоаналізу діяльності і розробки заходів з поліпшення роботи; розширення кола оцінювачів, у ролі яких, крім безпосереднього керівника, повинні виступати колеги по роботі, підлеглі, споживачі та клієнти.

Список літератури

1. Балабанова Л.В. Управління персоналом: Навч. посібник / Л.В. Балабанова, О.В. Сардак. – К.: Професіонал, 2006. – 512 с.
2. Головатий М. Ф. Управлінські аспекти соціальної роботи. Курс лекцій / М. Ф. Головатий, М. П. Лукашевич, Г. А. Дмитренко та ін. – К.: МАУП, 2004. – 368 с.
3. Завіновська Г. Т. Економіка праці: навч. посіб. / Г. Т. Завіновська. – К.: КНЕУ, 2003. – 432 с.
4. Колот А.М. Мотивація персоналу: Підручник. / А.М. Колот – К.: КНЕУ, 2002. – 337 с.
5. Савченко В. А. Управління розвитком персоналу: навч. посіб. / В. А. Савченко. – Київ : КНЕУ,2002. – 351 с.
6. Скопылатов И.А. Управление персоналом / И.А. Скопылатов, О.Ю. Ефремов. – СПб.: Изд-во Смольного университета, 2000. – 400 с.
7. Крушельницька О.В., Мельничук Д.П. Управління персоналом. К.: Кондор, 2003. – 296с.
8. Данюк В. М. Менеджмент персоналу: Навч. посіб. / В. М. Данюк, В. М. Петюх, С. О. Цимбалюк та ін.; За заг. ред. В. М. Данюка, В. М. Петюха. – К.: КНЕУ, 2004. – 398 с.
9. Федулова Л. І. Менеджмент організацій: Підручник/ Л. І. Федулова, І. В. Сокирник, В. В. Стадник, М. А. Йохна, О.С. Новикова, Є. Г. Рясних. – К.: Либідь, 2004. – 448 с.

УДК

К. Скачков, магістр гр. МЕ-18М-1,4
Центральноукраїнський національний технічний університет

ОСОБЛИВОСТІ СТРАТЕГІЧНОГО УПРАВЛІННЯ РОЗВИТКОМ СІЛЬСЬКОГОСПОДАРСЬКИХ ПІДПРИЄМСТВ

В ринкових умовах господарювання механізм стратегічного управління аграрними формуваннями перебуває на етапі становлення та постійного вдосконалення. Нестабільність зовнішнього середовища підприємств сприяє появі нових методів, систем і підходів до управління. На сьогодні більшість вітчизняних аграрних підприємств працюють у середовищі, що швидко змінюється та важко передбачається, саме тому гостро стоїть потреба використання у практичній діяльності методів стратегічного управління.

Стратегічне управління є вагомим інструментом забезпечення довгострокового розвитку сільськогосподарських підприємств. Практичне застосування стратегічного управління має на меті забезпечення результативності діяльності підприємства і формування його нових конкурентних переваг, що передбачає обґрунтування ефективної стратегії їх розвитку.

Разом з тим особливості сільськогосподарського виробництва, відсутність адаптованих методик оцінки типів їх розвитку призводять до його практичного застосування лише незначною кількістю підприємств, останні ж надають перевагу ситуаційному управлінню, яке дає можливості забезпечити утримання ринкової позиції тільки в коротко- та середньостроковій перспективі.

Дослідженню теоретичних основ та особливостей стратегічного управління підприємств присвячено значну кількість робіт зарубіжних і вітчизняних учених-економістів, серед яких варто відзначити наукові праці І. Ансофф, Дж. Еванса, Ф. Котлера, Л. Балабанової, П. Діксона, А. Загороднього, В. Мікловди, С. Свірідової, В. Харченко, М. Юданова та інших. Проблемам реалізації стратегії сільськогосподарської продукції, моделювання розвитку, приділяється велика увага у роботах О. Панухника, В. Россохи, І. Чукіної, Н. Ястремської та ін. Незважаючи на значний науковий доробок, дана тематика не втрачає своєї актуальності, адже кожне сільськогосподарське підприємство має свої специфічні особливості господарювання.

Термін “стратегічне управління” введено у вжиток на межі 60-70-х років XX ст. для підкреслення різниці між поточним управлінням на рівні виробництва (торговельно-технологічного процесу) і керівництвом, що здійснюється на вищому рівні управління фірмою.

Стратегічне управління – різновид діяльності, який спирається на людський потенціал як основу організації, орієнтує виробничу діяльність на запити споживачів, гнучко реагує і проводить своєчасні зміни в організації, що відповідають виклику з боку оточення і дозволяють добиватися конкурентних переваг, що в сукупності дає можливість організації виживати в довгостроковій перспективі, досягаючи при цьому своїх цілей [1].

Варто зазначити, що термін “стратегічне управління” і “стратегічний менеджмент” досить часто використовуються як синоніми, хоча деякі науковці вважають, що ці поняття не повністю ідентичні. Остання точка зору здається більш аргументованою, оскільки смислова різниця термінів управління та менеджмент пов’язана з їх структурною основою [2].

Кожен напрям стратегічного управління відрізняється від стратегічного менеджменту механізмами впровадження і реалізацією на практиці. Але для успішного розвитку підприємства необхідно розглядати їх у єдності. Найбільш всеохоплюючим є системний підхід до стратегічного управління як до набору взаємозалежних елементів, спрямованих на реалізацію мети, завдань підприємства шляхом виконання функцій планування, аналізу, комунікації, мотивації, контролю, оцінки, ухвалення управлінських рішень, в контексті сформованої загальної концепції розвитку

підприємства. При цьому результативність стратегічного управління забезпечується дотриманням процесу його здійснення, який включає декілька взаємопов'язаних етапів, зокрема: розроблення місії підприємства; визначення цілей організації; оцінка й аналіз зовнішнього середовища; визначення сильних та слабких сторін; аналіз стратегічних альтернатив; вибір стратегії; реалізація стратегії; оцінка стратегії [3].

Мета стратегічного управління – визначення місії, цілей та стратегій, розробка і забезпечення виконання системи планів як інструментів реалізації стратегічних орієнтирів з удосконалення підприємства .

Об'єктами стратегічного управління є організації, стратегічні господарські підрозділи і функціональні зони організації.

Предметом стратегічного управління є:

- проблеми, які прямо пов'язані з генеральними цілями організації;
- проблеми і рішення, пов'язані з яким–небудь елементом організації, якщо цей елемент необхідний для досягнення цілей, але в даний час відсутній або є присутнім в недостатньому об'ємі;
- проблеми, пов'язані із зовнішніми чинниками, які неможливо контролювати.

При цьому стратегічне управління будується на єдності наступних підходів:

- цілеспрямованості − стратегічне управління має бути спрямоване на досягнення стратегічних цілей;
- системності – елементи середовища і потенціалу підприємства оцінюються і управляються комплексно, у взаємозв'язку і взаємообумовленості;
- ситуативності – систематично відслідковується зміни середовища і проводиться адекватне коригування стратегічних планів і рішень залежно від динамічних змін ситуації;
- інтегральності – об'єднання зусиль, можливостей і сильних сторін на подолання загроз і слабкостей потенціалу та на досягнення в кінцевому підсумку стратегічних цілей діяльності;
- інноваційності – лише систематичне впровадження досягнення науково-технічного прогресу забезпечить високу конкурентостійкість підприємства і успішне досягнення ним стратегічних цілей;
- когнітивності – як передумова стратегічних змін.

Відповідно до змісту стратегічного управління виокремлено процеси безпосередньої розробки стратегії, стратегічного планування й стратегічного управління в цілому та диференційовано сукупність функцій стратегічного управління на такі групи:

- функції управління процесом визначення цільових орієнтирів;
- функції управління процесом розробки стратегій;
- функції управління процесом реалізації стратегій.

Впровадження стратегічного управління забезпечує незаперечні переваги:

- можливість піднятися над турбулентністю середовища, чітко бачити і забезпечувати досягнення стратегічних цілей;
- гнучкість управління, зведення до мінімуму негативних наслідків швидких змін і невизначеності середовища;
- зміцнення і розширення конкурентних переваг, забезпечення високої конкурентостійкості підприємства;
- забезпечення майбутньої прибутковості та інших стратегічних цілей;
- суттєве зниження ймовірності банкрутства.

Найбільший внесок у розробку теорії стратегічного управління зроблено науковцем І. Ансофф (1965 р.), який виділяв два види управління: стратегічний і оперативний. Діяльність зі стратегічного управління пов'язана з постановкою цілей і завдань організації, підтримкою продуктивних взаємин між організацією та її бізнес–середовищем, що дозволяють їй досягти своїх цілей, відповідають її внутрішнім можливостям і дозволяють залишатися сприйнятливою до зовнішніх викликів [4]. Виділення та відокремлення складових стратегічного та оперативного

управління, на нашу думку, дозволило змінити підходи до цих видів управління залежно від орієнтації на короткострокову перспективу чи довгостроковий горизонт управління.

Стратегічне і оперативне управління є режимами, наявними всередині керуючої підсистеми, які використовуються одночасно. Стратегічне управління дозволяє забезпечити діяльність організації в майбутньому, при зміні зовнішніх і внутрішніх факторів впливу, в той час як оперативне управління використовує розроблену раніше стратегію з метою досягнення поточних цілей організації.

Істотною відмінністю стратегічного управління, від оперативного, є його гнучкість, відсутність суворої структурованості. Оперативне управління є суворо регламентованим, більш стійким до змін. Дана обставина впливає і на тип організаційної поведінки управлінської структури. Для стратегічного управління є характерним підприємницький тип управління, а оперативне управління може бути успішно реалізовано за рахунок правильності прийняття управлінських рішень.

Стратегічне управління можна визначити як організаційно-економічний процес, який включає всебічний економічний аналіз внутрішнього і зовнішнього середовища аграрного підприємства, на основі якого формуються мета діяльності суб'єкта господарювання, яка б забезпечила конкурентоспроможність як підприємства, так і його продукції на внутрішньому і зовнішньому ринках, прибутковість виробничої діяльності та економічний розвиток.

Таким чином, передумовою впровадження стратегічного управління є доцільність розширення горизонту уваги вищого менеджменту на проблеми зовнішнього середовища підприємства, з відповідною реакцією на зміни, які відбуваються в ньому. Отже, можна зробити висновок про значні переваги стратегічного управління в порівнянні з оперативним [5].

Концепція стратегічного управління лежить в основі стратегічного мислення і знаходить вираз у наступних характерних рисах її застосування:

1. Базується на певному поєднанні теорії: системному, ситуаційному та цільовому підходах до діяльності підприємства, що трактується як відкрита соціально-економічна система. Використання тільки однієї із зазначених засад не дає можливості досягти потрібних результатів – розвитку підприємства у довгостроковій перспективі.

2. Орієнтує на вивчення умов, в яких функціонує підприємство. Це дозволяє створювати адекватні цим умовам системи стратегічного управління, що будуть відрізнятись одна від одної залежно від особливостей підприємства та характеристик зовнішнього середовища.

3. Концентрує увагу на необхідності збору та застосування баз стратегічної інформації. Аналіз, інтерпретація та застосування інформації для прийняття стратегічних рішень дає змогу визначити зміст та послідовність дій щодо змін на підприємстві завдяки зменшенню невизначеності ситуації.

4. Дозволяє прогнозувати наслідки рішень, що приймаються, впливаючи на ситуацію шляхом відповідного розподілу ресурсів, встановлення ефективних зв'язків та формування стратегічної поведінки персоналу.

5. Передбачає застосування певних інструментів та методів розвитку підприємств (цілей, "дерева цілей", стратегій, "стратегічного набору", стратегічних планів і програм, стратегічного планування та контролю тощо) [6].

Реалізація концепції стратегічного управління організацією можлива лише тоді, коли організація є стратегічно орієнтованою. Стратегічно орієнтована організація це така організація, в якій персонал має стратегічне мислення, застосовується система стратегічного планування, що дає змогу розробляти та використовувати інтегровану систему стратегічних планів, і здійснюється поточна, повсякденна діяльність, підпорядкована досягненню поставлених стратегічних цілей. Доцільно виділити основні положення стратегічного управління:

1. Стратегічне управління дає чітке уявлення про стратегічний потенціал розвитку підприємства, його майбутнє положення і можливість існування в конкурентному середовищі в довгостроковому період

2. Система стратегічного управління – своєрідна філософія існування підприємства, політика ведення бізнесу, що базується на розробці стратегії розвитку на засадах системного і

підприємницького підходів, високому професіоналізмі менеджерів із залученням всього персоналу до прийняття й реалізації стратегічних рішень.

3. Функціонування системи стратегічного управління вимагає створення відповідного підрозділу, функції якого пов'язані з постійними дослідженнями зовнішнього середовища, розробкою і реалізацією стратегічних планів розвитку підприємства [7].

Стратегічне управління дозволяє досягти наступних основних результатів:

– створити системний потенціал досягнення цілей організації. Цей потенціал складається з фінансових, сировинних і людських ресурсів організації; виробленої продукції (послуг), що затребуються ринком; сформованого позитивного іміджу організації;

– структури організації та її внутрішніх змін, що забезпечують чутливість до змін зовнішнього середовища і відповідну адаптацію.

Список літератури

1. Бєлявцев М.І. Стратегічне маркетингове управління збутом підприємств [Електронний ресурс] / М.І. Бєлявцев, М.М. Беспята //Маркетинг в Україні. 2010. – № 1. – С. 24-26. – Режим доступу: http:// nbuv.gov.ua/UJRN/Mvu_2010_1_7.
2. Ястремська О.М., Верещагіна Г.В. Стратегічне управління інноваційним розвитком підприємства. Харків: ВД "ІНЖЕК", 2010. – 392 с.
3. Кашуба Я.М. Вибір методів та підходів стратегічного управління розвитком підприємництва / Я.М. Кашуба // Економіка та держава. – 2011. – №9. – С. 16-24.
4. Ansoff I. Implanting Strategy Management / I. Ansoff, E. McDonnell. – 2nd ed. – New York: Prentice-Hall, 1990. – 544 p.
5. Чикуркова А.Д. Сутність та ключові характеристики стратегічного управління на підприємствах. Інноваційні засади сталого розвитку національного господарства: Міжнародна науково-практична конференція. м. Кам'янець-Подільський, 21-22 листопада 2014 року. Кам'янець-Подільський: Видавничий дім "Гальветика", 2014. Ч. 1. С. 211-214.
6. Алєксєєва Н.І. Класифікація базових стратегій зростання підприємства [Електронний ресурс] / Н.І. Алєксєєва // Вісник Східноєвропейського університету економіки і менеджменту. Серія: Економіка і менеджмент / Східноєвроп. ун-т економіки і менеджменту. – Черкаси, 2012. – № 3. – С. 71-80. – Режим доступу: http://nbuv.gov.ua/UJRN/Vsuem_2012_3_12.
7. Мікловда В.П. Ефективність стратегічного управління підприємствами : сучасні проблеми та перспективи їх вирішення. Держ. вищ. навч. закл. "Ужгород. нац. ун-т", Вищ. навч. закл. Укоопспілки "Полтав. ун-т економіки і торгівлі". Полтава: ПУЕТ, 2013. – 231 с.

УДК 657

А. Ткаченко, магістр гр. ООУ-18МЗ-1,4
Центральноукраїнський національний технічний університет

ПІДХОДИ ДО КЛАСИФІКАЦІЇ ЗАПАСІВ СІЛЬСЬКОГОСПОДАРСЬКИХ ПІДПРИЄМСТВ

Стаття присвячена дослідженню підходів сучасних фахівців до групування такої важливої категорії обліку, як запаси. Обґрунтована необхідність класифікації запасів сільськогосподарських підприємств за різними напрямками залежно від мети розгляду запасів. З метою організації та ведення обліку запасів сільськогосподарських підприємств запропоновано використовувати економічну та технічну ознаки класифікації. Наведено пропоновану класифікацію запасів з метою управління запасами сільськогосподарських підприємств

сільськогосподарське підприємство, запаси, класифікація, ознаки класифікації, економічна класифікація, технічна класифікація, класифікація з метою управління

Статья посвящена исследованию подходов современных специалистов к группировке такой важной категории учета, как запасы. Обоснована необходимость классификации запасов сельскохозяйственных

предприятий по разным направлениям в зависимости от цели рассмотрения запасов. С целью организации и ведения учета запасов сельскохозяйственных предприятий предложено использовать экономический и технический признаки классификации. Приведена предлагаемая классификация запасов с целью управления запасами сельскохозяйственных предприятий

сельскохозяйственное предприятие, запасы, классификация, признаки классификации, экономическая классификация, техническая классификация, классификация с целью управления

Постановка проблеми. Запаси є важливою обліково-економічною категорією та об'єктом бухгалтерського обліку, займають вагоме місце в оборотних активах та беруть участь у формуванні кінцевого продукту діяльності підприємства й входять до вартості його власного капіталу. Основною умовою здійснення господарської діяльності сільськогосподарських підприємств є достатній обсяг та раціональне використання виробничих запасів, за рахунок яких вони функціонують, забезпечуючи подальший розвиток суспільних економічних відносин.

Враховуючи високий ступінь конкуренції, постійні зміни взаємовідносин між виробниками, постачальниками, покупцями й державою, зростання ризику й відповідальності суб'єктів господарювання за результати діяльності, однією з основних умов отримання прибутку сільськогосподарськими підприємствами є якість управління виробничими запасами, що здійснюється на підставі оперативної та достовірної інформації, основним джерелом формування якої є система бухгалтерського обліку.

Постійні зміни чинного законодавства України, умов використання капіталу, зростаючі вимоги користувачів інформації, трансформація вітчизняного бухгалтерського обліку відповідно до вимог міжнародних стандартів зумовлюють об'єктивну необхідність поглиблення дослідження питань обліку виробничих запасів у сільськогосподарських підприємствах, взагалі, та такої його важливої складової, як класифікація, зокрема.

Аналіз останніх досліджень і публікацій. Проблеми організації та методології бухгалтерського обліку виробничих запасів досліджували вітчизняні вчені Н. Борщ, Т.А. Бутинець, Ф.Ф. Бутинець, І. Буфатіна, С.В. Голов, Н.М. Грабова, С.І. Дерев'янко, Т.М. Джинжиристий, В.П. Завгородній, Г.Г. Кірейцев, О.В. Мурашко, М.Ф. Огійчук, А.В. Озеран, В.О. Озеран, П.Т. Саблук, В.В. Сопко, Л.К. Сук, П.Л. Сук, Н.М. Ткаченко, С.М. Хмелевський, Л.В. Чижевська, Л.С. Шатковська, В.М. Шваб. Вагомий внесок у дослідження даної проблеми зробили іноземні вчені: С.В. Абрамов, Р.Н. Антоні, С.А. Вирабов, П.А. Костюк, О.А. Кролі, А.Ш. Маргуліс, Б. Нідлз та інші.

Однак, на сучасному етапі розвитку сільськогосподарських підприємств особливої уваги потребує вивчення питань організації та ведення обліку запасів, кваліфікованого підходу до вирішення організаційно-методичних питань щодо їх класифікації та можливості широкого використання при цьому інформаційно-комп'ютерних технологій, що підвищуватиме якість отриманої обліково-аналітичної інформації.

Постановка завдання. Мета написання статті полягає у долслідженні існуючих підходів до класифікації запасів сільськогосподарських підприємств з метою обгрунтування доцільного підходу до їх групування в межах бухгалтермького обліку.

Виклад основного матеріалу. Оскільки склад запасів сільськогосподарських підприємств досить різноманітний, то основою для побудови їх бухгалтерського обліку є класифікація, яка виступає об'єктом гострих наукових дискусій.

Класифікація запасів забезпечує виконання основних завдань обліку та контролю запасів, серед яких:

- раціональне визначення одиниці обліку запасів та формування номенклатури-цінника;
- організація складського господарства;
- правильне та своєчасне документальне оформлення всіх операцій з руху матеріальних цінностей;
- достовірне визначення первісної вартості запасів;
- визначення умов переоцінки запасів на дату балансу та методів їх оцінки вразі

вибуття;

- контроль за надходженням, заготівлею матеріальних цінностей, їх зберіганням;
- розкриття інформації про запаси у примітках до фінансової звітності.

Усі перераховані завдання сприяють формуванню інформації для управління запасами.

Існують різні точки зору щодо класифікаційних ознак. І.А. Карабаза [3] поділяє запаси на ті, які частково опосередковані діяльністю людини і ті, які повністю опосередковані. Л. Марущак [5] акцентує увагу на основних та допоміжних матеріалах, Л. В. Юрчишена [8] згадує про такі класифікаційні ознаки товарних запасів, як регулярність поповнення, за якою існує поділ на запаси регулярного поповнення і нерегулярного поповнення, залежно від відповідності попиту існують ходові та неходові запаси, залежно від чутливості до зміни товарообороту, від моменту та характеру оцінки - початкові, вихідні, середні та планові (прогнозні) товарні запаси. І.Б. Садовська [7] розглядає виробничі запаси за класифікаційними ознаками, які наведені в табл. 1.

Таблиця 1 - Класифікація виробничих запасів

№ п/п	Класифікаційні групи запасів	Вид запасів	Характеристика
1.	За призначенням і причинами утворення	Постійні	Частина виробничих запасів, що забезпечують безперервність виробничого процесу між двома черговими поставками
		Сезонні	Виробничі запаси, що утворяться при сезонному виробництві продукції чи під час сезонного транспортування
2.	За місцем знаходження	Складські	Виробничі запаси, що знаходяться на складах підприємства
		У виробництві	Що знаходяться у процесі обробки
3.	За рівнем наявності на підприємстві	Нормативні	Виробничі записи, що відповідають запланованим обсягам виробничих запасів, необхідних для забезпечення безперебійної роботи підприємства
		Понаднормові	Що перевищують їх нормативну кількість
4.	Відносно до балансу	Балансові	Запаси, що є власністю підприємства і відображаються в балансі.
		Позабалансові	Запаси, що не належать підприємству, і знаходяться у нього через певні обставини.
5.	За походженням	Первинні	Запаси, що надійшли на підприємство від інших підприємств і не підлягають обробці
		Вторинні	Матеріали та вироби, що можуть застосовуватися вдруге у виробництві
6.	За складом і структурою	Виробничі запаси	Запаси сировини, основних і допоміжних матеріалів, напівфабрикатів власного виробництва, купівельних напівфабрикатів, комплектуючих виробів, палива, запчастин, тари і тарних матеріалів, МШП
		Запаси НЗВ	Частина продукції, що не пройшла всіх стадій обробки та не прийнята ВТК
		Запаси готової продукції	продукція, виробництво якої завершене, що прийнята ВТК і знаходиться на складі
		Товарні запаси	Товари, що знаходяться, у сфері обігу, а також продукція, що знаходиться в дорозі

Деякі автори пропонують для обліку виробничих запасів вводити нові рахунки у План рахунків бухгалтерського обліку. Так, М. В. Калита, Л. Е. Рогозян [2, с.57] пропонують витрати на придбання і утримання запасів поділити на три категорії: витрати на підготовку замовлення, витрати на утримання запасів, витрати, пов'язані з нестачею (дефіцитів) запасів та використовувати рахунок 29: 291 "Витрати на підготовку замовлення", 292 "Витрати на утримання запасів", 293 "Витрати, пов'язані з нестачею (дефіцитом) запасів". Г. Довгань [1, с.88] рахунок 29 пропонує використовувати для обліку торгових націнок.

Доцільним є ведення синтетичного та аналітичного обліку виробничих запасів по рахунках, які вже існують, використовуючи їх поділ на субрахунки та аналітичні рахунки. В Методичних рекомендаціях з бухгалтерського обліку запасів, затверджених Міністерством фінансів України від 10.03.2007 №2 [4] вказано, що аналітичний облік запасів ведеться у розрізі місць зберігання, матеріально-відповідальних осіб та видів запасів, синтетичний облік наявності та руху запасів здійснюється в грошовій одиниці України на рахунках обліку запасів за Планом рахунків бухгалтерського обліку активів, капіталу, зобов'язань і господарських операцій підприємств і організацій та Інструкцією про його застосування, затвердженого наказом Міністерства фінансів України від 30.11.99 № 291.

Погоджуємось із думкою, яку висловлює О.М. Приймачок [6, с.174], пропонуючи ввести додаткові субрахунки виробничих запасів, а саме, до субрахунку 203 «Паливо». 20301 - Паливо на паливно-технологічні потреби, паливо для опалення печей, котлів, освітлення приміщень, 20302 - Паливо на енергетичні потреби, 20303 - Паливо на господарські потреби. Автором виділено окремий субрахунок 201.01 "Основна сировина", 201.02 "Додаткова сировина" (для обліку сировини), 201.03 "Допоміжні матеріали", 201.04 "Зворотні відходи".

Деталізація окремих субрахунків з обліку виробничих запасів сільськогосподарських підприємств спрощує отримання бухгалтерської інформації внутрішніми користувачами. Аналіз класифікаційних груп виробничих запасів показує, що основними є економічна та технічна класифікації. О.В. Мурашко [5] зазначає, що облік матеріальних запасів може ґрунтуватись лише на економічній (синтетичний облік) та технічній класифікації (аналітичний облік). Інші ж класифікаційні ознаки є не суттєвими до побудови ефективного обліку, оскільки їх елементи є занадто загальними.

Економічна та технічна класифікації конкретизують деталізацію виробничих запасів. При цьому, передбачений шестизначний код побудований за десятинною системою. Перші три цифри – код субрахунку, четверта цифра – код субрахунку другого порядку (відповідає економічній класифікації) (табл. 2), п'ята й шоста цифри – код аналітичного обліку, який є індивідуальним для кожного підприємства за наявними найменуваннями виробничих запасів (відповідає технічній класифікації).

Таблиця 2 - Деталізований перелік рахунків для бухгалтерського обліку виробничих запасів, який відповідає економічній класифікації

За субрахунками	За субрахунками другого порядку	За субрахунками	За субрахунками другого порядку
201 "Сировина і матеріали"	2011 "Основні матеріали"	206 "Матеріали, передані в переробку"	2061 "Матеріали передані"
	2012 "Допоміжні матеріали"	207 "Запасні частини"	2071 "Запчастини до тракторів"
	2013 "Сировина"		2072 "Запчастини до автомобілів"
202 "Купівельні напівфабрикати"	2021"Напівфабрикати"		2073 "Запчастини до комбайнів"
	2022 "Конструкції та вироби"		2074 "Запчастини до сільськогосподарських

			машин”
203 “Паливо”	2031“Технологічне паливо»		2075 “Інші запчастини”
	2032 “Господарське паливо”		2076 “ОФ деталей, вузлів, агрегатів”
	2033 “Моторне паливо”	208 “Матеріали сільськогоспо-дарського призначення”	2081 “Мінеральні добрива”
204 “Тара та тарні матеріали”	2041 “Тара з дерева”		2082 “Засоби захисту рослин”
	2042 “Тара з картону”		2083 “Біопрепарати”
	2043 “Тара з металу”		2084 “Медикаменти і хімікати”
	2044 “Тара для виготовлення та ремонту тари”		2085 “Насіння»
	2045 “Тара з пластмаси”		2086 “Матеріали переробки біологічних активів (корми) ”
205 “Будівельні матеріали”	2051 “Силікатні матеріали”	209 “Інші матеріали”	2091 “Матеріали від ліквідації основних засобів”
	2052 “Лісові матеріали”		
	2053 “Будівельний метал”		
	2054 “Металовироби”		2092 “Бланки суворого обліку”
	2055 “Санітарно-технічні матеріали”		
	2056 “Електротехнічні матеріали”		2093 “Відходи виробництва”
	2057 “Хімічні матеріали”		

Оскільки класифікація є вихідним моментом побудови обліку, то класифікація виробничих запасів для автоматизації і ефективного ведення синтетичного та аналітичного обліку буде мати вигляд, що представлений у табл. 3.

Таблиця 3 - Класифікація виробничих запасів

За субрахунками	Економічна класифікація	Технічна класифікація (аналітичний облік)
201 «Сировина і матеріали»	2011 «Основні матеріали»	201101 «Борошно» 201102 «Цукор» 201301 «Бавовна» 201302 «Молоко»
	2012 «Допоміжні матеріали»	
	2013 «Сировина»	
202 «Купівельні напівфабрикати»	2021«Напівфабрикати»	202101 «Зерно»
	2022 «Конструкції та вироби»	
203 «Паливо»	2031«Технологічне паливо»	203101 «Газ» 203102 «Керосин» 203201 «Бензин» 203202 «Автол» 203301 «Торф» 203302 «Вугілля»
	2032 «Господарське паливо»	
	2033 «Моторне паливо»	
204 «Тара та тарні матеріали»	2041 «Тара з дерева»	204101 «Ящики» 20402 «Кошики» 204201 «Коробки» 204301 «Бочки» 204302 «Бідони» 204401 «Бочкова клепка» 204402 «Фольга» 204501 «Пластмасові коробки»
	2042 «Тара з картону»	
	2043 «Тара з металу»	
	2044 «Тара для виготовлення та ремонту тари»	

	2045 «Тара з пластмаси»	
205 «Будівельні матеріали»	2051 «Силікатні матеріали»	205101 «Цегла» 205102 «Цемент» 205103 «Вапно» 205201 «Дошки» 205202 «Фанера» 205301 «Залізо листове» 205302 «Бляха» 205303 «Сталь» 205401 «Цвяхи» 205402 «Гайки» 205403 «Болти» 205501 «Крани» 205502 «Муфти» 205601 «Провід» 205701 «Фарба» 205702 «Оліфа» 205703 «Азбест»
	2052 «Лісові матеріали»	
	2053 «Будівельний метал»	
	2054 «Металовироби»	
	2055 «Санітарно-технічні матеріали»	
	2056 «Електротехнічні матеріали»	
	2057 «Хімічні матеріали»	
206 «Матеріали, передані в переробку»	2061 «Матеріали передані»	Матеріали передані за видами
207 «Запасні частини»	2071 «Запчастини до тракторів»	207101 «Лампи» 207201 «Акумулятори» 207301 «Підшипники» 207401 «Гайки» 207402 «Болти»
	2072 «Запчастини до автомобілів»	
	2073 «Запчастини до комбайнів»	
	2074 «Запчастини до с.г. машин»	
	2075 «Інші запчастини»	
	2076 «ОФ деталей, вузлів, агрегатів»	
208 «Матеріали сільськогосподарського призначення»	2081 «Мінеральні добрива»	208101 «Аміачна селітра» 208102 «Суперфосфат» 208401«Спирт» 208402«Пеніцилін» 208501 «Насіння пшениці» 208502 «Насіння вівса» 208503 «Насіння жита» 208601 «Силос» 208602 «Сінаж»
	2082 «Засоби захисту рослин»	
	2083 «Біопрепарати»	
	2084 «Медикаменти і хімікати»	
	2085 Біологічні активи «Саджанці і насіння»	
	2086 Біологічні активи «Корми»	
209 «Інші матеріали»	2091 «Матеріали від ліквідації о.з.»	209101 «Металобрухт» 209102 «Запчастини від ліквідації основних засобів»
	2092 «Бланки суворого обліку»	
	2093 «Відходи виробництва»	

Передбачений шестизначний код побудований за десятинною системою. Перші три цифри – код субрахунку, четверта цифра – код субрахунку другого порядку (відповідає економічній класифікації), п’ята й шоста цифри – код аналітичного обліку, який є індивідуальним для кожного підприємства за наявними найменуваннями виробничих запасів (відповідає технічній класифікації).

Висновки та перспективи подальших досліджень. Отже, систематизація й порівняльний аналіз поглядів вітчизняних та іноземних науковців на класифікацію виробничих запасів показали розмаїття існуючих групувальних ознак, що не сприяє їх практичному втіленню. З урахуванням обґрунтованої сутності виробничих запасів та необхідності побудови їх ефективного відображення в бухгалтерському обліку сільськогосподарських підприємств встановлено необхідність використання економічної та технічної класифікацій виробничих запасів, які знайшли своє відображення в деталізації бухгалтерських рахунків шляхом включення до їх складу субрахунків другого порядку та аналітичних рахунків виробничих запасів, що сприятиме гармонійній взаємоув’язці їх фінансового та управлінського обліку в сільськогосподарських підприємствах.

Список літератури

1. Довгань Г. Шляхи удосконалення обліку реалізації товарних запасів : [Текст] / Г. Довгань // Матеріали V Міжнародної науково-теоретичної конференції студентів, аспірантів і молодих вчених ["Соціально-

економічні, політичні та культурні оцінки і прогнози на рубежі двох тисячоліть"], (Тернопіль, 17 квітня 2007 р.) / ПВНЗ Інститут ек-ки і підпр-ва. – Тернопіль: ПВНЗ ІЕП, 2007. – С. 87-89.
2. Калита М.В., Рогозян Л.Є. Удосконалення обліку витрат на придбання та зберігання виробничих запасів : матеріали II Міжнародної науково-практичної конференції ["Наука без границ - 2005"], (Прага, 19-27 грудня 2005 р.) / Прага : Наука и образование, 2005. – С. 55.
3. Карабаза І.А. Економічна природа виробничих запасів гірничозбагачувальних підприємств: матеріали VII Міжнародної науково-практичної конференції ["Наука і освіта 2004. Бухгалтерський облік і аудит"], (Дніпропетровськ, 10-25 лютого 2004 р.) / Дніпропетровськ : Наука і освіта, 2004. – С. 35.
4. Методичні рекомендації з бухгалтерського обліку запасів, затверджені наказом Міністерства фінансів України від 10 січня 2007 року №2. Спосіб доступу : //http. www.liga.net.
5. Мурашко О.В. Сутність матеріальних запасів, їх класифікація та визначення у бухгалтерському обліку / О.В. Мурашко // Вісник Житомирського державного технологічного уні-верситету. Економічні науки. – Житомир : Житомир. держ. технолог. ун-т, 2005. – № 3(33). –С.134.
6. Приймачок О. М. Особливості класифікації виробничих запасів в хлібопекарському виробництві / О. М. Притймачок // Збірник наукових праць Черкаського державного технологі-чного університету. – Черкаси : Черкаськ. держ. технол. ун-т, 2004. – С. 172.
7. Світлична В.Ю. Актуальні проблеми організації і ведення обліку виробничих запасів підприємствами України [Електронний ресурс] / В.Ю. Світлична. — Режим доступу: http://www.economy confer.com.ua/full_ article/716
8. Юрчишена Л.В. Економічна природа товарних запасів та їх класифікація / Л. В. Юрчишена // Вісник Хмельницького національного університету. – Хмельницький : Хмельниц. нац. ун-т, 2005. – С. 181.

УДК 336:658.1

С. Фірюбіна, магістр гр. УФЕБ-18МЗ
Центральноукраїнський національний технічний університет

ТЕОРЕТИЧНІ ОСНОВИ ФОРМУВАННЯ СИСТЕМИ ЗАБЕЗПЕЧЕННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА В СУЧАСНИХ УМОВАХ

В статті розглянуті питання формування системи економічної безпеки підприємства з урахуванням сучасного етапу розвитку української економіки. Відзначено, що особливої актуальності у сучасному світі набуває інформаційна безпека як важлива складова економічної безпеки підприємства в умовах формування цифрової економіки. Визначено необхідність внесення змін до існуючої системи економічної безпеки в умовах формування цифрової економіки.
економічна безпека, підприємство, цифрова економіка, цифрові технології, інформаційна безпека

Постановка проблеми. У сучасному світі успішне функціонування і економічний розвиток підприємств багато в чому залежить від ефективності їх діяльності в галузі забезпечення економічної безпеки. До факторів, що ускладнюють забезпечення економічної безпеки вітчизняних підприємств, відносять нестабільність економічної та політичної ситуації, недосконаліть законодавчої бази, неефективне управління. Разом з тим нинішнє кризове становище значної частини підприємств, велика частина яких декларують збитковість діяльності, значною мірою зумовлено не лише соціально-економічним становищем у країні та несформованістю ринкових відносин, але й недостатнім рівнем розробки теоретико-методичних основ забезпечення економічної безпеки підприємств в сучасних умовах цифрової трансформації економіки України. Тому дослідження питання сучасних проблем діяльності вітчизняних підприємств, пов’язаних зі зниженням рівня їх економічної безпеки в умовах цифровізації економіки нашої країни є актуальними з теоретичної і практичної точки зору.

Аналіз останніх досліджень і публікацій. Питання теоретичного та практичного характеру забезпечення економічної безпеки суб’єктів господарювання досліджують у своїх

працях Л. Донець, З. Варналій, Т. Іванюта, А. Козаченко, В. Геєць, М. Кизим, Т. Клебанова, О. Черняк та ін. Разом з тим ще не вирішені питання методичного забезпечення управління економічною безпекою підприємств в якості основи для розробки й прийняття управлінських рішень із захисту економічних інтересів підприємств та своєчасного запобігання економічним загрозам. Система економічної безпеки підприємства в сучасних умовах цифрової трансформації економіки має врахувати підходи до організації кібербезпеки та інших аспектів, пов'язаних із цифровізацією економіки.

Мета статті. Метою даної статті є визначення необхідності урахування особливостей переходу до цифрової економіки в системі забезпечення економічної безпеки підприємства та сформувати основні принципи системи економічної безпеки підприємства з урахуванням впливу цифрової економіки.

Виклад основного матеріалу. Сфера досліджень поняття «економічна безпека» дуже різноманітна і отримала висвітлення в багатьох наукових напрямках. Економічна безпека може розглядатися на національному та регіональному рівні, рівні галузей економіки та окремих підприємств, а також на рівні безпеки особистості. В даному дослідженні ми будемо розглядати економічну безпеку підприємства в сучасних умовах переходу до цифрової економіки України.

В сучасних умовах використання цифрових технологій значно полегшує доступ підприємств до глобального капіталу, талантів та інших ресурсів. Сьогодні можна виділити такі основні технологічні тренди в сфері цифрової трансформації економіки:

- роботизація бізнес-процесів;
- перехід на зберігання інформації та проведення обчислень за допомогою «хмарних» технологій;
- наскрізна автоматизація та інтеграція виробничих і управлінських процесів в єдину інформаційну систему;
- поширення в економіці процесів софтизації і сервізації;
- перехід на електронний документообіг («безпаперові» технології);
- 3D-принтинг;
- застосування мобільних технологій для моніторингу, контролю та управління процесів в житті і на виробництві;
- перехід на реалізацію промислових товарів через мережу Інтернет;
- економіка спільної участі (англ. sharing economy), яка передбачає спільне користуванні людськими та фізичними ресурсами [1];
-перетворення традиційних робочих місць на «цифрові».

Зважаючи на особливості сучасного етапу розвитку економіки, до основних складових забезпечення економічної безпеки підприємства, таких, як фінансова безпека (стан фінансових ресурсів і фінансових потоків, що забезпечує сталий розвиток підприємства на основі зростання прибутку і капіталізації) та податкова безпека (стан фінансових ресурсів та податкового планування, яке забезпечує фінансову основу сталого розвитку підприємства при безумовному виконанні ним своїх податкових зобов'язань), вагомої ролі набуває забезпечення інформаційної безпеки підприємства.

Інформаційна безпека сучасного підприємства – це стан захищеності діяльності організації та її інформаційного середовища від негативного впливу дестабілізуючих чинників, яке забезпечує збереження конфіденційної інформації і дозволяє досягти соціально-економічні цілі створення організації.

Таким чином, для забезпечення стабільного функціонування підприємства потрібно постійно проводити роботу для підтримки належного рівня економічної безпеки підприємства. Зокрема, потрібно своєчасно проводити професійний аналіз загроз і ризиків, що генеруються цифровою економікою, таких як кібертероризм, незахищеність даних учасників трансакцій, проблеми захисту інтелектуальної власності тощо. Урахування загроз і ризиків, пов'язаних із цифровими технологіями, дозволить підприємству запобігти більшості форс-мажорних витрат. Тому так важливе впровадження систем захисту від

зовнішніх проникнень, контроль прав доступу високого рівня, розмежування прав доступу до інформації, культивування в колективі обережного ставлення до роботи з неперевіреними джерелами і каналами цифрової інформації [9].

Комерційне шпигунство та конкурента розвідка також підривають базу забезпечення інформаційної безпеки підприємства. Водночас велика частина підприємств, незважаючи на неетичність таких явищ, вдаються до них. Поява на ринку різноманітних пристроїв для підслуховування, інших сучасних технічних розробок дає можливим здійснювати комерційне шпигунство та конкуренту розвідку максимально швидко та якісно.

Крім того, комп'ютерні віруси, спам, легковажне ставлення співробітників до конфіденційної інформації також є суттєвою часткою загроз інформаційній безпеці підприємства. Для захисту від таких загроз підприємства мають залучати цифрові таланти, які володіють комплексом відповідних компетенцій.

Висновки. Для досягнення успіху в сучасних умовах становлення цифрової економіки вітчизняні підприємства повинні паралельно із впровадженням у своїй діяльності цифрових технологій активно працювати над забезпеченням економічної безпеки, зокрема її інформаційної складової. Виклики і загрози економічній безпеці та заходи щодо їх нівелювання повинні передбачатися при стратегічному плануванні економічного розвитку підприємств. Підприємства, які будуть найбільш підготовленими до роботи в нових цифрових умовах, володітимуть конкурентними перевагами і будуть мати можливість збільшити свою частку ринку.

Список літератури

1. Андрусяк А., Ормоцадзе М. Вигідно поділилися: що таке шерингова економіка по-українськи. URL: http://forbes.net.ua/ua/business/1412542-vigidno-podililisya-shcho-take-sheringovaekonomika-po-ukrayinski.
2. Архипов А. Экономическая безопасность: оценки, проблемы, способы обеспечения / А. Архипов, А. Городецкий, Б. Михайлов // Вопр. экономики.- 2004. - №12.- С. 38.
3. Донець Л.І. Економічна безпека підприємства: [навч. пос.] / Л.І. Донець, Н.В. Ващенко. – К.: Центр учбової літератури, 2008. – 240 с.
4. Економічна безпека: [навч. посіб.] / за ред. З.С. Варналія. – К.: Знання, 2009. – 647 с.
5. Іванюта Т.М. Економічна безпека підприємства: [навч. посіб. для студ. вищ. навч. закл.] / Т.М. Іванюта, А.О. Заїчковський. – К.: Центр учбової літератури, 2009. – 256 с
6. Козаченко А. В. Экономическая безопасность предприятия: сущность и механизм обеспечения : монография / А. В. Козаченко, В. П. Пономарев, А. Н. Ляшенко. - К. : Либра, 2003. - 280 с.
7. Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки та затвердження плану заходів щодо її реалізації від 17 січня 2018 р. No 67-р. Законодавство України: веб-сайт:URL: http://zakon.rada.gov.ua/laws/show/67-2018-%D1%80 (дата звернення: 12.12.2019 р.).
8. Моделювання економічної безпеки: держава, регіон, підприємство : монографія / В. М. Геєць, М. О. Кизим, Т. С. Клебанова, О. І. Черняк та ін. ; за ред. В. М. Гейця. - Х. : ВД "ІНЖЕК", 2006. - 240 с.
9. Сторожук О. В., Заярнюк О. В. Фінансова безпека підприємства в умовах цифрової економіки. Фінансово-кредитний механізм розвитку економіки та соціальної сфери: Матеріали ІІ Міжнародної науково-практичної інтернет-конференції, 24-25 жовтня 2019 р., м. Кропивницький. – К.: «Ексклюзив-Систем», 2019. С.182-184. URL: http://dspace.kntu.kr.ua/jspui/bitstream/123456789/9040/1/Zb_materiali_konf_2019.pdf (дата звернення: 12.12.2019 р.).
10. Україна переходить на «цифрову економіку». Що це означає? Укрінформ. Мультимедійна платформа іномовлення України: веб-сайт.URL: https://www.ukrinform.ua/rubric-society/2385945-ukraina-perehodit-na-cifrovu-ekonomiku-so-ce-oznacae.html (дата звернення: 10.12.2019 р.).
11. Хамініч С. Ю. Економічна культура в системі управління / Світлана Юріївна Хамініч. - Дніпропетровськ : Наука і освіта, 2005. - 140 с.

УДК 658.656.13

Д. Яндович, магістр гр. АДМ-18МЗ
Центральноукраїнський національний технічний університет

АКТУАЛЬНІ ПИТАННЯ УДОСКОНАЛЕННЯ ІННОВАЦІЙНОГО МЕНЕДЖМЕНТУ НА ПІДПРИЄМСТВІ

В статті розглянуті питання удосконалення інноваційного менеджменту дорожнього підприємства. Набули подальшого розвитку теоретичні положення щодо використання інновацій на галузевому рівні на стадіях обґрунтування та реалізації стратегії розвитку підприємства.
підприємство, дорожня галузь, інноваційний менеджмент

Постановка проблеми. Інноваційний розвиток в дорожньому будівництві полягає у використанні найбільш сучасної високопродуктивної техніки, удосконаленні технологій та застосуванні матеріалів, що відповідають рівню транспортних навантажень на дорожнє полотно і забезпечують більшу довговічність і надійність автомобільних доріг в межах виділених фінансових ресурсів. Проблеми розвитку дорожнього будівництва в Україні дуже актуальні, враховуючи загальний стан дорожніх комунікацій та рівень автомобілізації населення, що постійно зростає.

Аналіз останніх досліджень і публікацій.. Проблеми інноваційного менеджменту досліджують у своїх працях М. Йохна, С. Ілляшенко, І. Кукурудза, Н. Краснокутська, В. Плакіда, Л. Федулова та ін. Не дивлячись на значну кількість наукових праць, питання удосконалення інноваційного менеджменту підприємств дорожньої галузі залишаються актуальними.

Цілі статті. Метою написання даної статті є вивчення напрямків удосконалення інноваційного менеджменту підприємств дорожньої галузі в сучасних умовах трансформації економіки України.

Виклад основного матеріалу. В даний час потреба в інноваційному розвитку дорожніх підприємств визначається впливом наступних факторів:

- збільшення частки легкових автомобілів з високими динамічними характеристиками і вантажних автомобілів з підвищеними осьовими навантаженнями;
- інтенсивністю руху транспортних потоків, що сприяють істотному збільшенню рівня завантаження доріг і появи транспортних заторів, особливо в зонах впливу мегаполісів, що вимагає прискореного розвитку автомагістралей і швидкісних доріг, що відповідають міжнародним стандартам розвитку і будівництва, застосування вдосконалених систем організації руху;
- значною вартістю основних дорожньо-будівельних матеріалів, сучасної високопродуктивної техніки при одночасному підвищенні вимог до дотримання міжремонтних термінів, що потребує вдосконалення механізмів ціноутворення в дорожньому господарстві;
- очікуваним поширенням нових технологій при будівництві та експлуатації доріг, що тягне за собою зростання вимог до якості виробництва дорожніх робіт з урахуванням особливостей регіонів нашої країни;
- пріоритетним урахуванням вимог забезпечення безпеки руху та екологічних норм в дорожньому будівництві.

Вплив зазначених факторів вимагає від дорожніх підприємств істотної перебудови на принципах інноваційного розвитку.

Зауважимо, що як система управління інноваційний менеджмент складається з двох ланок: керуючої підсистеми (суб'єкта управління) і керованої підсистеми (об'єкта управління). Зв'язок суб'єкта управління з об'єктами відбувається за допомогою руху інформації. Цей рух інформації являє собою сам процес управління, тобто процес розроблення і здійснення керуючої дії суб'єкта управління на об'єкт управління.

Основним завданням інноваційного менеджменту, як складової стратегічного управління дорожнім підприємством, є визначення основних напрямів його науково-технічної і виробничої діяльності в таких сферах: розробка й запровадження нової продукції; залучення до будівництва та ремонту доріг нових ресурсів і нових технологій; освоєння нових методів організації дорожнього будівництва тощо.

Стратегія інноваційного розвитку дорожнього підприємства обов'язково повинна включати: оцінку стартових умов (зовнішні та внутрішні фактори функціонування суб'єкта господарювання); стратегічні цілі і пріоритети розвитку (з врахуванням змін, що відбуваються в економіці держави); основні напрямки реалізацій стратегічних цілей; механізм реалізації стратегії розвитку; інструментарій обліку, контролю та оцінки реалізації стратегії розвитку підприємства.

Діагностика як вид діяльності має здійснюватися на основі принципів: цілеспрямованості (зокрема – орієнтація на визначення стратегічних проблем; поєднання цілей з можливостями підприємства, наявністю чи доступністю необхідних для їх досягнення ресурсів); адаптивності (здатність враховувати зміни середовища і пристосуватись до них задля підвищення конкурентоспроможності, ефективності функціонування); багатоваріантності (використання різних підходів, методів, систем показників для забезпечення максимальної достовірності результатів); мінімізації ризику, що визначає превентивний характер цього інструмента, дослідження причин деструктивних явищ; впорядкованості (використання загальної методології дослідження у стратегічному менеджменті); постійної готовності до реагування, який передбачає, що рівновага підприємства є мінливою, тому постійне реагування на зовнішні прояви дозволить зміцнити позицію підприємства; адекватність реагування підприємства на міру реальної загрози його рівноваги, застосування механізмів нейтралізації загроз на основі визначення їх реального рівня.

На думку автора, необхідно вирішити такі завдання з удосконалення інноваційного менеджменту в дорожніх підприємствах:

- масштабне освоєння прогресивних технологій, включаючи систему інформаційного забезпечення, створення виробництв наукомістких видів продукції;
- координація дій наукових, проєктних і виробничих дорожніх організацій і підприємств, закладів вищої освіти з метою розробки комплексного підходу до вирішення задач інноваційного розвитку;
- забезпечення сприятливих економічних умов для активізації інноваційної діяльності, в тому числі розвиток малого інноваційного підприємництва;
- збереження і розвиток науково-технічного потенціалу дорожніх підприємств для підтримки сучасного технологічного рівня і ефективного використання критичних технологій;
- формування реєстру інноваційних технологій і технічних засобів в галузі дорожнього будівництва та їх впровадження.

Складність управління впровадженням інновацій полягає у недостатньо розвиненій законодавчій базі. Також є необхідність збільшення фінансування дорожнього господарства для прискорення інноваційному розвитку дорожньо-будівельних підприємств. На сучасному етапі розвитку необхідно розробляти і впроваджувати нові прогресивні технології, розвивати і вдосконалювати організацію дорожньо-будівельних робіт, використовувати складні матеріали, розробляти нові технологічні схеми і способи виконання робіт, що базуються на комплексній механізації і автоматизації виробничих процесів.

Висновки. Отже, сьогодні актуалізується проблема використання таких інструментів

інноваційного менеджменту як стратегічний моніторинг та аналіз стратегічного середовища (зовнішнього, безпосереднього або проміжного, внутрішнього), діагностика стану підприємства. В результаті реалізації інноваційної діяльності дорожніх підприємств підвищаться транспортно-експлуатаційні характеристики автомобільних доріг нашої країни, збільшаться міжремонтні терміни, підвищення безпеки дорожнього руху, відбудеться скорочення витрат на будівництво, реконструкцію, ремонт і утримання автомобільних доріг за рахунок використання прогресивних дорожньо-будівельних матеріалів, енергозберігаючих технологій, сучасних інформаційних технологій і систем зв'язку.

Список літератури

1. Балабанов И.Т. Инновационный менеджмент [Текст]: учебное пособие для вузов / И.Т. Балабанов. – СПб.: Питер, 2006. – 397 с.
2. Галушко В.О. Проблеми та перспективи розвитку дорожньої галузі / В.О. Галушко // Дорожня галузь України. – 2011. – № 2. – С. 12-15.
3. Йохна М.А. Економіка й організація інноваційної діяльності [Текст]: навчальний посібник / М.А. Йохна, В.В. Стадник. – К.: Видавничий центр «Академія», 2005. – 400 с.
4. Ілляшенко С.М. Інноваційний менеджмент / С.М. Ілляшенко. – Суми : ВТД, 2010. – 334 с.
5. Краснокутська Н.В. Інноваційний менеджмент [Текст]: навчальний посібник / Н.В. Краснокутська. – К.: КНЕУ, 2003. – 504 с.
6. Кукурудза І.І. Інноваційна діяльність в регіоні: стан, проблеми, перспективи / І.І. Кукурудза // Вісник економічної науки України. – 2012. – № 1. – С. 67–70.
7. Кулицький С. Проблеми розвитку мережі автомобільних доріг в Україні [Електронний ресурс] / С. Кулицький // Україна: події, факти, коментарі. – 2017. – № 22. – С. 56–65. – Режим доступу: http://nbuviap.gov.ua/images/ukraine/2017/ukr22.pdf. – Назва з екрану.
8. Мельник, О. Г. Інноваційні системи економічної діагностики підприємства на засадах індикаторів / О. Г. Мельник, І. Б. Олексів, Н. Ю. Подольчак, Р. В. Шуляр. – Львів : Магнолія. – 2009. – 241 с.
9. Механізм формування і реалізації стратегії управлінських інновацій [Електронний ресурс]. – Режим доступу : http://knowledge.allbest.ru/.
10. Мойсеєнко І.П. Інвестування : [навч. посіб.] / І.П. Мойсеєнко. – К. : Знання, 2006. – 490 с.
11. Плакіда В.Т. Конспект лекцій з дисципліни «Інноваційний менеджмент» / В.Т. Плакіда. – Х. : ХНАМГ, 2010. – 76 с.
12. Федулова Л.І. Менеджмент організацій : [підручник] / Л.І. Федулова. – К. : Либідь, 2004. – 448 с.

УДК 336.74

О. Ясененко, магістр гр. ФС-18М(1,4)
Центральноукраїнський національний технічний університет

ТЕОРЕТИЧНІ ПІДХОДИ ДО ВИЗНАЧЕННЯ СУТНОСТІ БАНКІВСЬКОГО КРЕДИТУВАННЯ

У статті розкрито сутність та особливості кредитування суб'єктів господарювання комерційними банками. Обґрунтовано вплив комерційних банків на розвиток кредитного ринку України. Показано роль кредиту у соціально-економічному розвитку країни. Відображено кредитування як одну із складових банківської діяльності, основне джерело забезпечення потреб суб'єктів господарювання у грошових ресурсах. Пояснено соціально-економічне значення кредиту та його вплив на економіку. Досліджено кредитну діяльність комерційних банків з урахуванням трансформаційних процесів в економіці України, її інтеграції у світове господарство. Висвітлено значення кредитного потенціалу та необхідність іпотечного кредитування. Розроблено пропозиції щодо удосконалення кредитування та покращення кредитної політики установами банків.

кредит, кредитування, банківська діяльність, ризики, кредитний потенціал, кредитні ресурси, кредитна політика

Постановка проблеми. Банківська система є частиною економічної системи країни і

має вагоме значення для національного господарства, що обумовлено визначеними повноваженнями, а також впливом банківської сфери на інші сектори. У період політичної та економічної кризи особливого значення набуває процес кредитування суб'єктів господарювання установами банків. Дослідження кредитної діяльності комерційних банків з урахуванням трансформаційних процесів в економіці України, її інтеграції у світове господарство, посилення конкуренції між банками, впровадження новітніх банківських технологій є особливо актуальним для організації банківської справи в нашій країні.

Аналіз останніх досліджень і публікацій. Пізнання сутності кредиту, його ролі в соціально-економічному розвитку країни привертали увагу людства з епохи ранніх цивілізацій та були предметом дослідження майже всіх течій і шкіл економічної науки.

Організації кредитної діяльності комерційних банків присвячено значну кількість праць вітчизняних і зарубіжних економістів. Питання кредитування досліджували такі вітчизняні вчені, як З. М. Васильченко, О. В. Васюренко, А. С. Гальчинський, Д. Д. Гладких, І. С. Гуцал, О. В. Дзюблюк, О. Т. Євтух, Ю. А. Заруба, Б. С. Івасів, О. А. Кириченко, В. В. Корнєєв, В. Д. Лагутін, Б. Л. Луців, І. О. Лютий, В. І. Міщенко, А. М. Мороз, Л. О. Примостка, К. С. Раєвський, С. К. Реверчук, М. І. Савлук, Р. І. Тиркало, Я. І. Чайковський та інші. Значний внесок у вивчення процесу кредитування належить таким зарубіжним економістам, як Б. Бухвальд, Р. Г. Габбард, Е. Дж. Долан, Б. Едвардс, Є. Ф. Жуков, Г. Г. Коробова, Т. Кох, О. І. Лаврушин, В. Лексіс, Ю. С. Маслєнченков, Р. Л. Міллер, Ф. С. Мішкін, Е. Морсман, Г. С. Панова, М. А. Пессель, Ж. Рівуар, П. Роуз, Дж. Сінкі, А. М. Тавасієв, В. М. Усоскін.

Відзначаючи цінність та значущість наукових доробок, необхідно зазначити, що у більшості праць розглядаються питання організації кредитних взаємовідносин банків із позичальниками, концептуальні засади управління кредитним портфелем банку.

Формулювання цілей статті. Метою наукової статті є поглиблення теоретичних основ організації кредитних відносин комерційних банків і розробка рекомендацій щодо оптимізації процесу формування та управління їх кредитним портфелем. Відповідно до мети дослідження були поставлені такі завдання:

- розкрити економічну роль і зміст кредитної діяльності комерційного банку в умовах кризи та трансформаційних процесів в економіці;
- дослідити сутність поняття «кредитний потенціал банку», визначити чинники його формування та реалізації, визначити склад системи банківського кредитування;
- охарактеризувати етапи процесу організації банківського кредитування.

Виклад основного матеріалу. Банківський кредит - це економічні відносини, які виникають з приводу перерозподілу кредитного потенціалу банку на умовах повернення, платності, строковості та цільового використання позичкових ресурсів.

У Законі України «Про банки та банківську діяльність» вказано, що банківським кредитом є будь-яке зобов'язання банку надати певну кількість грошей, будь-яка гарантія, будь-яке зобов'язання набути права вимоги боргу, будь-яке подовження терміну погашення боргу, яке дано в заміну на зобов'язання боржника повернути заборговану суму, а також погасити відсотки та інші збори з такої суми [1].

Кредитний потенціал банку - це максимально можливий обсяг власних та залучених коштів, який банківська установа може розмістити у заборгованість на принципах банківського кредитування та інвестування, а кредитні ресурси - це реальні кошти банку, які є складовою його кредитного потенціалу. Згідно з міжнародними стандартами, кредити класифікуються за багатьма ознаками, а саме: роллю банку в наданні кредиту, формою банківського кредиту, економічними суб'єктами-позичальниками, валютою кредиту, строками користування, формою забезпечення, методами надання та порядком погашення, характером процентної ставки та кількістю кредиторів.

Розв'язання проблем стабілізації та відродження економіки України можливі лише при інвестуванні значних ресурсів у промисловість, джерела одержання яких значно обмежені. Тому кредит під заставу нерухомості, тобто іпотечний кредит, повинен стати джерелом

поповнення основного капіталу промислових підприємств. Визначення іпотечного кредиту зафіксовано в Законах України:

- «Про іпотеку»: основне зобов'язання - зобов'язання боржника за договорами позики, кредиту, купівлі-продажу, лізингу, а також зобов'язання, яке виникає з інших підстав, виконання якого забезпечене іпотекою [2];
- «Про іпотечне кредитування, операції з консолідованим іпотечним боргом та іпотечні сертифікати»: іпотечне кредитування - правовідносини, що виникають з приводу набуття права вимоги іпотечного боргу за право чинами та іншими документами; іпотечний борг - основне зобов'язання за будь-яким правочином, виконання якого забезпечене іпотекою [3].

Закон України «Про заставу» спрогнозував деякі види застави: знайшов предмет застави, договір застави тощо. Можна вважати, що саме цим законом було відновлено іпотеку, яка є одним із найбільших дієвих та безпечних способів покращення кредитних умов та інших договорів [4].

Кредитна діяльність банку є складною системою, що відображає сукупність взаємопов'язаних елементів, які забезпечують реалізацію на практиці функцій кредиту та дотримання принципів кредитування. Основними елементами кредитного механізму є: суб'єкти, об'єкти кредитування, форми кредитування, порядок надання і погашення позик, система формування кредитних ресурсів та їхнє резервування, система формування і використання резервів з відшкодування можливих втрат від кредитної діяльності, економічний контроль та банківський нагляд за кредитною діяльністю банків.

Кредитування як фундаментальна складова діяльності комерційних банків є основним джерелом забезпечення потреб суб'єктів господарювання у грошових ресурсах та підґрунтям для збільшення інвестицій, сприяючи безперервності відтворювального процесу та зміцнюючи економічний потенціал. Доцільність банківських кредитних вкладень у різні галузі національного господарства значною мірою обумовлюється можливостями менеджменту банківських установ здійснювати оптимальне формування і управління кредитним портфелем, забезпечуючи належну ефективність банківської діяльності при мінімально можливому рівневі ризику. Зростання банківського кредитування без належного врахування ризиків, що при цьому виникають, та можливостей ефективно управляти сформованим кредитним портфелем несе в собі ризики для функціонування як окремих комерційних банків, так і банківської системи України.

Більшість науковців-економістів вважає, що сучасна економіка є «кредитною», а, отже, кредит - це всеохоплююче явище, що підвищує економічну активність суб'єктів господарювання та пов'язує широкий спектр їхніх економічних зв'язків. Кредит є засобом обміну, який підвищує зв'язки між окремими господарствами, що зливаються в одне. При застосуванні обміну тільки за готівкові гроші мінові взаємини пов'язують окремі господарства тільки під час обміну; за кредитного обміну окремі господарства стають пов'язаними на весь строк дії кредиту, тобто впродовж тривалішого періоду. Вони отримують особливий розвиток завдяки кредиту [7, с. 287].

Проблеми реального сектора економіки призводять до скорочення комерційного кредитування та до складнощів із погашенням банківських кредитів, а, отже, і до зростання проблемної кредитної заборгованості у банках, що негативно позначається на фінансовому стані останніх. Скорочення банківського кредитування, яке знижує економічну активність суб'єктів господарювання, зменшує їх рівень виробництва і доходів та викликає економічний спад, який стається при наявності проблем у фінансовій системі.

Кредит як фінансовий інструмент об'єднує реальний і фінансовий сектори економіки, насправді не є причиною, а тільки передавальним механізмом кризових явищ з реального сектора у фінансовий і навпаки. Й. Шумпетер вважав, що кредит - це в основному вироблення купівельної здатності для передачі її підприємцеві, що надає йому вільний шлях до народногосподарського потоку благ ще до того моменту, як він буде мати на це обґрунтоване право [8, с. 217].

М. Бунге зазначав, що кредит знищує ланцюги, які накладалися на виробництва нерухомістю капіталів та пасивною діяльністю праці [6, с. 363].

Отже, кредит має важливе соціально-економічне значення, а кредитні інститути, насамперед банки, забезпечують пропозицію кредиту і таким чином впливають на економіку. Відомо, що кредитна діяльність супроводжується значно великими ризиками. Тому і управління кредитними ризиками є вагомим вченням та практичною проблемою. Зокрема, в економічній літературі кредитному ризику надають значення імовірності неповернення позичальником отриманого кредиту та відсотків за користування позикою унаслідок фінансових ускладнень, банкрутства чи шахрайства [5, с. 479].

М. Туган-Барановський наголошував, що загальноекономічна криза починається з фінансової [7, с. 277]. На сучасному ж етапі значення фінансових процесів у коливаннях економічної кон'юнктури тільки зростає.

Таким чином, очевидним є те, що різні кредитори володіють різними можливостями і засобами отримання інформації щодо кредитоспроможності позичальника, а отже і різними можливостями захисту від кредитних ризиків.

Висновки. Таким чином, ефективному використанню ресурсів та стимулюванню економічного зростання сприяє розвиток кредиту, створення банків та кредитної системи в цілому.

Банківська система через надання кредитів організовує й обслуговує рух капіталу, забезпечує залучення, нагромадження та перерозподіл капіталу у ті галузі виробництва та обігу, де виникає у ньому потреба. Вплив комерційних банків на розвиток кредитного ринку України пояснюється тим, що вони є структурами, які акумулюють фінансові ресурси суспільства, трансформують їх у кредитні ресурси та спрямовують на розвиток економіки.

Важливим напрямом удосконалення інституційного забезпечення управління кредитним ризиком банків в умовах рецесії та кризи є створення Фонду акумуляції і викупу проблемних боргів, основним завданням якого буде викуп проблемної заборгованості у кредитних організацій, її подальше обслуговування і, по можливості, рефінансування на ринкових умовах. Необхідним є прийняття окремого Закону України «Про кредит» або Кредитного кодексу України.

Список літератури

1. Про банки і банківську діяльність: Закон України; за станом на 16.07.2015 [Електронний ресурс] / Верховна Рада України від 07.12.2000 р. № 2121-III. - Режим доступу: http://zakon.rada.gov.ua/2121-14
2. Про іпотеку: Закон України; за станом на 13.05.2014 р. [Електронний ресурс] / Верховна Рада України від 05.06.2003 № 898-IУ. - Режим доступу: http://zakon.rada.gov.ua/cgi- bin/laws/main.cgi?nreg=898-15
3. Про іпотечне кредитування, операції з консолідованим іпотечним боргом та іпотечні сертифікати: Закон України; за станом на 20.11.2012 р. [Електронний ресурс] / Верховна Рада України від 19.06.2003 р. № 979-IУ. - Режим доступу: http://zakon.rada.gov.ua/cgi- bin/laws/main.cgi? nreg=979-15
4. Про заставу: Закон України; за станом на 15.04.2014 р. [Електронний ресурс] / Верховна Рада України від 02.10.1992 р. № 2654-XII. - Режим доступу: http://zakon.rada.gov.ua/cgi- bin/laws/main.cgi?nreg=2654-12
5. Аналіз банківської діяльності : підручник / [А. М. Герасимович, М. Д. Алексеєнко, І. М. Парасій-Вергуненко та ін.] ; за ред. А. М. Герасимовича. - Вид. 2-ге, без змін. - К.: КНЕУ, 2006. - 600 с.
6. Сучасний дискурс : монографія / Бунге М.Х.; за ред. В. Д. Базилевича. - К.: Знання, 2005. - 697 с.
7. Туган-Барановский М. И. Периодические промышленные кризисы. История английских кризисов / М. И. Туган-Барановский // Общая теория кризисов. - М.: Наука - РОССПЭН, 1997. - 368 с.
8. Шумпетер Й. Теория экономического развития: (исслед. предпринимат. прибыли, капитала, кредита, процента и цикла коньюктуры) / Пер. с нем. В. С. Автономова и др.; общ. ред. А. Г. Милейского. - М.: Прогресс, 1982.

РОЗДІЛ ІІ

УДК 004

Я. Бабаліч, магістр гр. КІ-18М-1,4
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ ІОТ З ВИКОРИСТАННЯМ BLUETOOTH 5

У статті розроблено програмне забезпечення, яке призначено для системи IoT з використанням Bluetooth 5. Метою розробки є дослідження та програмна реалізація системи IoT з використанням Bluetooth 5.Об'єктом дослідження є процес IoT з використанням Bluetooth 5. Предметом дослідження є методи IoT з використанням Bluetooth 5. Методи дослідження базуються на методах Інтернету речей, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи IoT з використанням Bluetooth 5. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.
комп'ютерна інженерія, IoT, Bluetooth 5

Постановка проблеми. Майже кожна людина використовує Bluetooth: на смартфоні, планшеті, комп'ютері або для підключення аксесуарів, наприклад, бездротових навушників. У найближчому майбутньому ситуація не зміниться: на думку дослідників ринку (компанії ABI Research), в 2021 році буде придбане близько 5 млрд. Bluetooth-пристроїв. При цьому особливо великий потенціал росту буде спостерігатися в пристроїв, що використовують технологію «Інтернет речей»: наручні годинники, освітлювальні прилади або системи автоматичної підтримки температури.

П'яте покоління Bluetooth розроблене саме для «Інтернету речей». Наступні три інновації застосовуються винятково в енергозберігаючому режимі Low-Energy (LE):

– Підвищена швидкість передачі даних: максимальна швидкість збільшується з 1 до 2 Мбіт/с.

– Збільшений радіус дії: у зоні прямої видимості (без перешкод на шляху) він збільшений з 50 до 200 метрів.

– Поліпшена передача даних: через т. зв. «бікони» (маячки) може бути передане в 8 разів більше інформації.

Крім того, у новій специфікації Bluetooth застосовані оптимизуючі рішення, спрямовані на підвищення стійкості до перешкод. Це досить важливо, тому що Bluetooth працює у вкрай переповненому діапазоні частот 2,4 Ггц.

Основні нововведення Bluetooth 5 – висока швидкість передачі даних і збільшений радіус дії – обмежуються в енергоефективному режимі Low Energy. У ньому вас чекає невеликий підступ: одночасно можна використовувати тільки одну з переваг.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи IoT з використанням Bluetooth 5.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи IoT з використанням Bluetooth 5.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем IoT з використанням Bluetooth 5.

– Дослідження системи IoT з використанням Bluetooth 5.

– Програмна реалізація системи IoT з використанням Bluetooth 5.

Об'єктом дослідження є процес IoT з використанням Bluetooth 5.

Предметом дослідження є методи IoT з використанням Bluetooth 5.

Методи дослідження базуються на методах Інтернету речей, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. У той час як Wi-Fi б'є рекорди швидкості в гігабітному діапазоні, Bluetooth LE дотепер «тупцює» близько 1 Мбіт/с. Проте, Bluetooth 5 у режимі LE збільшує максимальну швидкість передачі даних у два рази. Зрозуміло, від цього Bluetooth LE не стане «ракетою», тому що існують деякі обмеження.

Швидкість передачі «нетто» в Bluetooth LE-режимі постійно збільшується. Але швидкість «брутто» 2 Мбіт/с в Bluetooth 5 є лише опціональною.

При значенні 2 Мбіт/с мова йде про швидкість «брутто», максимальна швидкість «нетто» при цьому залишиться на рівні 1,4 Мбіт/с. Крім того, це значення має силу тільки в ближній області дії, тому що для передачі більшого обсягу корисних даних в одному пакеті Bluetooth 5 «заощаджує» на корекції помилок.

Однак швидкість 2 Мбіт/с у режимі LE є скоріше опцією, що виробники можуть реалізувати у своїх пристроях. Як альтернатива також доступні швидкості 1 Мбіт/с, 500 Кбіт/с і 125 Кбіт/с.

Причому, за замовчуванням у всіх Bluetooth-пристроях установлена швидкість передачі даних 1 Мбіт/с, інші параметри є опціональними, а право вибору реалізації надано виробникам.

Також не можна сліпо покладатися на те, що всі пристрої, що використовують Bluetooth 5, підтримують більше швидкий LE-режим.

Інтернет речей без помилок

Хоча професійне встаткування й забезпечує передачу даних по Bluetooth-Каналі до 500 метрів, стандарт Bluetooth лише в цей час надав можливість енергозберігаючих підключень на відстані до 200 метрів.

Технологія Bluetooth застосовується головним чином у ближній області дії, хоча існує встаткування, що дозволяє передавати дані по Bluetooth на відстань до 500 метрів. Втім, подібні екстремальні радіуси дії вимагають значних витрат, тому що для цього необхідно істотно збільшувати потужність передавачів.

Крім LE-режиму стандарт Bluetooth уже досить давно визначає різні класи, у яких пристрою можуть передавати дані з потужністю до 100 мВт. Для таких Bluetooth-модулів, відповідно до параметрів класу 1, потрібно занадто більша потужність, що не підходить для інтернету речей.

Відтепер, із застосуванням Bluetooth LE, це виглядає інакше, тому що застосовувані в ньому Bluetooth-модулі збільшують радіус дії завдяки технології Forward Error Correction (FEC, прямої корекції помилок) без значного збільшення потужності передачі. Однак через збільшену дальність дії доводиться жертвувати швидкістю передачі даних.

Якщо подивитися на стек протоколів Bluetooth, можна побачити, що інновації для збільшення дальності дії Bluetooth 5 ставляться до самого нижнього (фізичному) рівня. Корисні дані передаються двічі й додатково шифруються, у такий спосіб приймаючий пристрій часто може самостійно виправляти помилки. При цьому наріжним каменем для шифрування є швидкість передачі символів.

Структура пакета даних Bluetooth з високою швидкістю

Bluetooth 5 в енергозберігаючому режимі просто збільшує частку корисних даних у пакеті для досягнення максимальної швидкості передачі 2 Мбіт/с.

У найпростішому випадку кожний біт передається двічі. Кожний нуль відправляється в такому варіанті як «00», одиниця – як «11». Це зменшує вдвічі максимальну брутто-швидкість передачі даних, з 1 Мбіт/с до 500 Кбіт/с. Проте, для ще більшої дальності дії стандарт Bluetooth визначає також розширене шифрування, при якому кожний біт

передається не двома, а вісьма символами. Кожний нуль кодується послідовністю символів «00110011», кожна одиниця – «11001100».

Структура пакета даних Bluetooth для збільшеного радіуса дії

Система корекції помилок передає корисні дані кілька разів і шифрує їхнім особливим образом, в остаточному підсумку в кожному пакеті передається менше корисних даних. Завдяки цьому збільшується відстань передачі пакетів даних Bluetooth-LE з 50 до 200 м.

Якщо в приймач надходить послідовність «11001101», можна легко визначити й виправити помилку в останньому біті. Однак швидкість передачі даних при цьому знижується до 125 Кбіт/с.

Бікони й створення мережі

Bluetooth 5 також збільшує довжину повідомлень, переданих без підключення, за допомогою Bluetooth-біконів. Подібним чином можуть відправлятися короткі інформаційні фрагменти. При використанні біконів Bluetooth 4.x забезпечує довжину повідомлення 30 байт, Bluetooth 5 передбачає більш ніж восьмикратне збільшення обсягу переданих даних (256 байт). Пристрої Bluetooth 5 можуть працювати у всіх режимах своїх попередників і завдяки цьому є назад сумісними.

Наступним етапом інтернету речей стане особлива специфікація для спрощеного об'єднання Bluetooth-пристроїв у єдину мережу, що повинна бути представлена в середині 2018 року. Завдяки цьому Bluetooth-пристрою зможуть у режимі енергозбереження приймати повідомлення від одного пристрою й передавати їх іншому. Подібним чином повинна бути додатково збільшена й дальність дії.

Розробка структурної схеми

Розумний Будинок управляє опаленням і стежить за комфортом

Чи працюєте Ви в офісі, чи перебуваєте з дітьми вдома або просто проводите сімейне дозвілля сидячи в екрана телевізора. Поки Ви зайняті своїми справами, Ваш Розумний Будинок управляє опаленням і стежить за комфортними умовами в приміщеннях.

Інтелектуальний будинок завжди подбає про те, щоб цілий рік усередині приміщення був комфортний мікроклімат, де й дихається легко, і працюється продуктивно й відпочинок проводиться чудово. З автоматичною системою управління опаленням Розумний Будинок завжди буде привітати Вас гарною й прекрасною погодою, а саме головне такий, котрої побажаєте Ви.

Постійний контроль температури приміщень і автоматичне управління опаленням попереджає виникнення й розвиток критичних ситуацій – занадто холодно, мерзлякувато й сиро, надто пекуче. Ваш Розумний Будинок дарує тільки добрий і турботливе тепло, затишок і комфорт. Управління кліматом і теплом у Вашім будинку дозволить не тільки відчувати цілорічну комфортну погоду в будинку, але й істотно заощаджувати витрати на енергоресурси до 40%.

Розумний Будинок – опалення. Можливості системи:

– Незалежна терморегуляція окремих приміщень Вашого будинку – комора, дитяча, кухня, бізнес-кабінет, спальня; у кожному окремому приміщенні встановлюється індивідуальний температурний поріг, що забезпечує максимальний комфорт приміщення залежно від його призначення;

– Термоконтроль у приміщеннях залежно від пори року й часу доби; одночасно відслідковується температура як усередині приміщення, так і за його межами – створюються сприятливі температурні умови усередині Вашого Розумного Будинку;

– Завдяки убудованим температурним датчикам відслідковується й регулюється температура в приміщеннях; Ви можете як вручну, так автоматично (використання сценаріїв) регулювати й контролювати роботу опалювального встаткування – включення / вимикання теплих підлог, радіаторів;

– Безпека системи опалення в Розумному Будинку забезпечується за рахунок своєчасного реагування на надзвичайні ситуації; у випадку порушення цілісності труб, виходу з ладу модулів системи опалення, відмови / поломки електричного нагрівального

кабелю (тепла підлога) відбувається їхнє повне відключення (знеструмлення); при цьому Ваш Розумний Будинок сповістить Вас про аварійну ситуацію;

– Кошти на покупку встаткування вертаються завдяки постійній економії на опаленні.

Як «співробітничають» Розумний Будинок і система опалення

За комфортну температуру повітря у Вашім будинку відповідають такі опалювальні прилади як радіатори, казани, нагрівальні кабелі підлоги й ін. Кожний із цих приладів має свій принцип роботи й виконує свою окрему функцію. Завдання всієї опалювальної техніки одна – обігрів приміщення з мінімальними втратами.

Установивши параметри бажаної температури для кожної окремої кімнати Ви задаєте системі програму контролю. Управління опаленням може здійснюватися як автоматично, так і вручну. Тепер у приміщеннях буде підтримуватися оптимальна й комфортна температура. Ваш Розумний Будинок сам визначить для кожного опалювального приладу індивідуальний режим роботи, що дозволить раціонально використовувати опалювальну систему в цілому. Тепер Ви з легкістю можете контролювати роботу як всієї системи так і окремих опалювальних приладів, що дуже зручно, а головне вигідно по енерговитратах.

Ваша «розумна» система опалення сама відкоригує температуру в будинку коли за вікном різке похолодання або відлига. З огляду на температуру за межами будинку, система регулює роботу всіх нагрівальних елементів так, щоб у приміщенні температура залишалася для Вас комфортної й оптимальної.

Приміром, уночі теплі підлоги можуть вимикатися системою, а до Вашого пробудження вже будуть прогрітими. Ви зможете програмувати режим роботи теплих підлог на всі дні тижня.

У випадку виходу з ладу опалювального встаткування, збоїти або припинення електроживлення система Вас про це проінформує й припинить роботу несправних елементів.

За допомогою єдиної панелі Ви можете управляти системою опалення так, як Вам це необхідно. Управляти можна й дистанційно. За допомогою мобільного телефону, через Інтернет з балкона другого поверху, з дивана або з Галапагосских островів.

А ще Ви завжди можете прогріти сауну або окремо варту баню прямо з офісу або за розкладом, наприклад, щоранку неділі. Активуйте режим «відпустка» і будинок сам про себе подбає. При Вашій відсутності опалювальна система буде працювати в ощадливому режимі, споживаючи мінімум енергії. А до Вашого приходу зробить температуру в будинку знову оптимальної й комфортної для Вас.

Навіщо потрібна «розумна» система опалення

З Розумним Будинком Ви здобуваєте домашнє тепло, затишок і комфорт – та якість життя, що не можуть подарувати елементи домашнього декору або інтер'єра.

Опалювальна система з убудованим інтелектом дозволить Вам істотно заощаджувати Ваші кошти. Ринок опалювального встаткування пестрить вигідними ціновими пропозиціями, а от ціни на енергоресурси неухильно ростуть. Витративши один раз на «розумну» систему Ви окупите свої витрати в доступному для огляду майбутньому.

У підсумку вся турбота по управлінню опаленням Розумний Будинок бере на себе. А Ви одержуєте повний контроль над всім устаткуванням не тільки коли Ви будинку, але й за його межами.

Системи контролю й управління доступом у будинок, офіс, квартиру, виробництво

Ще однією сучасною системою, що може інтегруватися в Розумний Будинок поряд з домофонією і відеоспостереженням, є система контролю й управління доступом (скорочено СКУД). На сьогоднішній день дані системи надають їхнім власникам широкі можливості по управлінню безпекою будинку й рівнем доступу в нього. Це має на увазі під собою, наприклад, розмежування прав доступу до різних приміщень, облік відвідувань і тривалість перебування на об'єкті.

СКУД – це комплекс технічних засобів, що вирішує 3 основні завдання:

– СКУД регулює переміщення людей на присадибній ділянці, у будинку або квартирі, на підприємстві.

– СКУД розподіляє права доступу в різні зони об'єкта (офісу).

– СКУД дозволяє створити на підприємстві систему обліку робочого часу.

Маються на увазі абсолютно прості, логічні й необхідні речі, які стосуються в першу чергу власників приватних будинків, більших квартир з розділеними приміщеннями, власників складських приміщень або підприємств. Приміром, у вас у будинку є домробітниця й Ви не бажаєте надавати доступ у яке-небудь приватне приміщення – робочий кабінет, серверна, котельня. Запрограмувавши необхідним образом систему контролю й управління доступом, Ви можете виділити доступ робочому персоналу тільки до певним і необхідним на вашу думку приміщенням.

Можливості системи контролю й управління доступом:

– Дозволяти санкціонований прохід через двері, обладнані елементами СКУД.

– Автоматичне або ручне розблокування дверей при надходженні сигналу «Пожежа» від системи пожежної сигналізації.

– СКУД може надавати доступ співробітникам у зони й приміщення відповідно до розмежування прав доступу – електронна система пропусків на підприємстві.

– Ведення й перегляд архіву й оперативної інформації.

– Можливість видачі звітів за часом проходу співробітників, робочого персоналу для обліку робочого часу.

– СКУД може інтегруватися із системами охоронної й пожежної сигналізації, відеоспостереження, Розумний Будинок на апаратному й/або програмному рівнях.

– Архівування всіх подій, що відбуваються в системі, – запити на вхід і на вихід, тривожні повідомлення, несправності, перехід устаткування на резервне електроживлення, коректування часу.

– Блокування точок доступу при виникненні позаштатних ситуацій і розблокування при необхідності.

– СКУД може передавати сигнали тривоги на АРМ у випадку несанкціонованого проникнення в зони доступу й виділені приміщення (наприклад, розкриття дверей).

– Автоматичне резервування бази даних відповідно до заданого розкладу на серверах.

– Локальна постановка приміщень на охорону (з охорони) виділених охоронюваних приміщень за допомогою зчитувачів.

Підставою для допуску в приміщення є електронні карти-ідентифікатори співробітника, мешканця будинку, робочого персоналу. Права доступу (дозволені зони доступу й тимчасових інтервалів) можуть установлюватися власником будинку, що управляє виробництвом, а також адміністратором СКУД. Вхід і вихід співробітників у будинок, а також прохід через зони повинен здійснюватися по особистих електронних картах-ідентифікаторам відповідно до дозвільної системи доступу в автоматизованому режимі.

Система контролю й управління доступом може складатися із централізованих і децентралізованих контролерів доступу, з'єднаних із сервером СКУД по IP мережі. До контролерів підключається периферійне встаткування. Для централізованого управління системою через АРМ і інтеграції її компонентів із системами безпеки можливе підключення СКУД до єдиної системи збору й обробки інформації за допомогою спеціально налаштованого програмного забезпечення.

Кому вигідна система контролю доступу в приміщення?

Система може враховувати час приходу й відходу не тільки постояльців і працівників будинку. Особлива користь СКУД очевидна для тих, у кого в родині є діти. Після того, як ваша дитина прикладе свій персональний ключ до зчитувача, Ви відразу ж одержите на свій телефон або планшет смс-повідомлення про цьому, а система Розумний Будинок запустить

необхідний сценарій: наприклад, відключить сигналізацію, вмикає світло в прихожій, активує або відключить системи опалення, охолодження, вентиляції, а при бажанні відключать всі телевізори, щоб ваше чадо не відволікалося від виконання домашнього завдання. Але головне: Ви завжди будете знати, що ваша дитина благополучно повернулася додому.

Також електронна система пропусків найчастіше використовується в офісах, на підприємствах, у банківській сфері. Для власників середнього й великого бізнесу використання таких систем полегшує в рази процес управління персоналом, підвищує ефективність використання робочого часу, і відповідно ресурсів.

Для реалізації відкриття дверей даною системою передбачено кілька варіантів. Відповідно, для різних завдань буде зручний свій. Наприклад, для шлагбаума найбільш зручний буде радіобрелок, для входу в будинок або квартиру – пластикова карта або електронний «ключ-таблетка», ну а для особистого робочого кабінету серйозного бізнесмена можна поставити клавіатуру для уведення пароля або навіть сканер відбитка пальця.

СКУД вирішує завдання безпеки об'єкта й знижує вплив «людського фактора» у випадку позаштатних, непередбачених ситуацій. СКУД разом із системою Розумний Будинок підвищує безпеку персоналу й відвідувачів, домочадців і постояльців, відповідає за схоронність матеріальних ресурсів на контрольованому об'єкті.

До складу системи контролю доступу в приміщення входять пристрої, що зчитують, контролери СКУД, з'єднані із сервером по IP мережі, електронні пропуски або біометричні ідентифікатори. До контролерів системи СКУД підключається периферійні встаткування. Всі зони входу-виходу (точки доступу) обладнаються зчитувачами.

Хто відповідає за клімат-контроль у будинку?

Ви замислювалися скільки кліматичної техніки у Вас будинку. Кондиціонери, спліт-системи, теплі підлоги, радіатори – всі ці побутові прилади хоча б у мінімальному наборі присутні в будинку кожного з нас. Кліматична техніка завзято трудиться за створення зони комфорту для Вас.

На перший погляд здаються всі ці прилади створені й працюють на «благо» свого хазяїна. Насправді дуже часто виникає ситуація «марності» роботи таких приладів. Коли опалювальна система завзято гріє повітря, а система кондиціювання одночасно те ж повітря прохолоджує.

Крім того, будь-яка кліматична техніка вимагає контролю й управління. Скільки часу Ви витрачаєте на це? Безумовно багато приладів оснащені блоками управління. Тільки уявити собі скільки таких окремих пультів управління може скопитися у Вас будинку. Як проконтролювати й попоратися з усім цим?

– Система Розумний Будинок знає як все повинне працювати. Ваш будинок подбає про це. А Вам залишається насолоджуватися нечуваним колись затишком і комфортом.

Розумний Будинок управляє кліматом і створює індивідуальне середовище для кожного.

З Розумним Будинком у кожній кімнаті можна створити свій мікро-клімат. Багатозоний клімат-контроль рятує від необхідності щораз набудовувати терморегулятори на радіаторах, включати й виключати кнопки на пультах кондиціонерів і іншої кліматичної техніки.

Тепер усе, що від Вас потрібно – указати комфортну для Вас температуру, вологість за допомогою єдиної панелі управління. Розумний Будинок візьме на себе управління кліматом і сам розпорядиться роботою всіх приладів. Робота кліматичного встаткування буде регулюватися автоматично, переходячи з денного в нічний режим. При цьому, Ваш Розумний Будинок подбає про економію енергоресурсів, перемикаючи всю техніку в режим «економ», коли Ви виїхали у відпустку.

Управління кліматом з розумом

Щоб одержати максимальну ефективність від роботи кліматичної техніки необхідна погоджена робота кожного із приладів. У вітальні необхідно нагріти повітря, на кухні стало

занадто пекуче, а в дитячій занадто сухе повітря? Оптимальна робота всіх складових кліматичної системи дозволить підтримувати в кожному приміщенні будинку індивідуальну кліматичну зону. Ваш будинок перетворюється в окремий мир зі своїм кліматом, засипаючи під час відсутності хазяїв і активуючись тільки вони з'являться.

Система Розумний Будинок подбає про клімат-контроль. Ваш будинок цілодобово стежить за такими параметрами як:

- Температура повітря.
- Рівень вологості.
- Кондиціювання.
- Фільтрація повітря.

Ваш Розумний Будинок самостійно підготує умови для сну, прогріє кімнату у вечірній час, а до ранку понизить температуру. Варто як тільки встановити температурний режим на панелі управління.

Управління вентиляцією залежно від температури й вологості в кожній кімнаті – система клімат-контролю сама визначить коли необхідно відкоригувати (підвищити / понизити) температуру в приміщенні, вологість, включити або виключити вентиляцію знаючи заздалегідь зазначені умови Вашого комфорту в будинку. Системі можна вказати індивідуальні умови мікроклімату для кожної окремої кімнати.

Управління іонізацією й озонуванням повітря – Ваш Розумний Будинок сам подбає про те, щоб у всіх кімнатах завжди було свіже, чисте й здорове повітря. Система визначить коли необхідно очистити повітря від бактерій, цвілі, неприємних заходів або тютюнового диму, вивчивши звички свого хазяїна. Розумний Будинок завжди подбає про Ваше самопочуття й здоровий сон.

Контроль і управління кліматом у спеціальних приміщеннях – винний льох, бібліотека, комора й інші спеціалізовані приміщення у Вашім будинку вимагають особливих умов мікроклімату. Ваш Розумний Будинок не дозволить зіпсується Вашої безцінної колекції картин або книг, управляючи й контролюючи умовами мікроклімату.

Можливості клімат-контролю в Розумному Будинку:

- Пороги нагрівання й охолодження – кожний опалювальний прилад має свої щаблі нагрівання. З урахуванням комфорту й економії енергії автоматика сама вирішує який щабель нагрівання призначити для того або іншого приладу. У такий спосіб підтримується комфортна температура у Вашім будинку в погодженому й ощадливому режимі.
- Кондиціювання – Розумний Будинок управляє погодженою роботою кондиціонерів, спліт-систем з іншими елементами обігріву й охолодження не вимагаючи Вашого втручання.
- Комфортне опалення – автоматика управляє радіаторами, теплими підлогами й конвекторами. Можуть використовуватися різні сценарії. Розумний Будинок контролює температуру повітря у всіх приміщеннях з використанням щаблів нагрівання:
- У спальній не повинне бути занадто пекуче, а у ванною же, навпаки, тепло вітається;
- У коридорах опалення не потрібно взагалі, а у вітальні хотілося б затишного тепла при перегляді улюбленого фільму або прийомі гостей;
- Кожну із цих температур протягом дня можна змінити.
- Вентиляція – контроль і регулювання подачі повітря, температури. Включення у використовуваному на даний момент приміщенні, відключення при від'їзді.
- Контроль вологості – автоматика управляє погодженою роботою повлажнювачів і вентиляційної системи. Підтримується комфортний рівень вологості в кожному приміщенні.

Заощаджуйте з комфортом

З Розумним Будинком завжди комфортно. Ви часто буваєте відсутні у будинку, наприклад, у будні дні або буваєте тільки по вечорах? «Розумна» електропроводка сама розпорядиться роботою кліматичної техніки – перемкнеться з економічного робочого

режиму на звичайний до Вашого приходу. Досить указати системі чого Ви бажаєте через мобільний телефон, комп'ютер, iPad або iPhone. І до Вашого приїзду все буде готово. Розумний Будинок дозволить Вам заощаджувати витрати на енергоресурси до 40%.

Управління освітленням і електроживленням

Робота всіх домашніх приладів залежить від безперебійності й безвідмовності електромережі. Система Розумний Будинок проконтролює й оптимально розподілить навантаження всієї мережі. Це дозволить продовжити термін служби електроприладів, а також заощадити грошові витрати на електроенергію. «Інтелект» системи відключить прилади, які тимчасово не використовуються (вимикачі, розетки, тепла підлога) або, коли надійде сигнал «перевантаження» мережі.

Їсти можливість плавно міняти напругу в мережі, тим самим регулювати рівень освітлення приміщень. Система сама виконує заздалегідь передбачені світлові сценарії – Вечір, Вечеря, Збирання, Перегляд кіно, Чергове освітлення й т.д. Можна групувати в такі сцени будь-яку комбінацію світильників, ролети й навіть вентиляцію або кондиціювання.

Які бувають системи управління освітленням

Залежно від комплектації й призначення, системи управління світлом розділяються на дві категорії – локальні й глобальні.

– У першому випадку, здійснюється локальне управління світловими приладами в окремо взятому приміщенні або кімнаті. Їхнє використання є найбільш актуальним для таких видів приміщень, де кожна з кімнат виконує різну функцію. Особливо це стосується комерційного сегмента, тому локальні моделі активно використовують у салонах, магазинах, торгових центрах, офісних приміщеннях, і т.д.

– Що ж стосується глобальної системи управління освітленням, то установка даного встаткування в Розумний Будинок має на увазі комплексну інтеграцію датчиків в усі джерела світла. Інакше кажучи, абсолютно весь набір освітлювальних приладів, включаючи навіть вуличні ліхтарі й підсвічування в шафах-купе, буде управлятися за допомогою єдиної й зручної панелі управління.

Систему управління освітленням у Розумному Будинку можна синхронізувати з іншими видами встаткування. Одним з найбільш популярних видів синхронізації є об'їдання систем для штучного й природного світла. Наприклад, можна об'єднати роботу даного встаткування з автоматизованими шторами або жалюзі. При цьому, якщо на вулиці стає темно, Розумний Будинок самостійно закриє вікна й вмикає світло.

Що вміє система управління світлом

Можливості Розумного Будинку дозволяють управляти:

– енергопостачанням – перемикання приладів в ощадливий режим енергоспоживання (день/ніч, зима/літо), зниження витрат на електроенергію до 30%; окремі енергозберігаючі системи не потрібні;

– освітленням у всіх приміщеннях – розбивка освітлення на кілька груп, дистанційне управління світлом у всьому будинку з будь-якої кімнати;

– освітленням залежно від пори року й доби – автоматичне включення освітлення з настанням темряви, залежно від ступеня яскравості зовнішнього освітлення (за межами будинку) плавно міняється рівень підсвічування внутрішнього;

– «прохідними» зонами – використовуються датчики руху для освітлення; світло ввімкнеться/виключиться у випадку появи/відсутності людини в «прохідній» зоні, програмувальний сценарій передбачає поводження системи освітлення;

– світловими сценаріями – при різних умовах регулюється освітлення усередині приміщення, наприклад, сценарій «Перегляд кіно» виконує приглушення світла в кімнаті;

– освітленням поза будинком – світлові сценарії підсвічування доріжок, фасаду будинку, саду залежно від умов;

– світлодіодним освітленням – імітація заходу / сходу в будинку. Можна вибрати будь-який колір і відтінок для освітлення й поміняти його через п'ять мінут, приміром, для роботи – холодні, для відпочинку – теплі тони.

Можливості, якими наділена система управління світлом, на цьому не обмежуються, оскільки вона також може:

– організувати світловий супровід – вирішує проблему нічного пересування по будинку, плавне наростання освітленості в зоні до необхідного рівня залежно від часу доби;

– забезпечити безперебійність електроживлення – резервні джерела електроживлення дозволять працювати безвідмовно всім приладам «Розумного будинку» у звичайному режимі;

– відключати частину електромережі – при перевантаженні всієї мережі частина електромережі може бути знеструмлена залежно від пріоритету щоб найбільш пріоритетна могла нормально функціонувати;

– стабілізувати напругу в електромережі – робота всіх електроприладів у будинку триває поза залежністю від перепаду напруги в мережі, що дозволяє при будь-якій якості енергопостачання працювати приладам у безпечному й стабільному режимі.

Дистанційне й автоматичне управління освітленням

Ваш Розумний Будинок проконтролює роботу всієї електропроводки. При бажанні Ви завжди можете відключити автоматику й перейти на ручне управління. Ви можете управляти світлом у Вашому будинку, квартирі або офісі дистанційно за допомогою пульта або єдиної панелі управління.

При цьому, вам необов'язково перебуває в приміщенні, оскільки робота системи управління освітленням може контролюватися й управлятися за допомогою звичайного мобільного телефону. Тепер, відіславши звичайне sms-повідомлення на спеціальний номер, Ви зможете включити / виключити світло в будинку, або перевести його в енергозберігаючий режим.

У процесі установки, наші фахівці заберуть старі вимикачі із всіх кімнат і замінять їх на єдину панель управління, що буде оснащена кнопковою або сенсорною клавіатурою.

Можливості панелі управління світлом:

– Кожна кнопка має від однієї до трьох функцій, які можуть бути запрограмовані відповідно до ваших побажань.

– Можливість активації ефектів наростання, загасання або затримки яскравості.

– Адаптивне визначення ступеня освітлення залежно від погодних умов і часу доби.

– Індивідуальне налаштування світлового встаткування для кожної з кімнат.

– Активація режиму «ефект присутності», що буде імітувати Ваше перебування в будинку.

– Включення / вимикання освітлення перед вашим приходом і після вашого відходу.

Із системою Мультирум Ваш Будинок справжній центр розваг

Включите телевізор і цілий будинок як на долоні...

Ви можете дивитися свою улюблену програму й одночасно стежити за тим, що відбувається у Вашім будинку. Тут видно гостюючи у входу, Ви спостерігаєте за дітьми в їхній кімнаті, перегортаєте архів фільмів і сімейних фотографій. Усе в одному місці, на центральному сховищі. Забудьте про купу дисків або пультів дистанційного управління, зараз пульт один.

Інтегрована в Розумний Будинок Мультирум система відкриває нові можливості. Тепер Ваш будинок може виконувати мультимедійні функції. Ви можете створювати трохи аудіо- або відео- зон. Управляти так просто. Одним натисканням включаються всі прилади – наприклад, телевізор і підсилювач, опускаються жалюзі й освітлення для перегляду фільмів готово.

Насолоджуйтеся, розважайтеся де завгодно разом з Multiroom

Тепер будь-яку кімнату для сімейного дозвілля й розваги вибрати так швидко й легко. Зручно розташовуйтеся й насолоджуйтеся розкішним почуттям, що Ви можете включити фільм у спальні, музику на кухні й у той же самий час перевірити, яку програму зараз переглядають Ваші діти.

Управляти системою Мультирум – одна насолода. З одного місця можна контролювати всі підключені зони. У будь-якій кімнаті можна підключитися до загального архіву фотографій, фільмів або музики й навіть до системи відеоспостереження.

Multiroom – що це?

Система Multiroom – це сучасна, багатофункціональна технологія по розподілі звукових і відеосигналів, що дозволить вам слухати музику й насолоджуватися переглядом будь-яких телепередач у кожній з кімнат Вашого будинку.

Вся аудіо- і відео- техніка розташовується в одній точці Вашого будинку. Джерела мультимедіа підключаються до спеціального пристрою, що є комунікатором всіх зон, де планується виводити музику й відео-зображення. Джерелами можуть бути IPad, DVD, TV-тюнер та інші пристрої. Тут виключається необхідність у всіх кімнатах установлювати апаратуру, програвачі, підсилювачі, проведення та інше. Сигнали з Мультирум транслюються в усі кімнати, які підключені по спеціальних каналах. У кожній підключеній кімнаті надається доступ до центрального сховища всього відео й аудіо.

Із чого складається система Multiroom:

- Комутатор матричного типу, що здатний приймати й передавати сигнали.
- Пульт для дистанційного управління.
- Потужні акустичні підсилювачі.
- Сенсорні настінні панелі управління.
- Функції системи Multiroom:
- Автоматизоване централізоване постачання звуком всіх кімнат з індивідуальним джерелом і рівнем гучності.
- Постачання відеосигналом всіх кімнат.
- Єдине сховище аудіо- і відео- даних на CD, DVD, HDD.
- Функція оповіщення й аудіо-зв'язку всіх кімнат.
- Звуковий супровід при переході з кімнати в кімнату.
- Озвучування спецприміщень – лазня, сауна, сад, басейн і т.д.

Як працює Мультирум система?

Працюючих по черзі або одночасно джерел аудіо й відео можуть бути один або трохи. За допомогою регулятора звуку можна моделювати рівень гучності як в одній кімнаті так і у всіх відразу. Управління системою Мультирум є досить комфортним і простим. Вам більше не знадобляться безліч пультів для управління радіо, телевізором, і різних домашніх плеєрів. Усе спрощується панеллю управління або портативним сенсорним дисплеєм, за допомогою яких Ви зможете управляти системою з будь-якого місця в будинку.

Переходячи з кімнати в кімнату Ви можете без переривання слухати улюблену музику в ідеальній якості й з однаковою гучністю, начебто Ви перебуваєте в тому самому приміщенні. А Ваш улюблений серіал або фільм піде за Вами й система автоматично перемкне звук і відео в іншу кімнату. Система Мультирум продовжить відтворення мультимедіа з того самого моменту, на якому Ви зупинилися.

А що ще вміє система Мультирум?

Системи Мультирум широко застосовні не тільки в будинках, квартирах, вона користується своєю популярністю в об'єктах комерційного типу – барах, ресторанах, кафе, фітнес-центрах, офісах, торговельних площах. Багатофункціональність системи включає також можливість інтеграції із системами безпеки. За допомогою панелі управління Ви легко зможете виводити зображення на екран телевізора, монітор з камер відео^-спостереження. Мультирумна система може використовуватися як джерело зв'язку по всьому будинку. Це

дуже зручно, коли в будинку є діти. Система Multiroom – це система Вашої безпеки й життєзабезпечення.

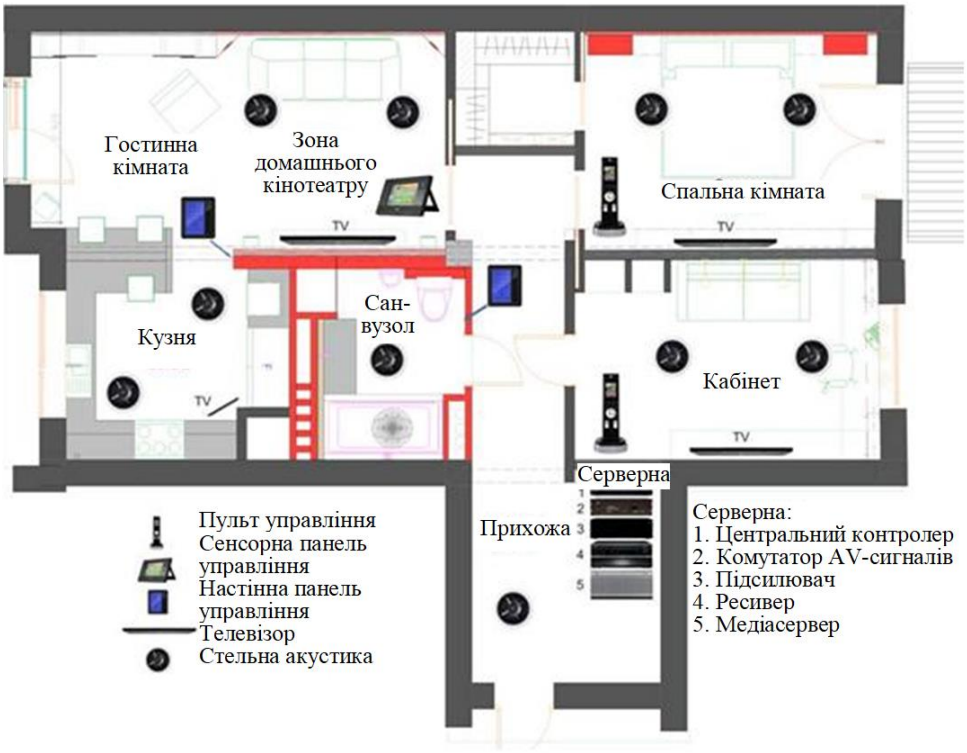


Рисунок 1 – Структурна схема системи

Економія – приємний бонус

Мультирум система – це не тільки ідеальна якість звуку й відео у Вашім Будинку. Із цією системою Вам не знадобиться витрачати додаткові гроші на покупку аудіо- і відео-апаратури для всіх кімнат. Тут досить одного комплекту спеціалізованого встаткування. І все готово. З Мультирум системою витрати на апаратуру зменшуються в рази, при цьому якість звуку й відео як у професійній студії. Тепер Ваш будинок звучить по-новому.

Управління воротами, шторами, жалюзі

Система Розумний Будинок дозволяє контролювати й управляти роботою всіх механізмів у Вашім будинку – воротами, шлагбаумами, шторами, жалюзі й іншим. Автоматизоване управління має ряд істотних переваг перед звичайними механізмами. Вагома перевага – можливість дистанційного контролю, управління системою на відстані. Це особливо важливо для тих випадків, коли вікна в приміщенні перебувають занадто високо або доступ до них перекритий меблями.

Багатофункціональна система управління механізмами в будинку (квартирі, офісі, виробництві) стає усе більше популярної й затребуваної на сьогоднішній день. За допомогою спеціалізованого пульта управління Ви зможете легко відкривати або закривати жалюзі, вікна, ворота, двері. Така система вже давно стала основний для більшості будинків, квартир і офісних приміщень у США і Європі, а тепер вона доступна й нам.

Автоматика Розумного Будинку дозволяє здійснювати:

– Управління воротами, вікнами, шлагбаумами, дверима.
– Управління шторами, жалюзі, ролетами, портьєрами.
– Управління телевізорами, відеопроекторами, екранами.
– Управління меблями й окремими предметами інтер'єра.

Розумна автоматика, фурнітура, приводи можуть інтегруватися в механізовані елементи (предмети побуту) Вашого будинку можуть і працювати спільно із системою Розумний Будинок. Ви з легкістю зможете ними управляти в будь-який час і з будь-якого зручного для Вас місця через пульт управління або панель, комп'ютер і навіть телефон.

Автоматичні штори, ролети, жалюзі й управління ними

У вашім будинку багато кімнат? Скільки часу Ви витрачаєте на закриття й відкриття важких портьєр або жалюзі? Бувають випадки коли Ви забуваєте пр відкритий рольставнях коли Вас немає будинку?

З Розумним Будинком Вам не прийде відволікатися від важливих справ, докладати зусиль і витрачати час на управління механізмами. У кімнатах завжди буде підтримуватися необхідний рівень освітлення поза залежністю від часу доби. Світить занадто яскраво сонце – штори автоматично закриються. Ви виїхали у відрядження й Ваш будинок буде імітувати Вашу присутність, захищаючись від зловмисників – рольставні відповідно до заданого сценарію будуть закриватися й відкриватися. Ваш будинок привітає Вас ранковим сонцем, відкривши штори. Подобається проводити сімейне дозвілля в домашньому кінотеатрі? Запрограмуйте заздалегідь сценарії і як тільки Ви зберетеся в кінозалі, начебто за бажанням, приглушить світло, закриються штори або жалюзі над вікнами.

Робота автоматики базується на датчиках, убудованих у карнизи. Виконавчі команди передаються через панель управління й система розпоряджається роботою модуля відповідно до зазначених умов.

Система здатна автоматично контролювати доступ сонячного світла в приміщення залежно від часу доби й погодних умов, закривати все жалюзі в будинку при постановці його на сигналізацію, забезпечувати оптимальні умови для знаходження в приміщенні.

Система автоматичного управління шторами, жалюзі й ролетами досить популярна не тільки в приватних будинках, квартирах, котеджах. Вона прекрасно підходить для офісу. Це дозволяє створити найбільш сприятливі робочі умови й заощадити час на користь продуктивності співробітників, не відволікаючи їх від роботи.

Автоматика для воріт, дверей, шлагбаумів і управління ними

Дистанційне управління воротами – дозволяє повністю автоматизувати процес відкривання й закривання воріт, шлагбаумів. Завдяки своїй універсальності, автоматизована система оптимально підходить для використання в котеджах, приватних будинках, дачах, а також на різних промислових і виробничих об'єктах.

Автоматика для воріт складається із блоку управління й датчиків з фотоелементами. Також додається пульт, за допомогою якого здійснюється дистанційне управління воротами.

При натисканні на певну кнопку на пульті, автоматика воріт приймає сигнал, після чого виконує відповідну команду.

Головним завданням фурнітури для воріт є запобігання можливості контакту стулок із що в'їжджає або виїжджає автотранспортом. Датчики встановлюються на відстані 30 – 90 див від поверхні землі й спрацьовують у той момент, коли на шляху воріт, що закриваються, перебуває яка-небудь перешкода – автомобіль, люди, тварини й т.д. При цьому, процес закриття / відкриття воріт, шлагбаума автоматично припиняється доти, поки перешкода не буде прибрано.

Управління предметами інтер'єра, меблями, проекторами й не тільки

Система дуже зручна у використанні, коли у Вашім будинку присутні дизайнерські задуми, доповнити які можна механізованим переміщенням різних предметів меблів і інтер'єра. Це не тільки стильно й неповторно, але й дуже практично. Наприклад, бар, що піднімається з журнального столика, розсувні дверцята, захований у стіні книжкову шафу дозволять сховати від очей «не вписується» в інтер'єр функціонал, але й істотно заощадити місце в приміщенні, розширити його візуально.

Розумний Будинок може управляти:

– Плазменними панелями, моніторами й РК-телевізорами – маскування в меблях, предметах інтер'єра, стінах, стелі.

– Відеопроекторами – при необхідності для перегляду відео переміщення в робоче положення, приховання в стелі, в елементах декору.

– Комп'ютерними моніторами, робітниками місцями – всі робітники елементи розміщаються в спеціальних ліфтах робочих столів, столах засідань, кабінетах керівників.

– Робочим устаткуванням на кухні, технікою у ванній кімнаті – маскування техніки під / у робочих поверхнях.

Головне завдання автоматизації управління механізмами – трансформувати кімнати будинку (квартири, офісу) коли Вам це необхідно. Наприклад, перетворювати гостинну кімнату в домашній кінотеатр і навпаки. Інженерні рішення сполучають гармонію, практичність і комфорт інтер'єра.

Основні переваги системи:

– Зручність користування.
– Багатофункціональність.
– Можливість програмування системи.
– Дистанційне управління.
– Простота в роботі й обслуговуванні.

Висновок. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів IoT з використанням Bluetooth 5. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем IoT з використанням Bluetooth 5; Досліджена система IoT з використанням Bluetooth 5; На основі отриманих результатів досліджень створена програмна реалізація системи IoT з використанням Bluetooth 5. Розроблені під час виконання роботи алгоритми дозволяють успішно вирішувати завдання IoT з використанням Bluetooth 5. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Босько В.В. Анализ и сравнительное исследование перспективных направлений развития цифровых телекоммуникационных систем и сетей / Смирнов А.А., Босько В.В., Мелешко Е.В. // Системи обробки інформації. – Х.: ХУ ПС, 2008. – Вип.7(74). – С.120-123.
2. Босько В.В. Разработка методики оценки середнего времени обслуживания информационных пакетов в телекоммуникационной сети / Смирнов А.А., Босько В.В., Мелешко Е.В. // Системи управління, навігації та зв'язку. – Київ: ДП «Центральний науково-дослідний інститут навігації і управління», 2009. – Вип. 2(10). – С.162-165.
3. Босько В.В. Разработка математической модели процесса динамического управления маршрутизацией данных в телекоммуникационной сети / Смирнов А.А., Босько В.В. // Системи управління, навігації та зв'язку. – К.: ДП «ЦНДІ навігації і управління», 2009. – Вип. 3(11). – С.208-210.
4. Босько В.В. Разработка метода определения оптимального множества путей передачи информации в телекоммуникационной сети / Смирнов А.А., Босько В.В. // Збірник наукових праць. – Х.: ХУПС, 2009. – Вип. 3(21). – С.102-108.
5. В.В. Босько. Разработка метода прогнозирования поведения информационного потока в телекоммуникационной сети // Збірник наукових праць. Харківського університету Повітряних Сил: – Х.:ХУ ПС, – 2010.-Вип. 3 (25) .- С.126-130.
6. Босько В.В. Исследование особенностей построения современных телекоммуникационных систем и сетей / Смирнов А.А., Босько В.В. // Проблемы информатики и моделирования. Материалы восьмой международной научно-технической конференции 26-28 ноября. – Х.: НТУ "ХПИ", 2008. – С.54.
7. Босько В.В. Исследование влияния времени мониторинга телекоммуникационной сети на точность прогнозирования поведения трафика / Смирнов А.А., Босько В.В. // Перша міжнародна науково-практична конференція "Проблеми й перспективи розвитку IT-індустрії" м. Харків , 18-19 листопада 2009р. – С.198-200.
8. Босько В.В. Анализ математических моделей телекоммуникационной сети / Смирнов А.А., Босько В.В. // Проблемы информатики и моделирования. Материалы девятой международной научно-технической конференции 26-28 ноября. – Х.: НТУ "ХПИ", 2009. – С.52-53.
9. Босько В.В. Метод повышения оперативности передачи данных в телекоммуникационной сети / Смирнов А.А., Босько В.В. // Збірник тез доповідей науково-практичної конференції "Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку" 24-25 березня. – Х.: АВВ МВС України, 2010. – С.54.

10. Босько В.В. Динамическое управление процессом маршрутизации данных в телекоммуникационной сети / Смирнов А.А., Босько В.В. // Тези доповідей Міжнародної науково-практичної конференції м. Вінниця, Україна 19-21 травня 2010 року. – Вінниця: ВНТУ, 2010. – С.231-232.
11. Можаєв О.О. Часова прозорість мережі, як характеристика, що визначає виконання необхідної якості обслуговування / О.О. Можаєв, О.Д. Анохіна, С.Ю. Гайдаров, С.Г. Семенов // Системи обробки інформації. – Х.: ХВУ, 2004. – Вип. 11(39). – С.133-139.

УДК 004

А. Бажан, магістр гр. КН-18МЗ
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ УПРАВЛІННЯ ВЕБ-САЙТОМ ДЛЯ ВИВЧЕННЯ ІНОЗЕМНИХ МОВ

У статті розроблено програмне забезпечення, яке призначено для реалізації системи управління веб-сайтом для вивчення іноземних мов. Метою розробки є дослідження та програмна реалізація системи управління веб-сайтом для вивчення іноземних мов. Об'єктом дослідження є процес інтерактивного вивчення іноземних мов за допомогою веб-ресурсів. Предметом дослідження є методи та алгоритми автоматизації системи вправ для вивчення іноземних мов за допомогою веб-ресурсів. Методи дослідження базуються на теорії об'єктно-орієнтованого програмування, теорії алгоритмів, теорії комп'ютерної лінгвістики, а також теорії математичної статистики. Результат роботи – програмна реалізація інтерактивних вправ для вивчення іноземних мов за допомогою веб-ресурсу. В процесі роботи над програмною моделлю виконано аналіз існуючих алгоритмів та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

комп'ютерні науки, вивчення іноземних мов, інтерактивні вправи, веб-сайти

Постановка проблеми. Знання іноземних мов, зокрема англійської є досить важливим у наш час. Для Вивчення будь-якої мови необхідно запам'ятовувати багато інформації, наприклад, слів, правил, тощо. Багаторазове проходження інтерактивних вправ значно полегшує даний процес. Тому розробка веб-ресурсів, які надають можливість проходження таких інтерактивних вправ та відслідковування прогресу користувачів є актуальною задачею.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні управління веб-сайтом для вивчення іноземних мов.

Мета й завдання дослідження. Метою роботи є дослідження, розробка та реалізація алгоритмів та методів системи управління веб-сайтом для вивчення іноземних мов.

Для досягнення поставленої мети в роботі вирішувалися наступні завдання:

– огляд та аналіз існуючих рішень в даній області досліджень на даний момент;
– реалізація усіх необхідних функцій в програмі для забезпечення поставленої мети;
– спрощення програмного продукту для зручності використання.

Об'єктом дослідження є процес інтерактивного вивчення іноземних мов за допомогою веб-ресурсів.

Предметом дослідження є методи та алгоритми автоматизації системи вправ для вивчення іноземних мов за допомогою веб-ресурсів.

Методи дослідження базуються на теорії об'єктно-орієнтованого програмування, теорії алгоритмів, теорії комп'ютерної лінгвістики, а також теорії математичної статистики.

Виклад основного матеріалу. Виходячи з теми роботи потрібно розробити програмне забезпечення системи управління сайтом для дистанційного вивчення іноземної

мови. Ідея розроблюваного програмного забезпечення – створити простий у використанні, легкий і цікавий у навчанні сайт для вивчення англійської мови.

Після проведення огляду існуючих систем та аналогів було прийнято рішення створити невеликий сайт для вивчення англійської мови за допомогою цікавих та ефективних вправ.

Для того щоб система ідентифікувала кожного користувача та відображала інформацію конкретно для нього було вирішено створити сторінку реєстрації користувача. Для реєстрації користувач повинен надати свій бажаний логін, E-mail та пароль.

Так як сайт матиме багато користувачів потрібно створити базу даних для сайту з таблицею, яка міститиме інформацію про акаунт користувача. Наведемо структуру даної таблиці:

– ID – ідентифікатор користувача;
– UserName – логін користувача;
– Password – пароль користувача;
– Email – E-mail користувача;
– Active – флаг активації акаунта.

Ця таблиця надасть можливість зробити перевірку на зайнятий логін або E-mail “на льоту”. Тобто за допомогою JavaScript та бібліотеки jQuery можна створити обробник натиснення будь-якої клавіши у полях, відведених для введення логіну на E-mail’у, а потім за допомогою технології AJAX створити запит до таблиці з вже зареєстрованими користувачами у БД та перевірити наявність в ній введених даних користувачем. Якщо хоча б один з об’єктів введених користувачем вже зайнятий, то йому можна вивести повідомлення “на льоту”, що введений ним логін або E-mail вже зайнятий. Такі речі перетворюють та налагоджують взаємозв’язок між користувачем та сайтом, що робить користування сайтом приємнішим.

Для перевірки достовірності введених даних користувачем було прийнято рішення зробити підтвердження реєстрації через E-mail. Тобто після введення всіх даних і натиснення кнопки реєстрація потрібно надіслати листа на пошту користувача з посиланням на деяку сторінку на сайті, яка буде перевіряти зміст цього посилання і, або активувати акаунт користувача, або повідомляти про помилку. Але для цього потрібно створити ще одну таблицю для збереження відповідних даних про користувача та активацію його акаунта. Структуру даної таблиці наведено нижче:

– UserID – ідентифікатор користувача для реєстрації;
– SecureKey – код активації акаунта;
– Email – E-mail користувача;
– RegConfirm – флаг підтвердження реєстрації;
– ChangePass – флаг зміни паролю акаунта.

Якщо на сайті існує сторінка реєстрації, то повинна бути і сторінка авторизації користувача, на якій користувач матиме змогу авторизуватись шляхом введення свого логіну та паролю. Далі система повинна перевірити введені дані з таблицею користувачів у БД та, або авторизувати користувача, надавши йому право на перегляд закритої інформації на сайті, або вивести повідомлення про помилку.

Після перегляду аналогів програмного забезпечення системи управління сайтом було вирішено створити мінімальний, простий та зрозумілий інтерфейс користувача, який включатиме в себе 3-4 кольори: чорний, тілесний колір, світло-синій та білий.

Також було вирішено створити так звані “хедер” (від англ. – header) та “футер” (від англ. – footer), які будуть мати простий дизайн та будуть відображатися на всіх сторінках сайту. “Хедер” та “футер” представлятимуть собою блоки даних, які будуть знаходитись відповідно вгорі та внизу сторінки. Цікавим рішенням було інтегрувати сторінку авторизації та виходу з профілю користувача у “хедер” у вигляді кнопки, при натисненні на яку буде відображатись діалогове вікно, в якому міститимуться поля для авторизації.

Так як на сайт будуть заходити користувачі з різних країн світу, було прийнято

рішення зробити сайт мультимовним, тобто зробити можливість зміни мови інтерфейсу сайту. Це можна реалізувати у вигляді кнопки у “хедері”, при натисненні на яку буде відображатись діалогове вікно зі списком різним мов, при натисненні на будь-яку з них сайт автоматично змінював мову свого інтерфейсу.

Для реалізації цієї задачі було вирішено створити файл у форматі JSON, який міститиме усі слова та фрази, які можна зустріти на сайті на різних мовах. Тоді при натисненні на будь-яку мову можна завантажити слова з даного файлу для обраної мови з подальшим виведенням отриманих слів у відповідні блоки сторінки.

Як і будь-який інший сайт розроблюване програмне забезпечення потребує навігаційного меню, за допомогою якого користувач зможе переходити до інших сторінок веб-сайту. Навігаційне меню було вирішено також приєднати до “хедера” сторінки для зручної навігації по сайту. Це меню представлятиме собою список з посиланнями на такі сторінки:

– головна - головна сторінка сайту, на якій користувач знайомитимется з деякою інформацією про веб-сайт та його можливостями;

– мої тренування - сторінка з тренуваннями для вивчення англійської мови;

– контакти - сторінка відображення контактів розробника програмного забезпечення системи управління сайтом, та форму зворотнього зв'язку;

– про нас – сторінка відображення інформації про розробника сайту.

На головній сторінці сайту було вирішено помістити слайдер із зображеннями частин сайту, тренувань та зображень по тематиці вивчення англійської мови, а також блок з інформацією, яка приваблювала увагу користувачів на реєстрації нового акаунта та проходження тренувань.

На сторінці “мої тренування” користувач зможе спостерігати різні тренування для поліпшення своїх знань з англійської мови. Але для того, щоб проходити будь-яке тренування він повинен обрати набір слів для вивчення. Тому було вирішено створити сторінку з наборами слів на будь-яку тематику, які з містили від 10 до 80 або більше слів відповідної тематики.

Так як наборів може бути дуже багато потрібно створити нову таблицю у базі даних для збереження інформацію про набори слів, а також створити нову таблицю в БД для збереження інформації про англійські слова, їх переклад, транскрипцію, зображення слова та звукового файлу. Наведемо структуру цих двох таблиць. Таблиця наборів:

– ID – ідентифікатор категорії;

– NameUA – назву категорії на українській мові;

– NameUK – назву категорії на англійській мові;

– NameRU – назву категорії на російській мові;

– WordsCount – кількість слів у наборі;

– Image – зображення набору.

Таблиця слів для наборів:

– ID – ідентифікатор слова;

– CollectionID – ідентифікатор категорії, до якої належить слово;

– Word – слово на англійській мові;

– TranslateUA – переклад слова на українську мову;

– TranslateRU – переклад слова на російську мову;

– Transcription – транскрипція слова;

– Image – зображення слова;

– Sound – шлях до файлу зі звуком слова.

У верхній частині сторінки “мої тренування” знаходитимется інформація про обраний набір слів, якщо його ще не обрано, на його місці буде знаходитись посилання на сторінку вибору наборів слів та посилання на форму завантаження слів із файлу. Так як користувач може забажати вивчити свої слова, яких немає у жодному з наборів або просто вивчити слова з якої-небудь книжки або статті, він може завантажити слова з файлу, з яких потім

створиться набір слів, який буде відображений тільки цьому користувачеві.

На сторінці “мої тренування” після вибору набору слів користувач має змогу обрати одне з тренувань для підвищення свого рівня знань англійської мови. На сторінці надано наступні тренування: слово-переклад, переклад-слово, вірно / невірно, конструктор слів та аудіювання. Для того, щоб зберігати інформацію про кожне пройдене тренування для кожного користувача було прийнято рішення створити таблицю в БД, яка міститиме всі ці дані. Структуру таблиці для збереження інформації про тренування зображено нижче:

– UserID – ідентифікатор користувача для якого потрібно зберігати інформацію про тренування;

– ActiveCollections – рядок в якому перелічені ідентифікатори наборів слів, які користувач обрав собі для вивчення;

– CollectionStarted – рядок типу JSON вигляду:

```
{ "word_tr": {"Weather":"0","Flowers":"1"},
  "tr_word": {"Weather":"1","Flowers":"1"},
  "truefalse": {"Weather":"0","Flowers":"0"},
  "construct": {"Weather":"0","Flowers":"0"},
  "listening": {"Weather":"0","Flowers":"0"}
}
```

який міститиме інформацію про те, що обране користувачем тренування з відповідним набором слів було розпочато або ні;

– ReshuffledWords – рядок типу JSON вигляду:

```
{ "word_tr":{"Weather":{"position":"0","words":[]},
            "Flowers":{"position":"0","words":[]}
           },
  "tr_word":{"Weather":{"position":"0","words":[]},
            "Flowers":{"position":"18","words":[]}
  }, ...
            }
```

який міститиме інформацію про поточну позицію слова у обраному тренуванні з відповідним набором слів;

– Progress – рядок типу JSON вигляду:

```
{ "word_tr": {"Weather":{"positive":"0","history":[]},
             "Flowers":{"positive":"0","history":[]}
             }, ...
}
```

який міститиме інформацію про прогресс тренування з відповідним набором слів та правильні та неправильні відповіді користувача до тренування.

Розглянемо кожне з них окремо та алгоритми їх роботи.

1. Слово-переклад

Опис вправи: користувачеві надається слово англійською мовою, та 5 варіантів перекладу його на російську або українську мови, дивлячись на обрану мову інтерфейсу сайту. Також при кожному новому слову броузер відтворює дане слово для того, щоб користувач сприймав його на слух. Завдання користувача – обрати зі списку варіантів правильний переклад наданого англійського слова. Цей процес проходить доки не буде пройдено усі слова, а потім буде відображено таблицю результатів даного тренування.

Теоретична реалізація тренування

На початку тренування система отримує набір слів, який користувач обрав та перевіряє у БД інформацію, чи проходив даний користувач це тренування з обраним набором слів, чи ні. Якщо ні, то система бере набір слів, перемішує його та бере перше слово з цього набору, його переклад обраною мовою, зображення та звук. Далі обирає два будь-яких переклада слів з цього ж набору і ще два переклада слів з усіх інших наборів. Далі на екрані відображається англійське слово, варіанти його перекладу та лунає звук англійського слова.

Коли користувач обирає один з варіантів система виводить зображення англійського слова на екран та перевіряє англійське слово обраного користувачем варіанта з англійським словом на екрані і якщо вони співпадають, то користувачу зараховується дане слово, виконується оновлення інформації в БД про теперішню позицію слова та перехід до наступного слова. Якщо ж користувач обрав невірний варіант, то система підсвічує правильний варіант, не зараховує слово як правильне, виконує оновлення інформації в БД про теперішню позицію слова та переходить до наступного слова. Цей процес триває доти, доки усі слова з набору не буде пройдено. Коли слова в наборі закінчились на екран виводиться інформація про кількість правильних слів, та список усіх слів в якому слова, на які користувач відповів правильно, відображені зеленим кольором, а на неправильні – червоним. Далі користувач має змогу повторити тренування або перейти до списку вибору нового тренування чи набору слів.

Якщо ж користувач вже проходив дане тренування з обраним набором слів, то спочатку система бере інформацію про теперішню позицію слова в наборі, а також весь набір перемішаних слів і продовжує процес так само як викладено вище, але вже не з першого слова, а з позиції, яка була вказана в БД. Таким чином користувач не повинен проходити тренування до кінця за один раз.

2. Переклад-слово

Дане тренування аналогічне до попереднього за винятком того, що тут користувачу надається вже не англійське слово, а його переклад на російську або українську мову, відповідно до обраної мови інтерфейсу сайту. А у варіантах до цього слова надає їх англійський переклад.

3. Вірно / невірно

Опис вправи: користувачу надається слово англійською мовою та з 50% вірогідністю переклад, або цього ж слова на російську або українську мову, або будь-якого іншого слова. Завдання користувача натиснути на кнопку вірно або невірно виходячи з наведених слів. Після проходження усіх слів користувачу надається інформація про результати тренування.

Теоретична реалізація тренування

Спочатку потрібно перевірити чи проходив вже користувач дане тренування з обраним набором слів. Якщо ні, то тренування починається з першого слова, якщо ж так, то теперішня позиція слова в наборі береться з БД. Далі система виводить англійське слово за вказаною позицією в наборі, та з 50% вірогідністю його переклад або переклад будь-якого іншого слова. При натисненні на кноку вірно або невірно, система перевіряє ці два слова, якщо англійське слово і його переклад співпадають і користувач натиснув клавішу вірно, програма зараховує дане слово і переходить до іншого. Якщо ж англійське слово і його переклад не співпадають і користувач натиснув кнопку невірно, то програма теж зараховує дане слово і переходить до іншого. В усіх інших випадках програма не зараховує слово і переходить до іншого слова за наступною позицією. Кожен раз перед завантаженням нового слова програма виконує оновлення інформації в БД про теперішню позицію слова в наборі, та відповіді користувача. Якщо користувач не виконає тренування до кінця, то він матиме змогу пройти його з того ж місця на якому закінчив.

Після проходження всіх слів на екран виводиться інформація про кількість правильних відповідей та список усіх слів в якому правильні відповіді відображені зеленим кольором, а неправильні – червоним. Далі користувач має змогу повторити тренування або перейти до списку вибору нового тренування чи набору слів.

4. Конструктор слів

Опис вправи: користувачу надається набір англійських букв і поле для їх розміщення. Завдання користувача шляхом натиснення на ці букви почерзі скласти слово на англійській мові. Після проходження усіх слів користувачу надається інформація про результати тренування.

Теоретична реалізація тренування

Спочатку потрібно перевірити чи проходив вже користувач дане тренування з

обраним набором слів. Якщо ні, то тренування починається з першого слова, якщо так, то теперішня позиція слова в наборі береться з БД. Система отримує слово на англійській мові, розбиває його на букви, та виводить їх на екран у відповідні блоки. Коли користувач збирає слово шляхом натиснення на букви, система перевіряє правильність зібраного англійського слова. Якщо слово зібрано правильно, система виконує оновлення інформації в БД про теперішню позицію слова в наборі та переходить до наступного слова, якщо непраильно – система підсвічує ту частину слова починаючи з літери, яка найперша була вибрана неправильно. Далі користувач може перезібрати слово знову. Процес триває доки користувач не збере слово правильно, тоді програма виконає оновлення інформації в БД про теперішню позицію слова в наборі та перейде до наступного слова. Після проходження всіх слів на екран виводиться список усіх слів в яких були допущені помилки та їх кількість відповідно до кількості усіх слів в наборі. Далі користувач має змогу повторити тренування або перейти до списку вибору нового тренування чи набору слів.

5. Аудіювання

Опис вправи: користувачу надається поле для введення тексту та одразу ж лунає звук англійського слова. Завдання користувача написати слово, яке він почув у відповідному полі. Якщо слово написано неправильно – воно не зараховується, інакше – зараховується. Після проходження усіх слів користувачу надається інформація про результати тренування.

Теоретична реалізація тренування.

Спочатку, як завжди, потрібно перевірити чи проходив користувач дане тренування з обраним набором слів. Якщо ні, то тренування починається з першого слова, якщо так до теперішня позиція слова в наборі береться з БД. Далі програма завантажує звук англійського слова за вказаною позицією в наборі та одразу ж відтворює його. Коли користувач введе слово, яке він почув, програма перевірить введене ним слово з англійським словом. Якщо вони співпадуть, то це слово буде зараховано, інакше – ні. Далі система виконає оновлення інформації в БД про теперішню позицію слова в наборі та перейде до наступного слова. Після проходження всіх слів на екран виводиться інформація про кількість правильних слів, та список усіх слів в якому правильні слова відображені зеленим кольором, а неправильні – червоним. Далі користувач має змогу повторити тренування або перейти до списку вибору нового тренування чи набору слів.

Розробка структурної схеми

Структурна схема сайту – це сукупність об’єктів, частин сайту та взаємозв’язки між ними. Вона призначена для відображення загальної структури сайту, тобто його основних блоків, вузлів, частин та головних звя’зків між ними.

Структурну схему розроблюваного сайту зображено на рисунку 3.1.

Зі схеми можна побачити, що сайт має головну сторінку з якої користувач може перейти до сторінки реєстрації, відновлення паролю, сторінки “Про нас”, сторінки контактів, тренувань, профілю користувача та до сторінки адміністративної панелі. Також на головній сторінці користувач може авторизуватись або вийти зі свого акаунта.

З адміністративної панелі користувач може перейти до перегляду або редагування інформації про користувачів, слайдів, які відображаються на головній сторінці, а також до сторінки конфігурації наборів слів для тренувань. Також зі сторінки наборів слів адміністратор сайту може перейти до сторінки додавання нових слів у вже створений набір слів або створити новий.

Зі сторінки тренувань користувач може перейти до сторінки вибору набору слів або до конкретного тренування, якщо набір слів вже вибраний.

Серед базових тренувань на сайті реалізовано:

1. Вправа «Слово - переклад».
2. Вправа «Переклад - слово».
3. Вправа «Вірно/невірно».
4. Вправа «Зібрати слово з літер».
5. Вправа «Аудіювання».

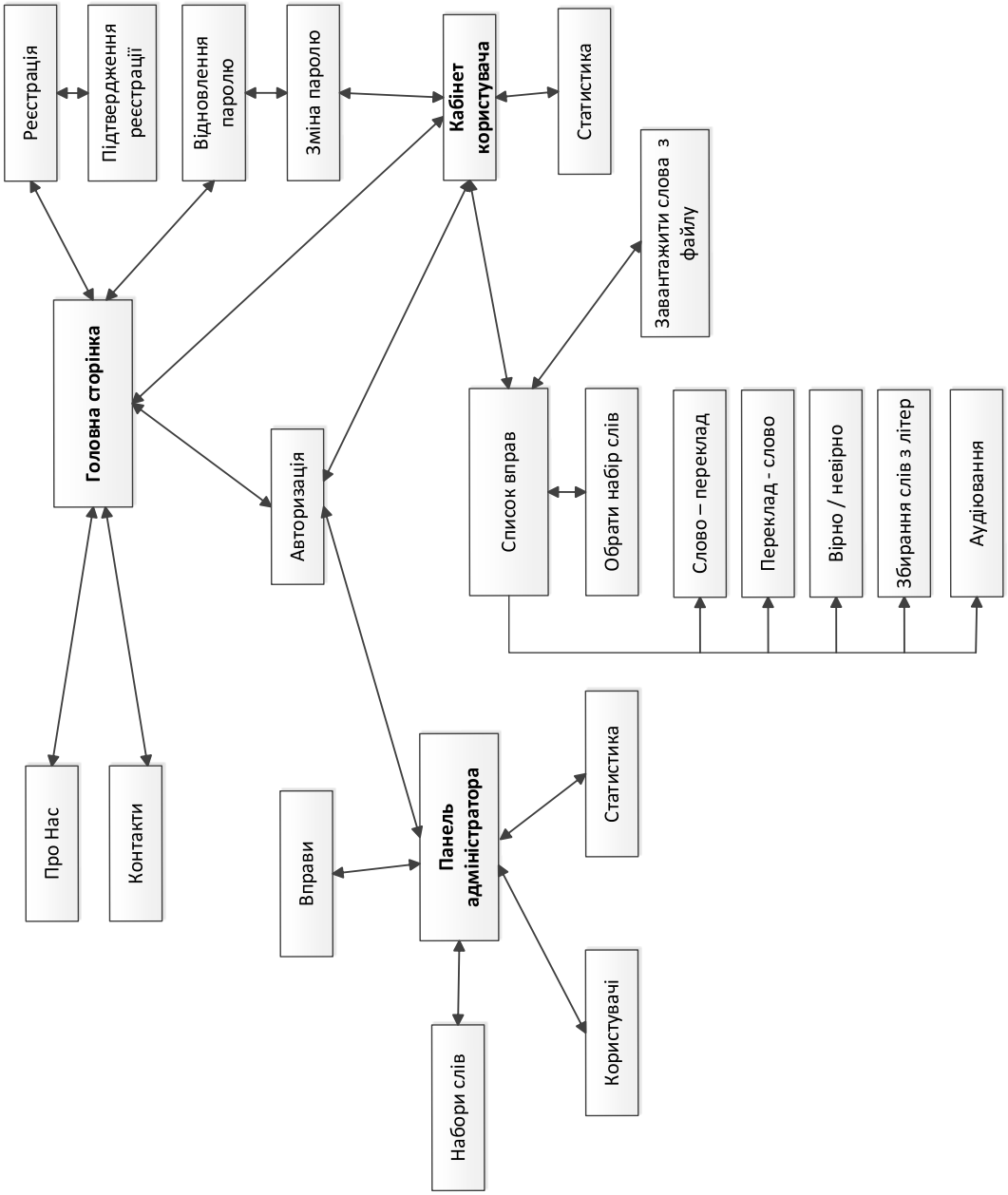


Рисунок 1 – Структурна схема розроблюваного сайту

Висновок. У статті розглянуто та проаналізовано існуючі на даний момент рішення в області інтерактивного вивчення іноземних мов; реалізовано задачу розробки системи управління веб-сайтом для вивчення іноземних мов; реалізовано задачу визначення прогресу користувача системи; створено простий інтуїтивно зрозумілий інтерфейс вітчизняної програми для вивчення іноземних мов.

Список літератури

1. Гаевский А.Ю. 100% самоучитель. Создание Web-страниц и Web-сайтов. HTML и JavaScript / А.Ю. Гаевский, В.А. Романовский. - М.: Триумф, 2015. - 464 с.
2. Зеньковский В.А. 3D-эффекты при создании презентаций, сайтов и рекламных видеороликов / В.А. Зеньковский. - М.: БХВ-Петербург, 2017. - 508 с.
3. Китинг Д. Flash MX. Искусство создания web-сайтов / Китинг, Джоди. - М.: ТИД ДС, 2016. - 848 с.
4. Кузнецов М.В. PHP. Практика создания Web-сайтов / Кузнецов, М.В. и. - М.: БХВ-Петербург, 2015. - 102 с.
5. Снелл Н. Абсолютно ясно о создании Web-страниц и Web-сайтов / Снелл, Нэд. - М.: Триумф, 2015. - 224 с.

6. Хассей Т. WordPress. Создание сайтов для начинающих (+ CD-ROM) / Т. Хассей. - М.: Эксмо, 2016. - 538 с.
7. Андреев А. Е. Дискретная математика: прикладные задачи и сложность алгоритмов : учебник и практикум для академического бакалавриата / А. Е. Андреев, А. А. Болотов, К. В. Коляда, А. Б. Фролов. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2019. — 317 с.
8. Аверина, Т. А. Численные методы. Верификация алгоритмов решения систем со случайной структурой : учебное пособие для вузов / Т. А. Аверина. — Москва : Издательство Юрайт, 2019. — 179 с.
9. Игошин, В.И. Теория алгоритмов: Учебное пособие / В.И. Игошин. - М.: ИНФРА-М, 2013. - 318 с.
10. Канцедал, С.А. Алгоритмизация и программирование : Учебное пособие / С.А. Канцедал. - М.: ИД ФОРУМ, НИЦ ИНФРА-М, 2013. - 352 с.
11. Крупский, В.Н. Математическая логика и теория алгоритмов: Учебное пособие для студентов учреждений высшего проф. образования / В.Н. Крупский, В.Е. Плиско. - М.: ИЦ Академия, 2013. - 416 с.

УДК 004

В. Білий, магістр гр. КН-18М-1,9
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ ДИНАМІЧНОЇ ГЕНЕРАЦІЇ РОЗКЛАДУ ЗАНЯТЬ НА БАЗІ ОС WINDOWS 10

У статті проведено дослідження розробленого програмного забезпечення, призначене для динамічної генерації розкладу занять на базі ОС Windows 10. Метою розробки є дослідження та програмна реалізація системи динамічної генерації розкладу занять на базі ОС Windows10. Об'єктом дослідження є процес складання розкладу за допомогою засобів операційної системи Windows 10. Предметом дослідження є методи та алгоритми складання розкладу занять на основі операційної системи Windows 10. Методи дослідження базуються на теорії алгоритмів, використанні булевої алгебри та чисельних методів, а також математичного апарату теорії складання розкладу. Результат роботи – програмне забезпечення системи динамічної генерації розкладу занять на базі операційної системи Windows 10. В процесі роботи над програмною моделлю виконано аналіз існуючих програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення. Розроблено зручний інтерфейс з користувачем. Наведені інструкції по роботі з програмними засобами. Програму розроблено в середовищі Microsoft Access з використанням вбудованої мови програмування Visual Basic for Applications.
комп'ютерні науки, розклад занять, генерація

Постановка проблеми. Однією з найважливіших складових у підготовці висококваліфікованих спеціалістів своєї справи є чітка організація навчального процесу, яка може бути реалізована лише при якісному його плануванні.

Формування семестрового розкладу занять – надзвичайно відповідальне, та складне завдання керування навчальним процесом ВНЗу, коледжу, школи тощо. Воно характеризується значною трудомісткістю, а його успішна реалізація можлива лише при врахуванні всіх підрозділів навчального закладу.

Розклад навчальних занять – це кінцевий результат планування, що регламентує та впорядковує навчальну роботу слухачів, студентів та науково-педагогічних працівників навчального закладу. Ефективність навчального процесу напряму випливає з якості організації розкладу занять. Саме тому відповідальність за складання розкладів обумовлена безпосереднім впливом кінцевого результату створення розкладу на ефективність та якість організації навчання. Розклад занять закладає організаційний фундамент реалізації навчальних програм та планів.

Трудомісткість та складність цього процесу обумовлена саме участю багатьох представників різних ланок управління, планування і забезпечення навчального процесу при підготовці, обробці і використанні великої кількості нормативної навчальної методичної документації та іншої інформації. Тому великі часові витрати, помилки та суб'єктивізм – є тим неповним переліком недоліків, що вимушує звертатися до інформаційних технологій, які в змозі звести до мінімуму існуючі негаразди шляхом автоматизації процесу конструювання розкладу занять.

На сьогодні існує ряд програмних продуктів, що так, чи інакше допомагають у вирішенні проблем складання розкладу занять в навчальних закладах. Проте ціна на них, як правило, досить висока, наявні певні складнощі в експлуатації, і ці програми часто не враховують деякі нюанси при організації навчального процесу. Тому вирішення вищезгаданих проблем та побудова нового, оригінального програмного забезпечення обумовлює актуальність моєї роботи.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини системи динамічної генерації розкладу занять на базі ОС Windows 10.

Мета й завдання дослідження. Метою розробки є програмна реалізація системи динамічної генерації розкладу занять на базі ОС Windows10.

Для досягнення поставленої мети необхідно виконати наступні завдання:

- підготувати основні теоретичні відомості, необхідні для вирішення поставленої задачі;
- дослідити існуюче програмне забезпечення для вирішення подібних задач, виявити його переваги і недоліки, врахувати їх при розробці програмного забезпечення за завданням магістерської роботи;
- розробити структурну і функціональну схеми, а також діаграму процесів;
- розробити та оптимізувати алгоритм роботи програмного забезпечення;
- обрати кращу мову програмування для реалізації такого завдання та написати програмне забезпечення, використовуючи розроблений алгоритм;
- відлагодити розроблене програмне забезпечення, при наявності помилок в роботі виправити їх;
- дослідити та обгрунтувати економічну ефективність використання розробленої програми;
- здійснити аналіз небезпечних та шкідливих факторів, що впливають на програміста при розробці даного програмного забезпечення, розробити заходи з охорони праці;
- зробити висновки щодо розробленого програмного забезпечення, основних його переваг, призначення тощо.

Розроблена програма повинна мати зручний інтерфейс користувача і включати в себе довідкову інформацію.

Об’єктом дослідження є процес складання розкладу за допомогою засобів операційної системи Windows 10.

Предметом дослідження є методи та алгоритми складання розкладу занять на основі операційної системи Windows 10.

Методи дослідження базуються на теорії алгоритмів, використанні булевої алгебри та чисельних методів, а також математичного апарату теорії складання розкладу.

Було впроваджено рішення, здатне покращити та вдосконалити процес складання навчального розкладу занять, а саме генетичний алгоритм та цільову функцію, які інтегровані в магістерську роботу. Генетичний алгоритм працює з популяцією особин, кожна з яких має хромосоми, які відповідають типу ресурсу (викладачі; академічні групи, підгрупи та потоки; аудиторії), а цільова функція має безпосередній вплив на ймовірність участі хромосоми в генерації розв’язків-нащадків.

Програмний продукт, розроблений в рамках даної магістерської роботи, було виконано на замовлення навчального відділу ЦНТУ, проте він може використовуватися й іншими навчальними закладами з метою вдосконалення планування освітнього процесу.

Виклад основного матеріалу. Програмне забезпечення для динамічної генерації розкладу, система, яка розроблена в процесі виконання роботи, є складною багатофункціональною системою, що призначена для максимальної автоматизації складання розкладу з урахуванням усіх можливих нюансів та особливостей, що можуть виникнути в процесі роботи.

До функціональної частини бази даних можна віднести таблиці, запити, макроси та модулі. В розроблюваному програмному забезпеченні міститься 18 таблиць (де зберігаються дані по викладачах, предметах, групах, список дисциплін тощо), 15 запитів (для реалізації вибірки потрібних даних за обраними критеріями), 13 макросів (в яких реалізовані такі механізми, як пошук аудиторії/дисципліни/групи/викладача, вибір навчального плану, закриття форми і т.д.) та 1 модуль для (опису деяких найпростіших функцій). Всі таблиці

бази даних створювалися в режимі конструктора, оскільки саме в цьому режимі є можливість задати найточніші налаштування полів створюваної таблиці.

Як відомо, у Access існують запити декількох типів: запити на вибірку, на зміну, параметричні запити і перехресні. Для реалізації задачі, поставленої в магістерській роботі, зокрема відображення потрібних користувачу даних, або зміни існуючої інформації в базі даних, достатньо було реалізувати запити двох типів: на зміну та на вибірку, оскільки потреби в більш складних запитах для опису вищезгаданих дій не виникло. Запити на вибірку це запити, які не змінюють ні дані, ні їх структуру, а лише вибирають з них потрібну інформацію за певним критерієм. Завданням запитів на зміну є зміна даних або зміна структури даних БД. Результатом запиту на вибірку є таблиця, що містить в собі дані, які відповідають заданим критеріям вибірки. Результати виконання запиту на зміну можуть бути різними, це може бути таблиця в яку додано нові поля або видалено вже наявні, може бути створення нової таблиці або видалення вже наявної, оновлення вже існуючих в таблиці даних.

Всі запити в розробленій базі даних реалізовані за допомогою мови SQL, хоча деякі з них можна представити і у вигляді QBE-запитів.

Було використано декілька макросів. Макрос представляє послідовність макрокоманд вбудованої мови Access, що задають автоматичне виконання деяких операцій. В програмі було реалізовано 13 макросів, для автоматизації різноманітних дій: пошуку аудиторії, групи, дисципліни, закриття форми тощо.

Загалом функціонування системи має 2 основні складові: зміну, зберігання та виведення інформації, що пов’язана з навчальним процесом (різноманітні дані про викладачів, кафедри, аудиторії, групи тощо) та, власне, механізм складання розкладу, який оперує цими даними.

Всю необхідну для складання розкладу інформацію зосереджено в таблицях бази даних, які пов’язані між собою та об’єднані в єдину систему.

Дисципліни

Найменування дисципліни	Шифр кафедри
Матеріали для напилення, наплавлення і трібоматеріалозна	ЕРМ
CAD/CAM систем в ГКВ	АВП
CAD/CAM-системи	МВ
Стратегія діяльності та аналітичне забезпечення її реалізації	АУДИТ
PR-менеджмент	МЕНЕДЖ
PR-технології та реклама в інформаційній сфері	УКР
Web технології в управлінні та проектуванні	АВП
Web-програмування	МАРКЕТ
Автоматизація виробничих процесів	ТМ
Автомат. документ. корпорат.систем	УКР
Автоматизоване проектування машин	БШМ
Автоматизація та роботизація КШВ	ОМТ
Автоматизоване проектування штампувальних цехів та дільн	ОМТ
Автоматизація інженерних розрахунків в машинобудуванні	ТМ
Автоматизація обладнання ливарного виробництва	МтаЛВ
Автоматизація планово-економічних розрахунків	ЕОВ
Автоматизація технологічних процесів	АВП

Рисунок 1 – Таблиця «Дисципліни»

Оперування та перегляд цих даних здійснюється за допомогою інтерфейсу користувача у вигляді форм, кнопок та полів пошуку, а також запитів та макросів. Задля розширення повноважень у складанні розкладу, список наявних груп, перелік аудиторій, дисциплін та викладачів користувач може змінювати за бажанням у спеціально створених

для цього формах. Реалізовано також функцію пошуку за різними критеріями у формах для відображення складових навчального процесу. Наприклад, у вікні «Кафедри» потрібну кафедру можна знайти не лише за назвою, але й за даними про завідуючого кафедри.

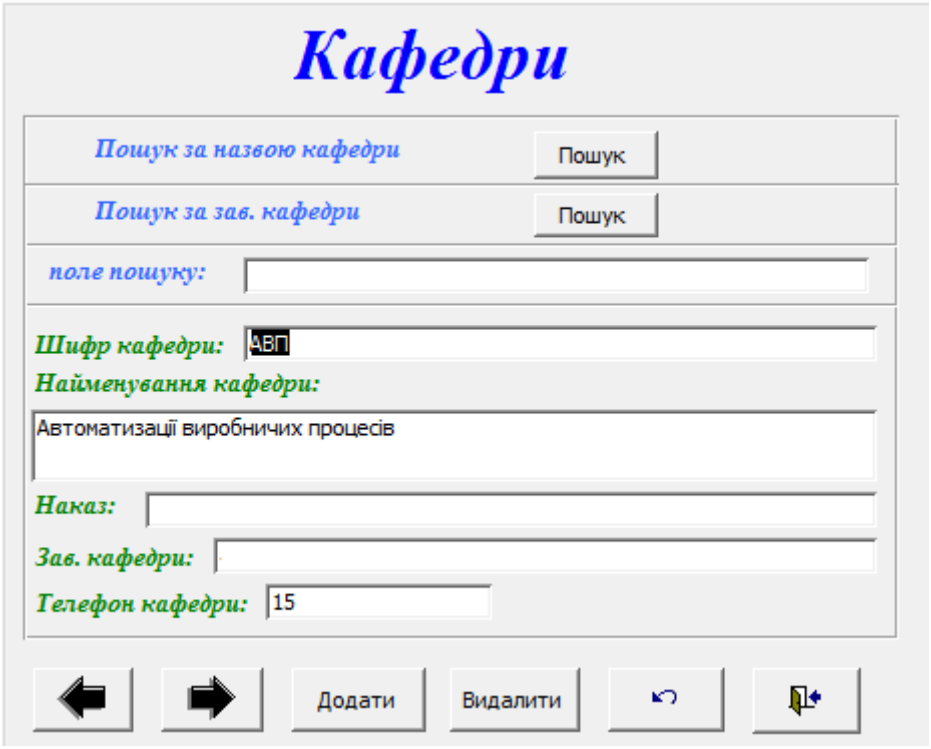


Рисунок 2 – Вікно «Кафедри»

Сам механізм створення розкладу реалізовано за допомогою функцій та процедур, написаних на вбудованій в систему Microsoft Access мові Visual Basic for Applications. Ця мова є дещо спрощеним варіантом реалізації мови програмування Visual Basic, що вбудована в лінійку продуктів Microsoft Office. Вона покриває та розширює функціональність спеціалізованих макро-мов, таких як WordBasic, що застосовувалися раніше.

Visual Basic for Applications являється інтерпретованою мовою. Вона близька до мови Visual Basic, але може виконуватися лише в рамках додатку, в який вона вбудована. Крім того, вона може використовуватися для керування одним додатком з іншого з допомогою OLE Automation (наприклад, таким чином можна створити документ Word на основі даних з Excel). Visual Basic for Applications функціонально багата і надзвичайно гнучка.

До переваг цієї мови відносять порівняно легкість освоєння, завдяки якій додатки можуть створювати навіть користувачі, що не програмують на професійному рівні. До особливостей Visual Basic for Application можна віднести також виконання скрипта саме в середовищі офісних додатків. Наявна можливість використовувати (але не створювати) бібліотеки DLL.

Недоліком є проблеми з оберненою сумісністю різних версій. Ці проблеми, в основному, пов’язані лише з тим, що код програми звертається до функціональних можливостей, що з’явилися в новій версії програмного продукту, які відсутні в старій. Також до недоліків часто відносять надто високу відкритість коду, тим не менш, більшість програмних продуктів дозволяють користувачеві використовувати шифрування коду та встановлення паролю для його перегляду.

Нижче продемонстровано код функції-обробника кнопки видалення запису з таблиці «Цикл дисциплін», написаної на мові Visual Basic for Applications.

```
Private Sub Видалити_Click()
Dim spt As String
On Error GoTo werr2
```

```
spt = Nz(Список0)
‘ заносимо обраний запис до змінної
rst.FindFirst "[Цикл дисциплін]='" & spt & "'"
‘ якщо пусто, тоді закінчуємо виконання функції
If rst.NoMatch Then Exit Sub
‘ Якщо видалення підтверджено – видаляємо запис
If MsgBox("Видалити запис?", vbYesNo + vbDefaultButton2 + vbQuestion) = vbYes Then
    rst.Delete
    Список0.Requery
    Список0.SetFocus
    Додати.Enabled = True
    Видалити.Enabled = False
    Зберегти.Enabled = False
End If
Exit Sub
‘ якщо помилка, то
werr2:
DoCmd.RunMacro "Помилка оновлення"
End Sub
```

Дана функція видаляє обраний користувачем запис з таблиці «Цикл дисциплін» в базі даних. Перед видаленням система перепитає чи справді здійснити операцію видалення. Отримавши підтвердження від користувача, програма видалить запис з бази даних.

Далі будуть представлені структурна та функціональна схеми,а також діаграма процесів, які дадуть наочне уявлення про принципи функціонування вузлів програмного забезпечення та взаємодію між ними.

Розробка структурної схеми

Структурна схема – схема, яка визначає основні функціональні частини виробу, їх взаємозв'язки та призначення. На рисунку показані основні вузли програмного забезпечення та їхню взаємодію між собою: ядро системи, своєрідний центр обчислень та механізм реалізації всіх операцій, «отримує» в головному меню від користувача вказівку про те, яку операцію слід виконати і які дані потрібно вивести. Далі йде звертання до бази даних з метою отримання необхідної інформації такої як, наприклад, список наявних аудиторій та дисциплін, працюючих викладачів тощо. Після чого, якщо користувач працює з розкладом, запускається окремий модуль для даного комплексу операцій, після завершення яких виводиться результат на екран, або направляється на друк за бажанням користувача.

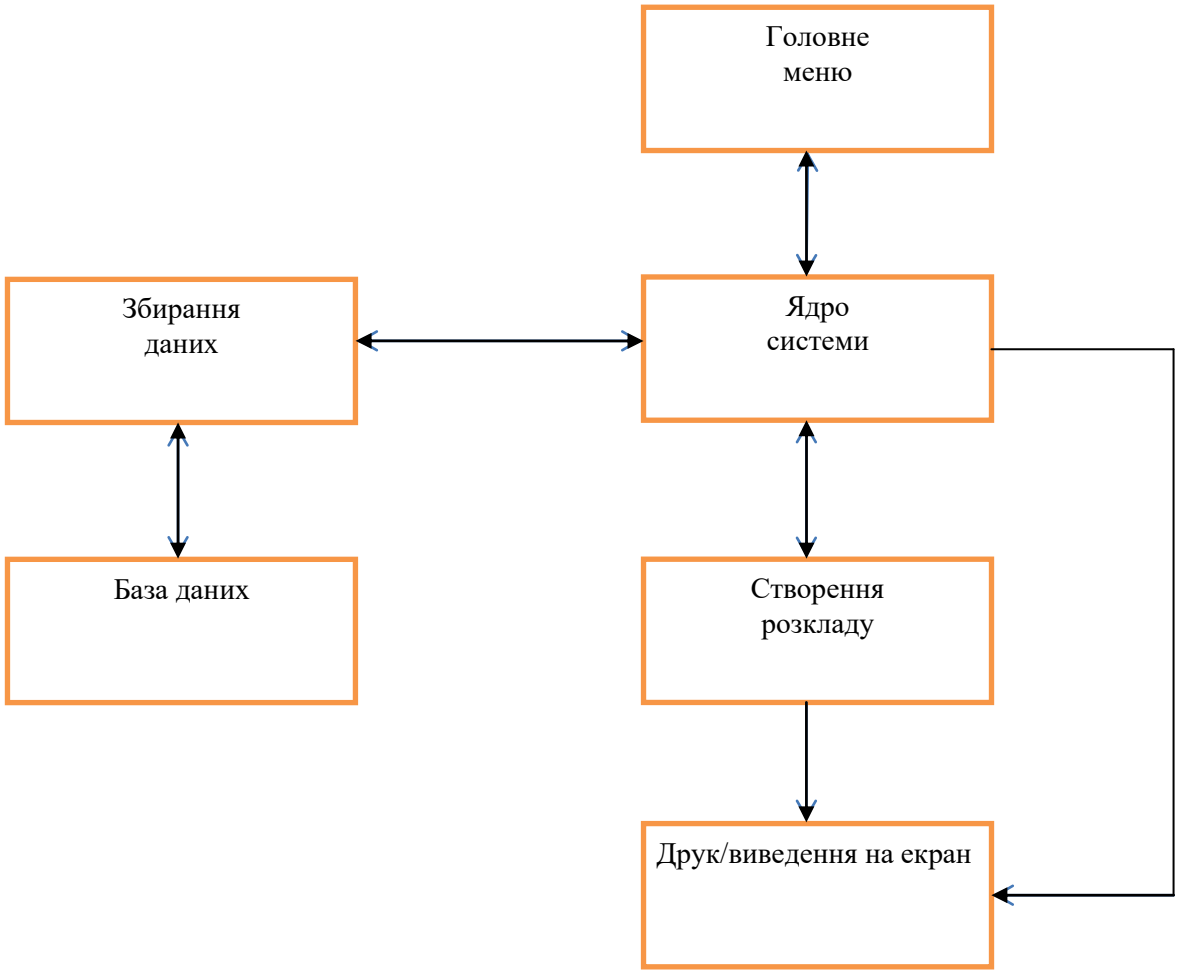


Рисунок 3 – Структурна схема програми

Висновок. У статті розглянуто прогамне забезпечення, призначене для динамічної генерації розкладу занять на базі ОС Windows 10. Перед розробкою роботи мною було розглянуто програмне забезпечення аналогічного типу та спрямування. Було з'ясовано, що ціна на такі програмні продукти досить висока, їх розроблено для великих підприємств або вони складні у експлуатації. Також для введення вищезгаданих програм у експлуатацію необхідна підтримка, що потребує великих матеріальних затрат, спеціальні договори про супровід і потреба цілого штату співробітників, що будуть займатися її підтримкою. Саме тому було прийнято рішення про розробку нового оригінального програмного забезпечення, легшого в експлуатації та на платформі MS Access. Далі було розглянуто опис процесів розробки та обґрунтування вибору MS Access, як засобу проектування. Він має всі риси класичної СУБД і надає до-даткові можливості. За допомогою Access можна створити додаток, що працює в середовищі Windows і повністю відповідає нашим потребам по управлінню даними. Першими етапами побудови програмного забезпечення була побудова структурної та функціональної схеми, що призначені для відображення основних функціональних та структурних складових програми та їхніх взаємозв'язків, а також діаграми процесів для наочного представлення почерговості виконання дій програми. Ці схеми дозволили збудувати базу даних, що використовується в даному програмному забезпеченні. Було розроблено таблиці, створено запити звіти і форми для успішного використання програми. Як наслідок, було створено автоматичну систему, яка вирішує всі поставлені завдання:

- введення, редагування та видалення інформації, що є основою для складання розкладу.

- введення, редагування та видалення об'єктів розкладу, до яких відносяться: викладачі, дисципліни, аудиторії, факультети, курси, групи;
- виведення звітів: розклад занять, розклад для викладачів, розклад аудиторій;
- інформаційна система має зручний графічний інтерфейс та проста в освоєнні.

Список літератури

1. Клим Б.В., Юрчишин В.М. Організація баз даних – Івано-Франківськ: Факел, 2010. – 224 с.
2. Грабер М. Введение в SQL. – М.: Лори, 1996 – 379 с.
3. Дейт К. Введение в системы баз данных // 6-издание. – Киев: Диалектика, 1998. – 784 с.
4. Семенов С. П. Татаринцев Я. Б. Сравнительный анализ подходов к автоматизации составления расписаний учебных занятий в образовательных учреждениях 2010.- Известия Алтайского государственного университета, 2010.-Т.105.
5. Лагоша Б. А. Комплекс моделей и методов оптимизации расписания занятий в вузе / Б. А. Лагоша,
6. А. В. Петропавловская. – М. : Экономика и математические методы. – 1993 г. – 410 с.
7. Лазарев А. А., Гафаров Е. Р. Теория расписаний. Задачи и алгоритмы / А. А. Лазарев, Е. Р. Гафаров –М. : Физический факультет МГУ, 2011.
8. Попов Г. А. Формализация задачи составления расписания в высшем учебном заведении / Г. А. Попов – Вестник АЕТУ. – 2006. – № 1.
9. Костюк В.И., Мартинес Х.О., Зорин В.В. Использование алгоритмов последовательной обработки для составления расписаний / Вопросы создания АСУ ВУЗ. М.: НИИВШ, 1976. – С.3-5.
10. Безгинов А.Н. Обзор существующих методов составления расписаний / А.Н. Безгинов, С.Ю. Трегубов // Информационные технологии и программирование: – М.: МГИУ, 2005. – Вып. 2 (14). – С. 5-18.

УДК 004

В. Босько, магістр гр. КН-18МЗ
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ АНАЛІЗУ ЗАСТОСУВАННЯ РІЗНИХ ТИПІВ БАЗ ДАНИХ В СУЧАСНИХ ІС

У статті розроблено програмне забезпечення, яке призначено для системи аналізу застосування різних типів баз даних при розробці WEB застосунків. Метою розробки є дослідження та програмна реалізація системи аналізу застосування різних типів баз даних при розробці WEB застосунків. Об’єктом дослідження є аналіз існуючих реалізацій об’єктно-орієнтованих БД з погляду на продуктивність роботи. Предметом дослідження є розробка сховищ даних на основі ООБД. Методи дослідження базуються на зберігання даних, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи ІС на основі ООБД у якості сховища даних . В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення. Розроблено зручний інтерфейс користувача. Наведені інструкції по роботі з програмними засобами.

комп’ютерна інженерія, ООБД, WEB ресурси

Постановка проблеми. На сьогоднішній день неможливо представити відсутність інформаційних технологій у нашому житті. Важко уявити сучасне виробництво, науку, культуру,економіку або спорт без участі комп'ютерів. Комп'ютеризоване програмне забезпечення має місце у всіх вищенаведених сферах забезпечення життєдіяльності. Воно допомагає людям у роботі, розвагах, освіті та наукових дослідженнях.

Будь-яка сучасна організація не може обійтися без бази даних. Це навчальні заклади, банки, магазини, заводи, будь-які підприємства і державні установи. Вони використовують їх для перекладу даних в електронний вигляд і об'єднання даних, а також оперативного доступу

до них. Це дозволяє економити час і кошти на витрати. Звичайно, зниження часу є лише побічним ефектом автоматизації. Найголовніше завдання розвитку інформаційних технологій в зовсім іншому - в придбанні тією чи іншою організацією виключно нових якостей, які надають їй істотну конкурентоспроможність. А це дорогого коштує. До того ж, зараз установка і управління бази даних не є таким вже й важким процесом, як це було десятиліття тому. Коли проектування і управління базами даних були не автоматизовані. Система управління базою даних дозволяє створювати базу даних, оновлюючи в ній зберігається інформацію, забезпечуючи оперативний доступ до неї для перегляду і пошуку інформації. Актуальність теми полягає в тому, що в нових системах управління базами даних є функція не тільки зберігання даних в своїх структурах, проте можна і зберігати програмний код, за допомогою якого і йде взаємодія з користувачем або програмно - апаратним засобом

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи аналізу застосування різних типів баз даних в сучасних ІС.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи аналізу застосування різних типів баз даних в сучасних ІС.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

- Огляд існуючих систем баз даних які використовуються в сучасних ІС
- Дослідження концепції об’єктно-орієнтованих баз даних.
- Програмна реалізація ІС на основі ООБД у якості сховища даних.

Об’єктом дослідження є аналіз існуючих реалізацій об’єктно-орієнтованих БД з погляду на продуктивність роботи.

Предметом дослідження є методи розробки сховищ даних на основі ООБД.

Методи дослідження базуються на методах зберігання даних, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Виходячи з теми роботи потрібно розробити програмне забезпечення системи управління сайтом та підключенням баз даних різного типу для аналізу продуктивності роботи.

Ідея розроблюваного програмного забезпечення – створити простий у використанні сайт факультету для внесення виданих викладачами посібників до якого задля тестування продуктивності робити будуть підключатися різні типи БД і наповнюватися відповідними даними.

Аналіз і вибір бази даних

Порівняємо продуктивність реляційних та об’єктно-орієнтованих баз даних на практиці. Для цього ми розглянемо швидкість та об’єм пам’яті, що використовується при додаванні, зчитуванні та повторному зчитуванні великої кількості даних. Також критерієм для порівняння буде розмір бази даних, заповненої даними.

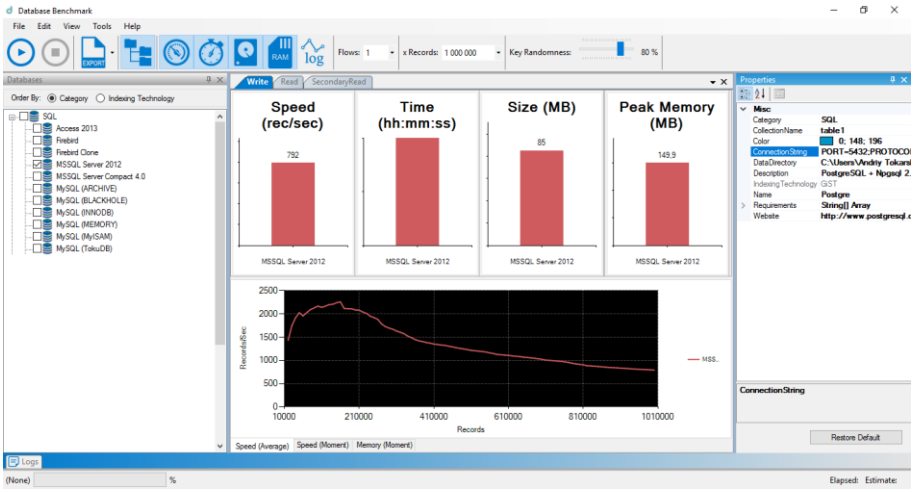


Рисунок 1 - Інтерфейс Database Benchmark

Для порівняння будемо використовувати програму Database Benchmark v3.0.0. Ця програма може вимірювати продуктивність дуже великої кількості баз даних, серед яких є як реляційні, так і об'єктні. Database Benchmark дозволяє спостерігати за процесом тестування у реальному часі. Розроблена із використанням .NET Framework + WPF.

Порівнювати будемо такі бази даних, як Microsoft SQL Server 2016, Db4Objects, VelocityDb, Volante, Perst. Всі ці бази даних можливо тестувати із використанням Database Benchmark.

Тестувати будемо швидкість і затрати пам'яті на додавання та читання одного мільйона записів, а також розмір відповідних баз даних.

Таблиця 1 - Швидкість операцій, виконуваних базами даних (у записах/сек)

	Додавання	Читання	Повторне читання
Db4Objects	9898	4839	4868
Perst	1894	1175	1194
VelocityDb	145603	30452	426333
Volante	15447	136968	119346
MS SQL Server 2016	792	412031	435002

Таблиця 2 - Максимальні затрати оперативної пам'яті (у Мб)

	Додавання	Читання	Повторне читання
Db4Objects	1134.1	1134.2	738.3
Perst	130	122.3	112.1
VelocityDb	256.2	272.5	272.6
Volante	2423.5	2505.7	2498
MS SQL Server 2016	149.9	130.5	130.5

Таблиця 3 - Розмір заповнених баз даних (у Мб)

Db4Objects	Perst	VelocityDb	Volante	MS SQL Server 2016
229.9	188.6	53.1	123	85

У таблицях 1-3 занесені результати вимірювання продуктивності баз даних.

Таблиця 1 показує швидкість виконання операцій, таблиця 2 показує затрати пам'яті на виконання цих операцій, а таблиця 3 – розміри баз даних.

Результати тестування реляційних баз даних

Для порівняння із об'єктно-орієнтованими базами даних мною було протестовано реляційну базу даних Microsoft SQL Server. Database Benchmark згенерував таблицю і заповнив її такими даними: число типу BIGINT, що виступає основним ключом таблиці, дві колонки типу VARCHAR(255), дві колонки типу INT, дві колонки типу REAL, і колонка типу DATETIME. Таблицю було заповнено одним мільйоном записів, що видно із рисунка 2.

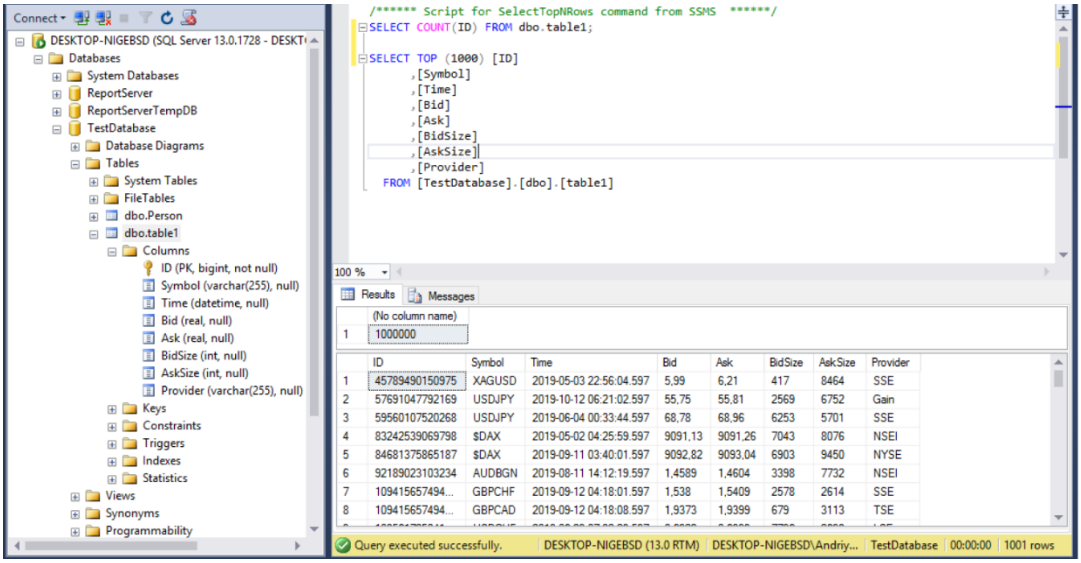


Рисунок 2 – Заповнення таблиці для тестування

Із результатів виконання програми Database Benchmark отримуємо, що Microsoft SQL Server є найповільнішою серед протестованих баз даних по швидкості додання нових записів.

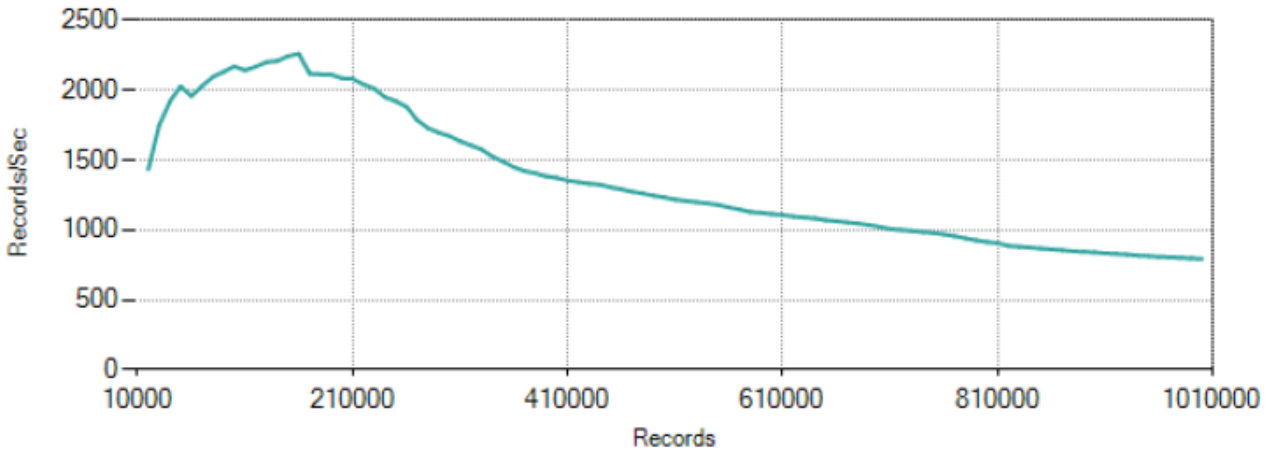


Рисунок 3 - Графік залежності середньої швидкості додання нових записів від кількості записів в SQL Server

Рисунок 3 демонструє, що швидкість додання нових записів починає стрімко спадати після того, як кількість записів досягне приблизно 200000, але навіть в кращому випадку SQL Server не може сперечатись із більш швидкими у цьому плані базами даних VelocityDb, db4objects, Volante.

Проте розмір бази даних дорівнює всього 85Mbyte, що є другим результатом після VelocityDb.

Але жодна із протестованих об'єктних баз даних не перегнала SQL Server у плані швидкості читання даних. Крім того, SQL Server не вимагала великих затрат оперативної пам'яті. Менше оперативної пам'яті вимагає лише база даних Perst.

MS SQL Server є ідеальною для збереження даних, якщо в інформаційній системі виникає необхідність швидкого вилучення даних, а нові дані заносяться не дуже часто. Також важливою перевагою SQL Server над іншими базами даних є велика кількість гарно структурованої документації, чого не можна сказати про інші бази даних.

Результат тестування об'єктно-орієнтованих баз даних представлено на рисунку

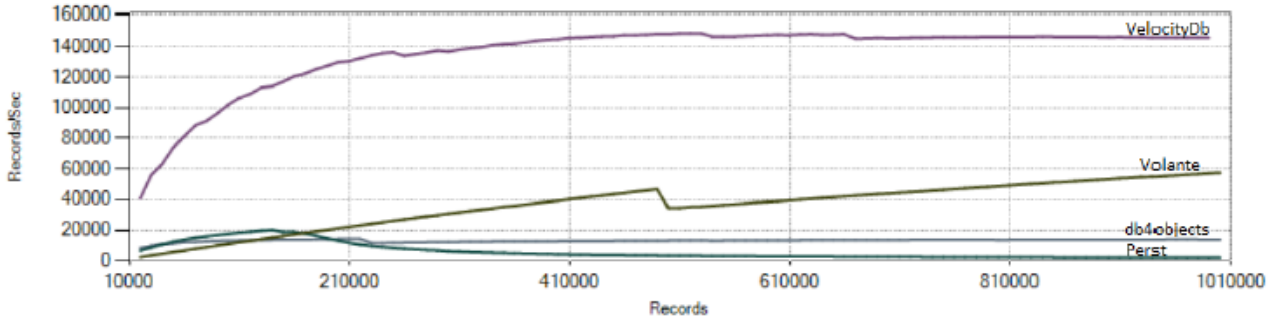


Рисунок 4 – Тестування ООБД

Серед об'єктних баз даних, по-перше слід виділити базу даних, що явно програла іншим у плані продуктивності. Цією базою даних є Perst. Хоча вона показує найкращі результати в плані затрат оперативної пам'яті, вона явно програє всім у плані швидкості вилучення інформації, і виграє лише SQL Server у плані швидкості додавання інформації.

Єдиною причиною використовувати Perst є необхідність мінімізації затрат оперативної пам'яті, але MS SQL Server програє Perst у цьому плані не дуже сильно. Крім цього, Perst не має багатьох очевидних сильних сторін, що є у SQL Server.

База даних VelocityDb виграє відразу у трьох характеристиках: розмір заповненої бази даних та швидкість додання нових записів. Крім того, швидкість повторного читання даних близька до значення цієї швидкості в MS SQL Server.

БД Volante виграє VelocityDb по значенню швидкості першого читання записів, але всі операції додавання, читання і повторного читання записів дуже дорогі. Додавання і читання одного мільйону записів із використанням Volante коштувало близько 2.5 Gbyte RAM.

БД Volante і VelocityDb являються in-memory database. Вони вирішують проблему дуже повільного доступу до пам'яті на жорсткому диску. In-memory databases спираються на збереження даних на оперативному запам'ятовуючому пристрої. Це робить доступ до даних дуже швидким.

Серед протестованих об'єктних баз даних, очевидно, найкращою можна назвати VelocityDb. Її можна використовувати при необхідності швидкої обробки великої кількості даних, а також для швидкого зчитування даних, особливо при необхідності їх повторного зчитування. У випадку необхідності використання безкоштовної об'єктної бази даних хорошим варіантом буде Db Volante.

Опис інформаційної системи

У роботі реалізована інформаційна система, що використовує у якості сховища даних об’єктно-орієнтовану базу даних VelocityDb. Вибір бази даних обґрунтований результатом порівняльного аналізу баз даних.

Інформаційна система зберігає у базі інформацію про працівників і клієнтів, а також про посібники та історію їх перегляду або скачування. Працівник може додавати нові книги, а також відмічати, що конкретний клієнт(студент) користувався(скачував) зазначеною літературою .

Також інформаційна система здатна повідомляти користувача про те, що у якихось його колег сьогодні день народження, а також є можливість перегляду книг, які переглядали колеги.

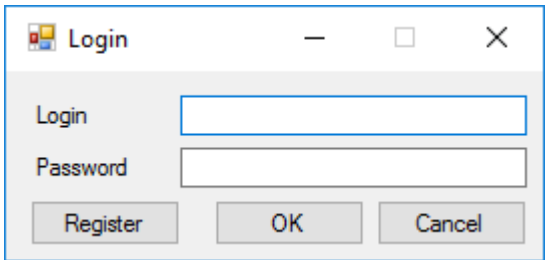


Рисунок 5 – Форма входу користувача

Для початку користування програмою користувачу потрібно буде авторизуватись (форма авторизації зображена на рисунку 11). Якщо у працівника існує обліковий запис, можна ввести логін і пароль, у іншому випадку – потрібно натиснути кнопку Register.

Для реєстрації користувача потрібно обов’язково вказати свої прізвище та ім’я, а також логін та пароль (рисунок 6).

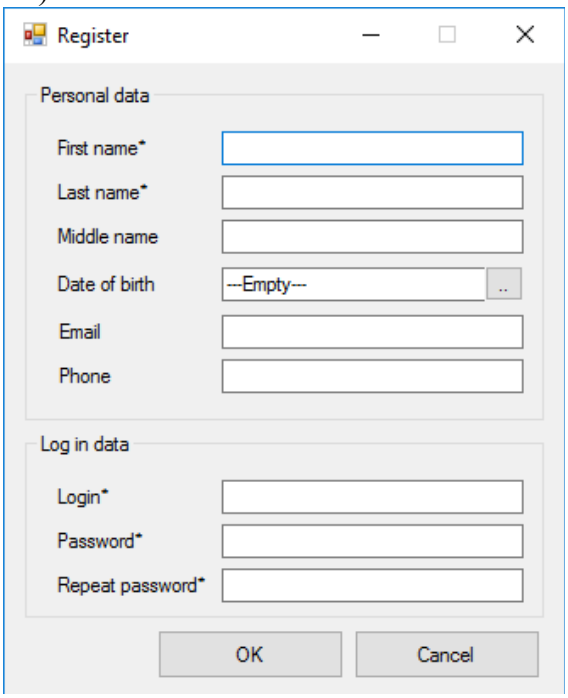


Рисунок 6 – Форма реєстрації

Після авторизації програма перенаправляє користувача на вікно із головним меню програми, зображеним на рисунку 7.

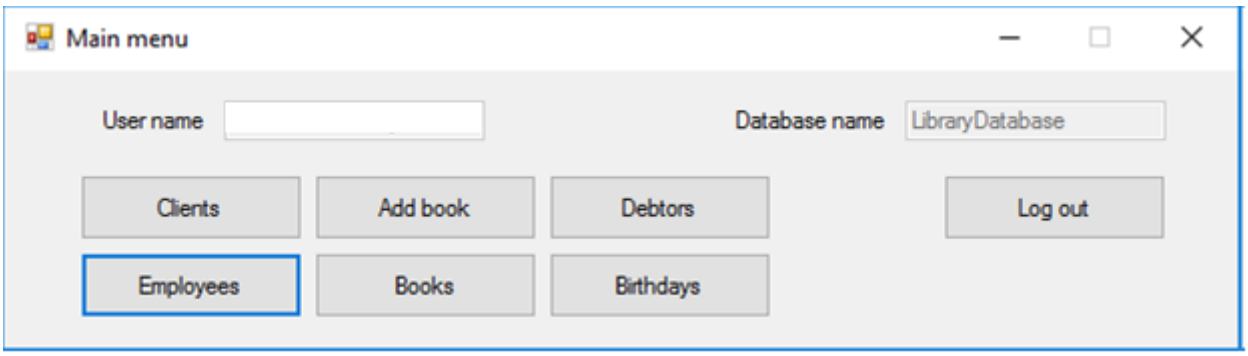


Рисунок 7 - Головне меню програми

Із меню можна перейти на вікна із клієнтами, працівниками. Також можна перейти на вікно додання книги, списку книг та списку людей, у яких сьогодні день народження.

Для перегляду списку книг потрібно натиснути на клавішу Books. Відкриється вікно, зображене на рисунку 8. Подвійний клік на рядок із книгою відкриє детальну інформацію про книгу. Тоді відкриється вікно, зображене на рисунку 8.

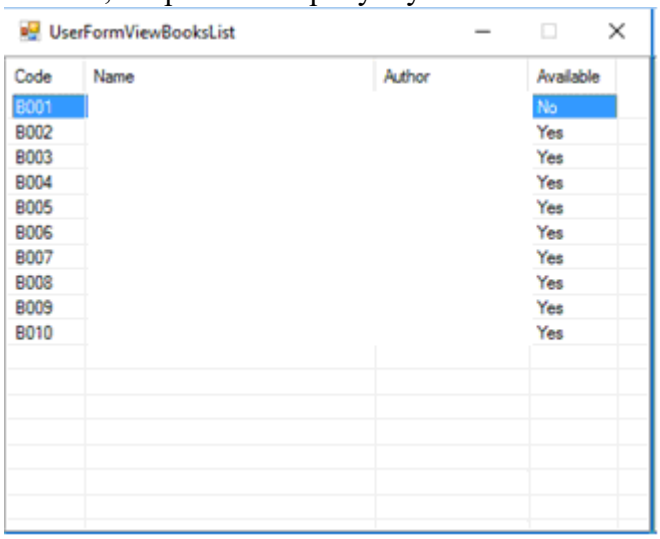


Рисунок 8 – Вікно із списком посібників

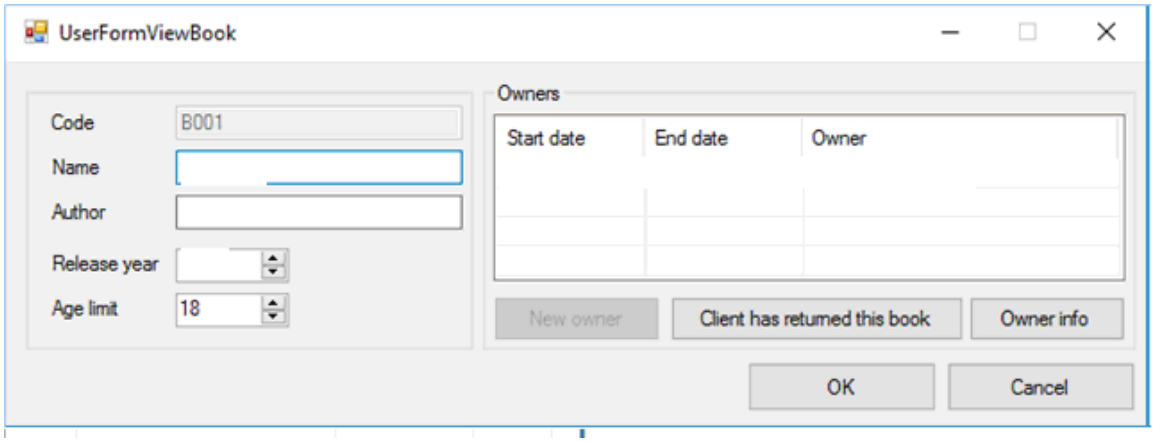


Рисунок 9 – Вікно із детальною інформацією про посібники

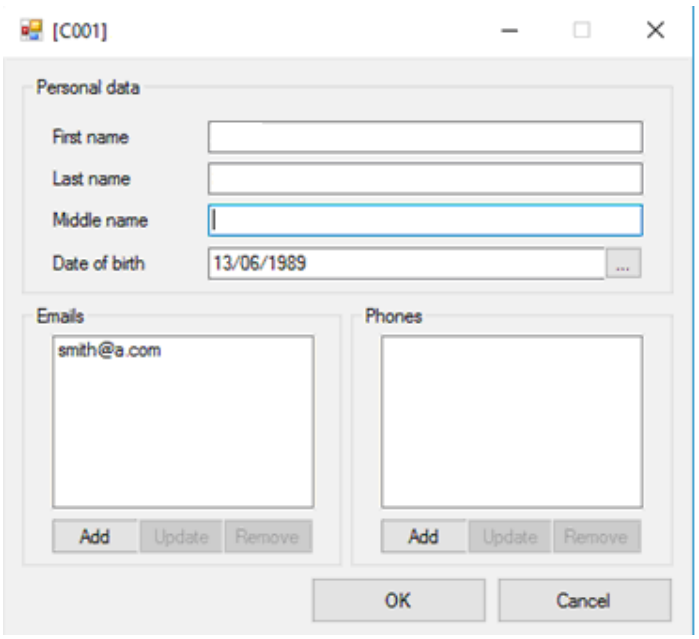


Рисунок 10 – Вікно із інформацією про людину

На рисунку 10 зображене це вікно. Як бачимо, серед персональної інформації людини є її ПІБ, дата народження, що може бути і не вказаною, а також списки її телефонів та електронних адрес. Натиснення кнопки ОК підтверджує зміни інформації.

Вище вказані вікна показують структуру даних, що зберігаються у розробленій інформаційній системі.

Серед інформації, що зберігається у книзі, можна виділити її код, назву, ім'я автора, рік випуску, вікові обмеження та історію користування. Із інформації із вікна, зображеного на рисунку 10, можна сказати, що користувач із кодом C001 та іменем скачав книгу Witcher 13 червня 2019 року. Натиснення кнопки Client has returned this book підтверджує, що клієнт повернув книгу. Із допомогою кнопки New owner можна вибрати нового користувача книгою, а дата початку користування для нього відразу ж встановиться на сьогоднішню. До речі, для книг із віковим обмеженням не можна вказати клієнта із невказаним віком або віком молодше значення вікового обмеження у якості користувача.

На рисунку 11 зображена UML-діаграма класів, які використовує дана інформаційна система. Клас OptimizedPersistable – клас, що знаходиться у бібліотеці вбудованої бази даних VelocityDb, тобто створювався не мною. У ньому є дуже велика кількість методів та властивостей, на діаграмі сною вказані лише найнеобхідніші для мене – властивість Id та метод Unpersist.

Id використовується для зберігання ідентифікатора об’єкта, що зберігається у базі.

Метод Unpersist створений для видалення об’єкта із бази даних. Варто відмітити, що цей метод є віртуальним, і його при необхідності можна перевантажити і написати власну реалізацію очистки, якщо це потребується. Наприклад, у класі Person цей метод перевантажений таким чином, що він видаляє спочатку списки телефонів та електронних адрес, а потім і сам об’єкт.

OptimizedPersistable у даній інформаційній системі є базовим класом для класів Person та Book. У свою чергу, класи Employee та Client походять від Person.

Клас Database є статичним, у ньому зберігається лише один статичний метод, реалізований для спрощення отримання об’єктів із бази даних.

Клас ThisApplication є класом, що зберігає у собі налаштування програми, а саме ім’я бази даних та авторизований працівник.

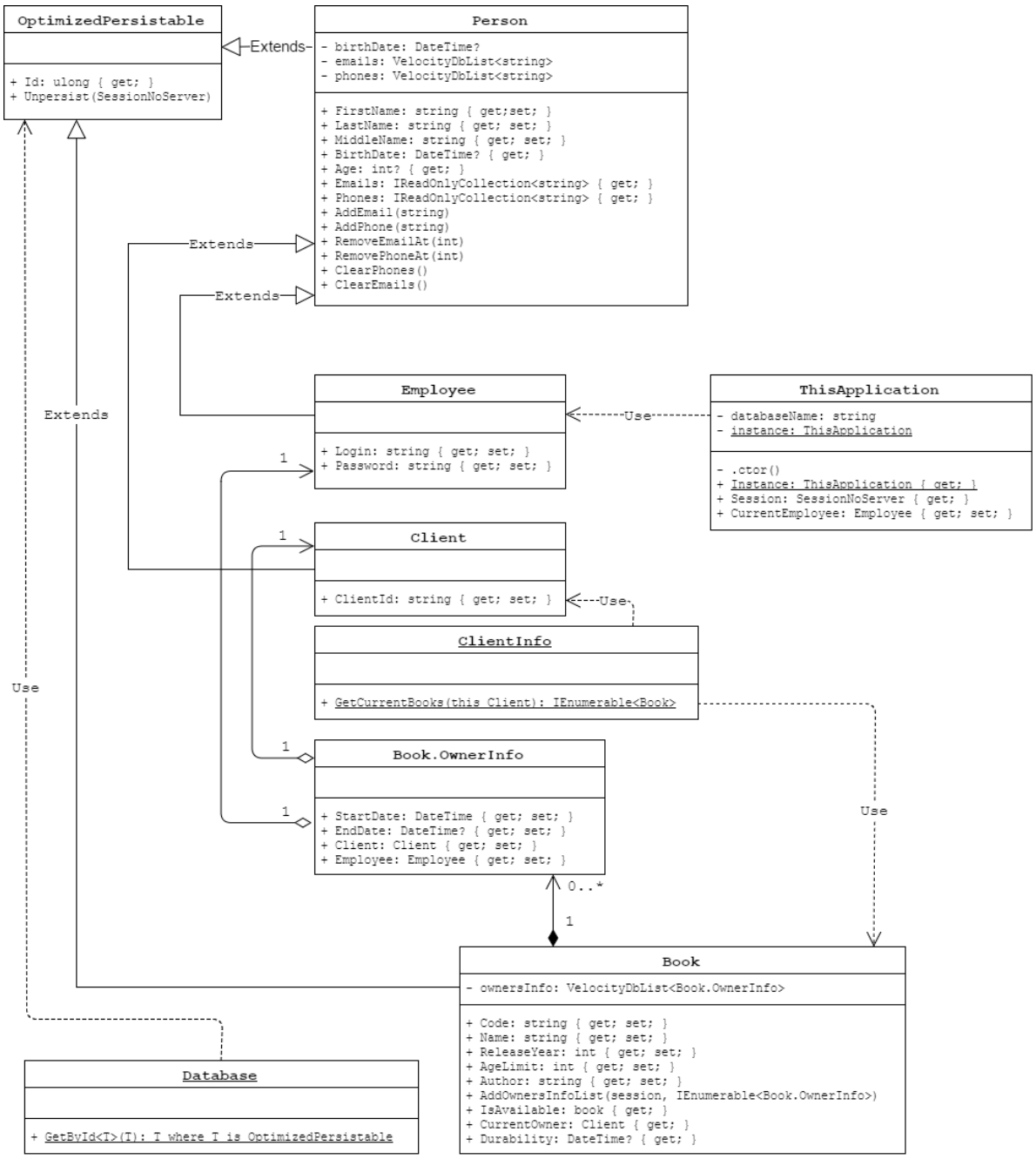


Рисунок 11 – UML-діаграма класів інформаційної системи

Розробка структурної схеми

Структурна схема сайту – це сукупність об’єктів та частин сайту та взаємозв’язки між ними. Призначенням структурної схеми є наглядне відображення складових частин сайту, його основних блоків, вузлів та взаємозв’язок між ними.

Структурна схема розробленої системи зображена на рисунку 12. На ній показано структуру.

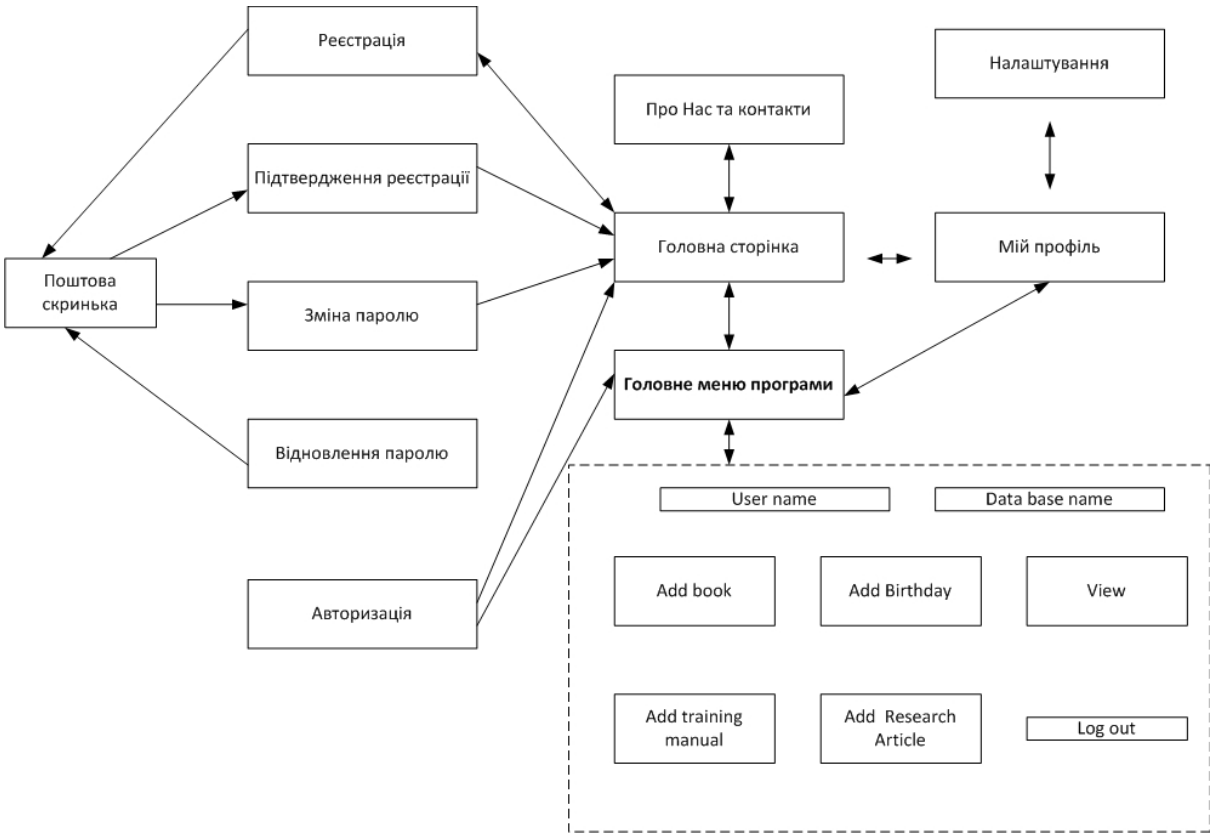


Рисунок 12 – Структурна схема

Зі схеми можна побачити, що сайт має головну сторінку з якої користувач може перейти до сторінки реєстрації, авторизації та до сторінки адміністративної панелі сайту. Зі сторінки реєстрації користувач може потрапити на сторінку авторизації. На сторінці авторизації користувач має можливість перейти на сторінку відновлення паролю, якщо він забув свій пароль для входу. Також можна потрапити до сторінки усіх проектів користувача. Звідси користувач може перейти до сторінки окремого проекту або до сторінки свого профілю. Також на цій сторінці користувач може вийти зі свого профілю.

Інформаційна система зберігає у базі інформацію про працівників і клієнтів, а також про посібники, методичні вказівки та видані наукові статті. Працівник може додавати нові книги. В кожній із книг зберігається їх історія перегляду співробітниками.

Також інформаційна система здатна повідомляти користувача про те, що у якихось його колег сьогодні день народження, а також є можливість перегляду інформації доданої співробітниками.

Висновок. У статті розглянуто та проаналізовано програмне забезпечення, яке призначено для системи аналізу застосування різних типів баз даних при розробці WEBзастосунків. В межах України в недостатній мірі представлені вітчизняні розробки в цій області з застосуванням ООБД. У роботі наведені теоретичне узагальнення й рішення наукового завдання дослідження методів застосування ООБД. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем побудованих з використанням різних типів БД; Досліджена система побудови WEBза стосунків з використанням ООБД; На основі отриманих результатів досліджень створена програмна реалізація системи застосування ООБД при розробці ПЗ. Розроблені під час виконання роботи алгоритми дозволяють успішно вирішувати застосування ООБД при розробці ПЗ. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки. Розроблене програмне забезпечення має простий, дружній та зручний інтерфейс користувача, що

забезпечує легкість у освоєнні роботи програмного продукту, зручність у використанні, і не потребує особливих спеціальних знань.При створені програмного забезпечення було використано об'єктно-орієнтований підхід з використанням таких технологій та мов програмування: HTML 5, CSS 3, JavaScript + jQuery + AJAX, PHP + PDO, JSON, що відповідають сучасним тенденціям у галузі веб-розробки. Програма реалізована на мові високого рівня PHPз відкритим вихідним кодом. Дана мова програмування дозволяє найбільш ефективно обробляти дані і спеціально сконструйований для веб-розробок і вбудовується безпосередньо в HTML. Це дозволило мінімізувати строк розробки програмного забезпечення, і, як слід, зменшити витрати на його розробку. Запропоноване програмне забезпечення ділиться на загальне програмне забезпечення, що поставляється із засобами обчислювальної техніки й спеціальне програмне забезпечення, що спеціально розроблене для даної конкретної системи й включає програми, що реалізують її функції. Програма призначена для виконання під управлінням будь-якої багатозадачної операційної системи так як для її використання потрібен лише сучасний браузер такий як "GoogleChrome", "MozillaFirefox", "Opera" та "Safari". Даються необхідні рекомендації з установки розробленого програмного забезпечення. Для підвищення рівня безпеки запропоновано застосовувати стандартні функції php: password_hash, password_verify для збереження даних користувача, а також використано методи для протидії XSS-атакам та SQL-ін'єкціям. В цілому створене програмне забезпечення підтверджує правильність використаних проектних рішень та повністю відповідає вимогам технічного завдання. Створене програмне забезпечення має потенційну можливість для подальшого вдосконалення і застосування у різних галузях.

Список літератури

1. Гмурман В.Е. Теория вероятностей и математическая статистика / В.Е. Гмурман. – М.: Высшая школа, 2003. – 479 с.
2. Городецкий А.Я. Информационные системы. Вероятностные модели и статистические решения. Учебн. пособие / А.Я.ГородецкийСПб: Изд-воСПбГПУ, 2003. 326 с.
3. ДСТУ 2481 – 94 Системи оброблення інформації інтелектуальні інформаційні технології. Терміни та визначення. – Х.: ДЕРЖСТАНДАРТ УКРАЇНИ, 1994. – 33 с.
4. Ершов В.А. Мультисервисные телекоммуникационные сети / В.А. Ершов, Н.А. Кузнецов – М.: Изд. МГТУ им. Н.Э. Баумана, 2003. – 432 с.
5. Мартыненко И.И. Автоматика и автоматизация производственных процессов.-М.:Агропромиздат,1985.-208 с.
6. Вишневский В.М. Теоретические основы проектирования компьютерных сетей / В.М. Вишневский – М.: Техносфера, 2003. – 512 с.
7. Галкин В.А. Телекоммуникации и сети / В.А. Галкин, Ю.А. Григорьев. – М.: МГТУ имени Н.Э. Баумана, 2003. – 608 с.
8. Гонсалес Р. Цифровая обработка изображений / Р. Гонсалес, Р. Вудс. – М.: Техносфера, 2005. – 1072 с.
9. Городецкий А.Я. Информационные системы. Вероятностные модели и статистические решения. Учебн. пособие / А.Я.Городецкий СПб: Изд-воСПбГПУ, 2003. 326 с.
10. Смірнов О.А. Програмування комп'ютерних мереж. Основи HTML, CSS, JAVA-SCRIPT. Методичні вказівки. Кіровоград 2007–107 с.

УДК 336.717

О. Браниш, магістр гр. ФС-18М(1,9)
Центральноукраїнський національний технічний університет

АЛЬТЕРНАТИВНІ ШЛЯХИ НАРОЩЕННЯ КАПІТАЛУ В БАНКАХ УКРАЇНИ

Проаналізовано сучасний стан особливостей формування банківського капіталу. Розглянуто проблеми капіталізації банківський установ в країні, надана оцінка їх фінансового стану в сучасних умовах. Визначені чинники впливу на створення капіталу в банку та запропоновані альтернативні шляхи для його нарощення в банківській сфері використовуючи досвід інших країн світу.
банківський капітал, інфляція, капіталізація, регулятивний капітал, реструктуризація позичок, принцип «Парето» статутний капітал

Для того, що розвивались економічні відносин в нашій державі існує потреба в удосконаленні банківської системи. Адже його високий рівень капіталізації банківської системи впливає на забезпечення фінансової стабільності в умовах вирішення глобальних проблем та світової фінансової інтеграції.

Проблема що стосується капіталізації банківських установ постійно існувала в країні, враховуючи те, що частка статутного капіталу банківської системи не перевищує 35%, а для порівняння в країнах Європи вона досягає 40%, в США – 80%. Тому, можна зазначити, що нарощення рівня капіталізації банків України це головне завдання, що вплине на покращення діяльності комерційних банків, а отже і на стан економіки держави.

Основними питаннями розробки наукових підходів щодо нарощення банківського капіталу розглядалось такими вченими як:Ж. Довгань [2], А. Загородній, О. Сліпушко, Г.Вознюк [4], А. Мороз, М. Савлук, С.Мочерний [3] та багато інших науковців. Кожен з них визначав в своїх дослідженнях сутність капіталу банку, його класифікацію проблеми та напрями його нарощення. З огляду на зміни законодавчої бази, що стосується банківського сектору, маркро- та мікроекономічних потреб на сьогоднішній день банків в додаткових ресурсах для покращення їх фінансового стану, цей напрям дослідження і досі залишається актуальним.

Метою написання статті - дослідження теоретичних аспектів, щодо формування та використання банківського капіталу в Україні з урахуванням прикладу інших країн для альтернативних шляхів його нарощення в сучасних умовах.

У 2014 році Верховна Рада ухвалила Закон «Про заходи, спрямовані на сприяння капіталізації та реструктуризації банків», яким передбачається пом’якшення вимог до банків через девальвацію гривні. Відповідний закон «Про внесення змін до Закону «Про заходи, спрямовані на сприяння капіталізації та реструктуризації банків» надає право НБУ не відносити банк до категорії проблемних і неплатоспроможних, у разі якщо зменшення розміру регулятивного капіталу, значення нормативу адекватності регулятивного капіталу, нормативів поточної і короткострокової ліквідності, збільшення обсягу негативно класифікованих активів банку, за якими слід оцінювати ризик і формувати резерви згідно з нормативно-правовими актами НБУ, зумовлене девальвацією курсу гривні або формуванням резервів для відшкодування можливих втрат за активними банківськими операціями [27].

Враховуючи сучасні вимоги, згідно з Законом України «Про спрощення процедур реорганізації та капіталізації банків» та «Про збільшення капіталу банків України» від 4 лютого 2016 року, НБУ зобов’язав банки поетапно збільшити капітал до 500 млн. гривень – до 11 липня 2024 року (таблиця 1). Основним макроекономічним фактором, що спричинив зміни вимог до статутного капіталу, стала криза 2014–2015 рр. та підписання Угоди про асоціацію України з ЄС.

Таблиця 1 - Вимоги до статутного та регулятивного капіталу

Статутний капітал має становити не менше, ніж		Мінімальний розмір регулятивного капіталу банку (Н1), що отримав банківську ліцензію до 11.07.2014р., має становити	
До 17.06.2016р.	120 млн. грн.	До 17.06.2016р.	120 млн. грн.
До 11.07.2017р.	200 млн. грн.	До 11.07.2017р.	200 млн. грн.
До 11.07.2018р.	300 млн. грн.	До 11.07.2018р.	300 млн. грн.
До 11.07.2019р.	400 млн. грн.	До 11.07.2019р.	400 млн. грн.
До 11.07.2020р.	450 млн. грн.	До 11.07.2020р.	450 млн. грн.
До 11.07.2024р.	500 млн. грн.	До 11.07.2024р.	500 млн. грн.

Джерело: [1]

Враховуючи ці вимоги, мінімальний розмір статутного капіталу має становити 120 млн. грн., а після 11 липня 2017 року він повинен бути не меншим ніж 200 млн. грн.

Із 1 січня 2018 р. НБУ запровадив щорічну оцінку стійкості банків. Вона складається з трьох етапів[26]:

Перший – перевірка аудиторськими фірмами, включеними до Реєстру аудиторських фірм, якості активів банку та прийнятності забезпечення за кредитними операціями.

Другий – екстраполяція результатів першого етапу та оцінка достатності капіталу банку станом на дату оцінки.

Третій – оцінка НБУ достатності капіталу банку за результатами стрес-тестування за базовим та несприятливим макроекономічними сценаріями на трирічному горизонті прогнозування.

Здійснимо оцінку фінансового стану банків в Україні. На рисунку 1 зображена динаміка чисельності банків в Україні.

Отже, програма реформ щодо оздоровлення банківської системи, запропонована НБУ, призвела до суттєвого зменшення їх кількості. З 2015 року до 04.2020 року їх чисельність скоротилась на 46% (це 88 банківських установ), серед них банків з іноземним капіталом зменшилось на 67% (17 установ), з національним капіталом зменшення на 70 банків (36%).

Основними проблемами формування банківської системи є: зростання недовіри до банків; подорожчання кредитних ресурсів; неплатоспроможність населення; неефективний механізм рефінансування українських банків.

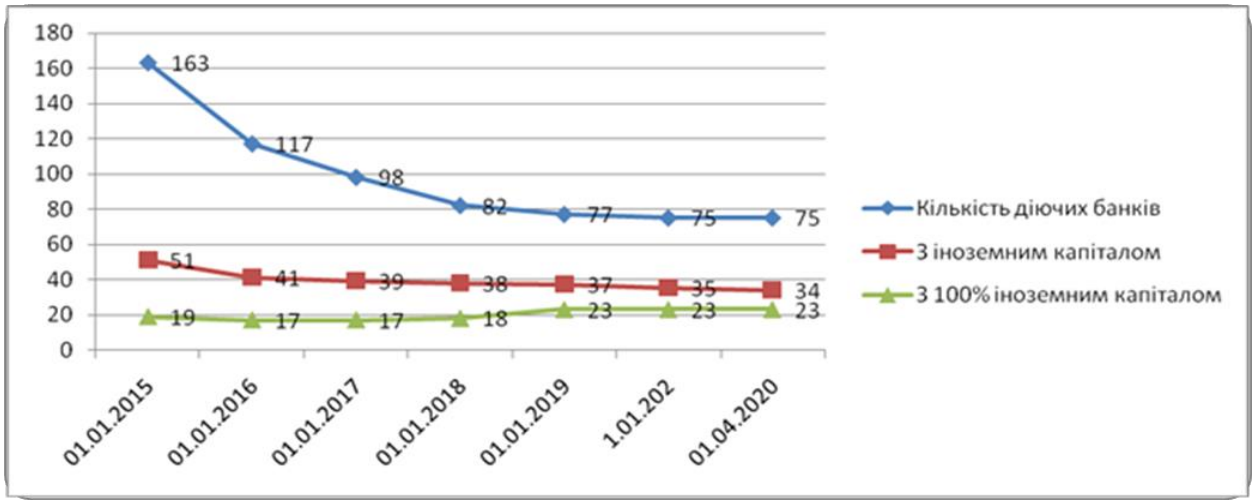


Рисунок 1 - Динаміка змін чисельності банків в Україна за 2015-2020рр., одиниць [6]

В таблиці.2 наведені дані, що характеризують розмір капіталу банківських установ.

За даними таблиці 2 побудуємо динаміку змін капіталу банківських установ в Україні (рис..2.).

Вивчаючи данні таблиці 2 та рисунку.2 ми можемо зазначити, розмір пасивів банківських установ має тенденцію до зменшення (на 3%), хоча власний капітал навпаки збільшився на 35% як і статутний капітал. Це в свою чергу вплинула і на рівень рентабельності як до 2019 мав від'ємне значення, що пояснюється збитковістю банківської діяльності за цей період. У 2017 році рентабельність найменш негативна, що зумовлене скороченням збитків банківського сектору відносно попередніх періодів. Станом на початок 2020 року його розмір складає 34,18%.

Таблиця 2 - Розмір капіталу банківських установ в Україні (млн. грн.)

Показники	01.01.15	01.01.16	01.01.17	01.01.18	01.01.19	01.01.20	01.04.20
Пасиви	1316852	1254385	1256299	1336358	1360764	1294460	1564923
Капітал всього	148023	103713	123784	163597	155650	200854	206577
Статутний капітал	180150	222170	414668	495377	465532	470712	470733
Зобов'язання банків	1168829	1150672	1132515	1172761	1205114	1293606	1358346
Зобов'язання банків в іноземній валюті	-	667246	644223	613696	487929	568561	650549
Кошти суб'єктів господар.	261372	318568	369913	403927	406166	498156	516145
Кошти фізичних осіб	416371	402137	437152	478565	508869	552592	610451
Кошти не банківських установ	-	30474	42813	22907	23794	1973	1977
Регулятивний капітал	188949	13974	109653	115817	126116	147100	
Достатність регулятивного капіталу, %	15,6	12,74	12,69	16,1	16,18	18,7	
Рентабельність капіталу, %	-30,46	-51,91	-116,74	-15,96	10,73	34,18	30,46
Частка капіталу в пасивах, %	11	8	9,9	12	11,4	15,5	13

Джерело:[7]

У 2014 році особлива увага приділялась нагляду за найбільшими системоутворюючими державними банками, такими як АТ «Ощадбанк» та АТ «Укрексімбанк», а також банками, які рекапіталізовані за участю держави, зокрема АБ «Укргазбанк», АТ «Родовідбанк» та ПАТ АКБ «Київ». У 2015 році до них додались «Український банк реконструкції та розвитку», ПАТ «Розрахунковий центр», а у 2016–2017 роках – ПАТ КБ «Приватбанк».

У 2018 році банки перейшли на новий стандарт МСФЗ 9, тому погіршили оцінку активів, що були в їхніх портфелях на початок року. У підсумку власний капітал сектору знизився на 27 млрд. грн., причому близько 90% цієї суми сформували державні банки. Проте отриманий протягом року чистий прибуток значною мірою компенсував зниження капіталу через застосування нового стандарту. Від початку року регулятивний капітал зріс на 9%, хоча власний капітал зменшився на 9.3%.

Статутний капітал банків зріс на 11,9 млрд. грн. (2.4% р/р) це було пов'язано з тим, що акціонери зробили нові внески або перевели отриманий прибуток. Розмір достатності капіталу на сьогодні перевищує мінімально необхідний. На кінець жовтня банки, яким належало 70% чистих активів, мали показник адекватності капіталу понад 15%.

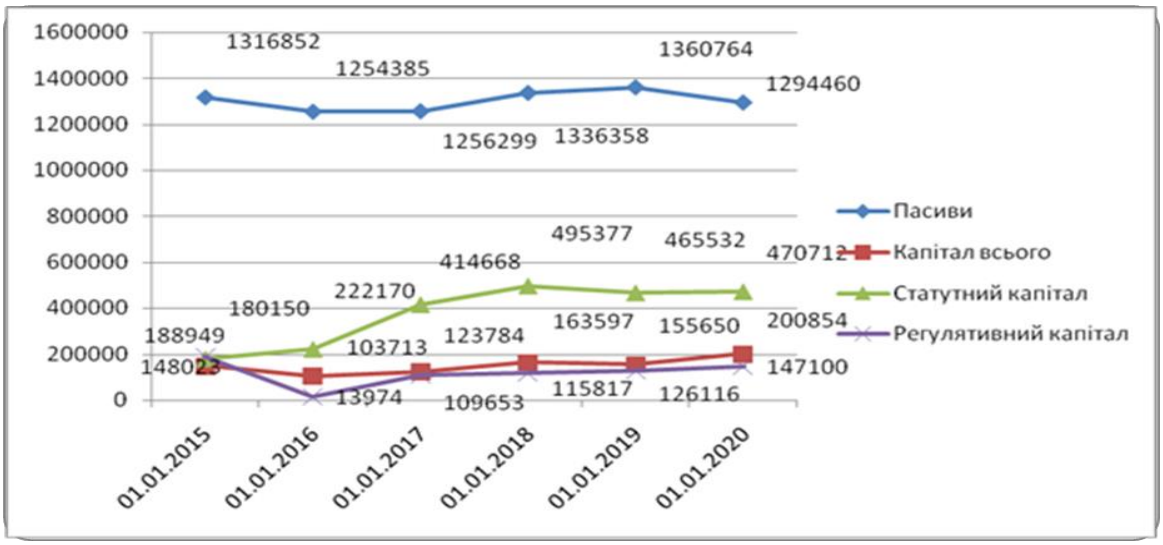


Рисунок 2 - Динаміка змін капіталу банківських установ за 2015-2019рр.,(млн. грн.) [7]

Можна зазначити, що одним з основних чинників, що негативно впливає на власний капітал банків, є наявність проблемної заборгованості в будь-якій банківській установі. Адже рівень її зростання призводить до необхідності формування значних обсягів резервів, зниження ефективності банківської діяльності та може зумовлювати її збитковість, може суттєво впливати на достатність розміру власного капіталу банків.

Якщо надавати характеристику державним банкам (це стосується також і Приватбанку), то внаслідок обмеженого розміру капіталу вони вичерпали можливості подальшого його зростання. Головною проблемою , що стосується діяльності державних банків України, то це є відсутність системного бачення їх ролі в реалізації кредитної складової національної економічної політики.

Враховуючи статистичні дані щодо формування банківського капіталу можна зазначити наступні чинники, які впливають на стабільність банківської системи:

1. Макроекономічний фактор, це загальноекономічна криза, що триває в Україні і по сьогоднішній день. Це забезпечується за рахунок нестабільності в проведенні реформ, зниження суспільного виробництва, обмеженості фінансових ресурсів в комерційних банках.
2. В наслідок збільшення кількості неплатоспроможних суб'єктів господарювання, які перебувають на стадії банкрутства. Це суттєво також впливає на розвиток банківського капіталу, в наслідок несвоєчасності сплати заборгованості підприємців, скорочення залишків на рахунках клієнтів. Особливо це стосується розвитку тіньової системи в нашій державі держави, коли намагаються поза банками здійснювати розрахунки.
3. Інфляція – це процес, що впливає на фінансову нестабільність держави. Коли обмежується можливість населення здійснювати довгострокові заощадження в комерційних банках, що знижує реальний попит на банківські продукти.
4. Наведені вище чинники пов'язані з недосконалістю існуючої законодавчої та нормативної бази в регулюванні банківської діяльності. Для запобігання погіршення фінансових можливостей банку, вони намагаються зменшити ризики використовуючи більш жорсткі вимоги до кредитоспроможності позичальника, це в сою чергу, обумовлює і недоступність позичок та обмежує базу для отримання доходів.

5. Внутрішніми факторами впливу на капітал банку є: недостатній рівень капіталізації банківської системи; високі ризики кредитування, неефективний банківський менеджмент; враховуючи зміни вимог споживача існує малий спектр послуг банку.

Зрозуміло, що для подальшого удосконалення капіталоутворюючих заходів банківської системи потрібно приділяти увагу і досвіду інших країн. Довід інших країн світу свідчить, що фінансова криза і в них існує. Тому, для цього вони створюють певний механізм для антикризового управління банківської системи країни.

Основними інструментами для цього створення є створення типових планів, методологію, сутність передбачення кризових ситуацій тощо. А саме: механізми нагляду, підвищення рівня координації та централізації (SSM), регулювання банківських криз (SRM), капіталізації, що використовує ресурси спеціального фінансового фонду обсягом 500 млрд євро (SRF), єдині правила та стандарти (single rulebook), які включають посилені вимоги до умов формування капіталу комерційних банків, національних схем гарантування виплат за депозитами, а також законодавчих норм та норм щодо запобігання банкрутствам банківських інститутів [5].

З дослідження, який нами був проведений, щодо банківської системи інших країн, альтернативними заходами для стабілізації банківської системи є:

1. Реструктуризація позичок - для вирішення проблеми неповернення кредитів банки. За рахунок викупу проблемних позичок, пролонгації строків кредитування та зниження відсоткових ставок. Це дає змогу оздоровити кредитний портфель банку.

2. У період світової фінансової кризи створена програма звільнення провідних банків від проблемних активів.

3. Об’єднання банківських установ, створюючи корпорації для управління проблемними активами, у випадку коли відбувається погіршення платоспроможності банків. Викуповуючи проблемні кредити банків з метою відновлення її ефективності шляхом продажу таких активів за максимальною ціною.

4. Вагомим із пріоритетних напрямків - зниження витрат банківських установ. Він здійснюється за рахунок стратегії щодо мінімізації витрат і базується на принципі Парето «80/20», тому перш ніж реалізовувати агресивну політику з мінімізації витрат, необхідно провести глибокий аналіз діяльності банку, виокремити основні напрямки витрат та можливості їх зменшення.

5. Значну увагу банки намагаються приділяти щодо підтримки довіри з боку клієнтів. Для цього використовують певні заходи для позитивного іміджу банку серед населення.

Розглядаючи приклади інструментів, щодо покращення розміру капіталу банків, ми можемо зазначити, що важливим кроком підвищення капіталізації банківського сектору України має стати вдосконалення системи ризик-менеджменту в банках.

Основними дієвими принципами системи управління ризиками в банківській установі є: наявність стратегії управління ризиками; наявність відповідної організаційної структури; принцип колегіальності, розділення конфліктів інтересів[5].

Висновки. Отже, підвищення рівня капіталізації банківської системи обов’язково сприятиме зростанню її конкурентоспроможності та опосередковано вдосконалить організаційну структуру банківської системи шляхом консолідації банківського капіталу.

Використання рейтингових звітів банків та підвищення ролі банківських асоціацій матимуть суттєвий вплив на окремі групи населення і сприятимуть активізації їх соціальної функції, а водночас і відкритому діалогу між банками та суспільством.

Для України найпоширеніші інструменти, які можуть використовувати для управління банківським капіталом є: рефінансування, введення тимчасових адміністрацій, регулювання рівня мінімального резервування, видача стабілізаційних кредитів, реструктуризація заборгованостей, зменшення витрат внаслідок скорочення мережі банківських філій (особливо неприбуткових) тощо.

Можна зазначити, що інструменти антикризового управління які наша держава може застосовувати, не завжди має позитивні наслідки в процесі подолання кризи. Як приклад це кредити рефінансування НБУ. Тому, для банківської системи значні обсяги рефінансування стали одним із факторів який вплинув на значну девальвацію національної валюти. Тому, в подальших дослідженнях слід ґрунтовно вивчати наслідки впливу кожного із антикризових інструментів, які планується використовувати державою в межах системи.

Список літератури

1. Базельські основні принципи ефективного банківського нагляду. URL: http://www.bank.gov.ua/Bank_supervision/ (дата звернення: 15.02.20)
2. Довгань Ж. Діяльність вітчизняних банківських установ в умовах економічної кризи. Світ фінансів. Вип.4. 2010., С. 196-201.
3. Економічна енциклопедія. У трьох томах. за ред. С. В. Мочерний та ін. : Видавничий центр «Академія». Т.2, Київ, 2001. 848 с.
4. Загородній А. Г., Сліпушко О.М., Вознюк Г.Л. Словник банківських термінів. Банківська справа: Термінологічний словник. К. : Вид-во «Аконіт», 2000. 605 с.
5. Міжнародний досвід капіталізації банків та її вплив на боргову сферу . Деревко О.С. Ринок фінансових послуг. 2016. URL: file:///C:/Users/Юра.админ-ПК/Downloads/Npndfi_2016_3_8.pdf (дата звернення: 24.03.20)
6. Основні показники діяльності банків України URL: http://www.bank.gov.ua/control/uk/publish/article (дата звернення 25.03.20
7. Статистичний бюлетень Національного банку України (електронне видання). 2019. URL: http://www.bank.gov.ua/Statist/elbul.htm (дата звернення 25.03.20)

УДК 004

Д. Будейкін, магістр гр. КН-18М-1,4
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ МОДУЛЮ РЕЛЕЙНОГО ЗАХИСТУ ДЛЯ КОМПЛЕКСНОЇ ТРАНСФОРМАТОРНОЇ ПІДСТАНЦІЇ НА ПІВДЕННОУКРАЇНСЬКІЙ АЕС

У статті проведено дослідження модулю релейного захисту для комплексної трансформаторної підстанції на Південноукраїнській атомній елекстростанції. Метою роботи є створення програмного продукту, який забезпечує функціональність модулю релейного захисту для комплексної трансформаторної підстанції на Південноукраїнській атомній елекстростанції за визначеними технічними вимогами. Об'єктом дослідження є процеси моніторингу та контролю швидких процесів в режимі реального часу. Предметом дослідження є методи моніторингу та контролю швидких процесів в режимі реального часу. На основі дослідження побудовано алгоритми роботи модулю релейного захисту, створено програмний продукт, який реалізує розроблені алгоритми та принципи функціонування. В процесі роботи виконано аналіз існуючих засобів релейного захисту електричних систем та проведено дослідження доцільності створення нових мікропроцесорних реле та терміналів; створено програмне забезпечення, яке на відміну існуючих аналогів, використовує переваги сумісного використання FPGA та мікроконтролеру, що дозволило витримати посилені часові вимоги щодо швидкості реакції системи на аварійні ситуації. Результатом роботи є реалізація програмного забезпечення, яка завдяки системному підходу до розробки структури, додатково зменшує час реакції системи за рахунок використання більш сучасних протоколів з керуючою ЕОМ. Розроблено інструкції по роботі з програмними засобами. Програма може виконуватися на мікропроцесорних системах, які мають в основі мікроконтролери STM32F449. Для кроскомпіляції програмного коду було використано компілятор C++ для архітектури ARMv7. Результати роботи впроваджено в модулях релейного захисту для комплексної трансформаторної підстанції на Південноукраїнській атомній елекстростанції.

програма, моніторинг, контроль, мікроконтролер, релейний захист

Постановка проблеми. Системи електропостачання є складними виробничими об'єктами кібернетичного типу, всі елементи яких беруть участь в єдиному виробничому процесі, основними специфічними особливостями якого є швидкоплинність явищ і неминучість пошкоджень аварійного характеру. Тому надійне та економічне функціонування систем можливе тільки при автоматичному керуванні ними. Для цієї мети використовується комплекс автоматичних пристроїв, серед яких першорядне значення мають пристрої релейного захисту та автоматики.

Зростання споживання електроенергії і ускладнення систем електропостачання вимагають постійного вдосконалення цих пристроїв. Спостерігається тенденція створення автоматизованих систем керування на основі використання цифрових універсальних та спеціалізованих обчислювальних машин. Разом з тим широко застосовуються і найпростіші засоби захисту і автоматики: плавкі запобіжники, автоматичні вимикачі, магнітні пускачі, реле прямої дії, магнітні трансформатори струму та інші. Найбільш поширені захисти по струму, прості пристрої автоматичного повторного включення, автоматичного включення резервного джерела живлення та автоматичного частотного розвантаження.

Надійність роботи електроенергетичних систем в значній мірі визначається правильністю роботи пристроїв релейного захисту та автоматики (РЗА), що досягається вдосконаленням методів та засобів, як релейного захисту так і належною якістю технічного обслуговування при відповідній кваліфікації персоналу,який експлуатує пристрої РЗА.

Відповідно до вимог ПТЕ ЕС і М (п.12.9.1) силове електроустаткування електростанцій, підстанцій, теплових мереж, повітряних та кабельних ліній електропередавання повинне бути захищене пристроями релейного захисту від коротких замикань і порушень нормальних режимів.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у модулі релейного захисту для комплексної трансформаторної підстанції на Південноукраїнській АЕС.

Мета й завдання дослідження. Метою роботи є створення системи контролю засобів релейного захисту, яка б відповідала поставленим технічним вимогам.

Таким чином,задачами роботи є аналіз існуючих засобів релейного захисту електричних систем та дослідження доцільності створення нових мікропроцесорних реле та терміналів; створення програмного коду для забезпечення функціонування та контроль якості роботи засобів релейного захисту.

Об'єкт дослідження– методи виконання та контролю релейного захисту трансформаторної підстанції на Південноукраїнській АЕС.

Предмет дослідження – модулі релейного захисту для комплексної трансформаторної підстанції на Південноукраїнській АЕС.

Методи дослідження – при виконанні роботи було використано наступні методи: аналіз при вивчені технічних вимог до пристрою та програмного забезпечення; структурний аналіз для визначення необхідних складових компонентів пристрою та їх характеристик; системний підхід для розробки порядку взаємодії компонентів програмного забезпечення; моделювання для прогнозування характеристик пристрою під керуваннямрозробленого програмного продукту.

Виклад основного матеріалу. Згідно з технічним завданням(ТЗ) до розробки системи, яка пропонується до розробки, розглянемо основні апаратно програмні модулі, що будуть задіяні при роботі системи.

Згідно рисунка 1 ми маємо структурно два взаємопов'язані елементи(модулі), які складають цільний мегамодуль.

Ліва частина мегамодуля — підмодуль FPGA. Хоча цей модуль і не входить до мети розробки, але є складовою частиною мегамодуля, який входить до окремого апаратного засобу реалізації всієї системи.

FPGA(field-programmable gate array) - пристрій на напівпровідниках, які можуть бути налаштовані користувачем або розробником після його виготовлення.

За іншою термінологією: «програмується користувачем» або PLIS. PLIS програмуються шляхом зміни логіки роботи принципової схеми.

FPGA можуть бути модифікованими практично в будь-який час у процесі їх використання. PLIS складаються з логічних блоків, однакових перемикачів з великою кількістю входів і одним виходом (логічні вентилі або gates). У цифрових схемах такі перемикачі реалізують базові логічні операції AND, NAND, OR, NOR і XOR. У більшості сучасних мікропроцесорів функції логічних блоків фіксовані і не можуть змінюватися. Принципова відмінність PLIS полягає в тому, що і функції блоків, і конфігурація з'єднань між ними можуть змінюватися за допомогою спеціальних сигналів, що посилаються схемою.

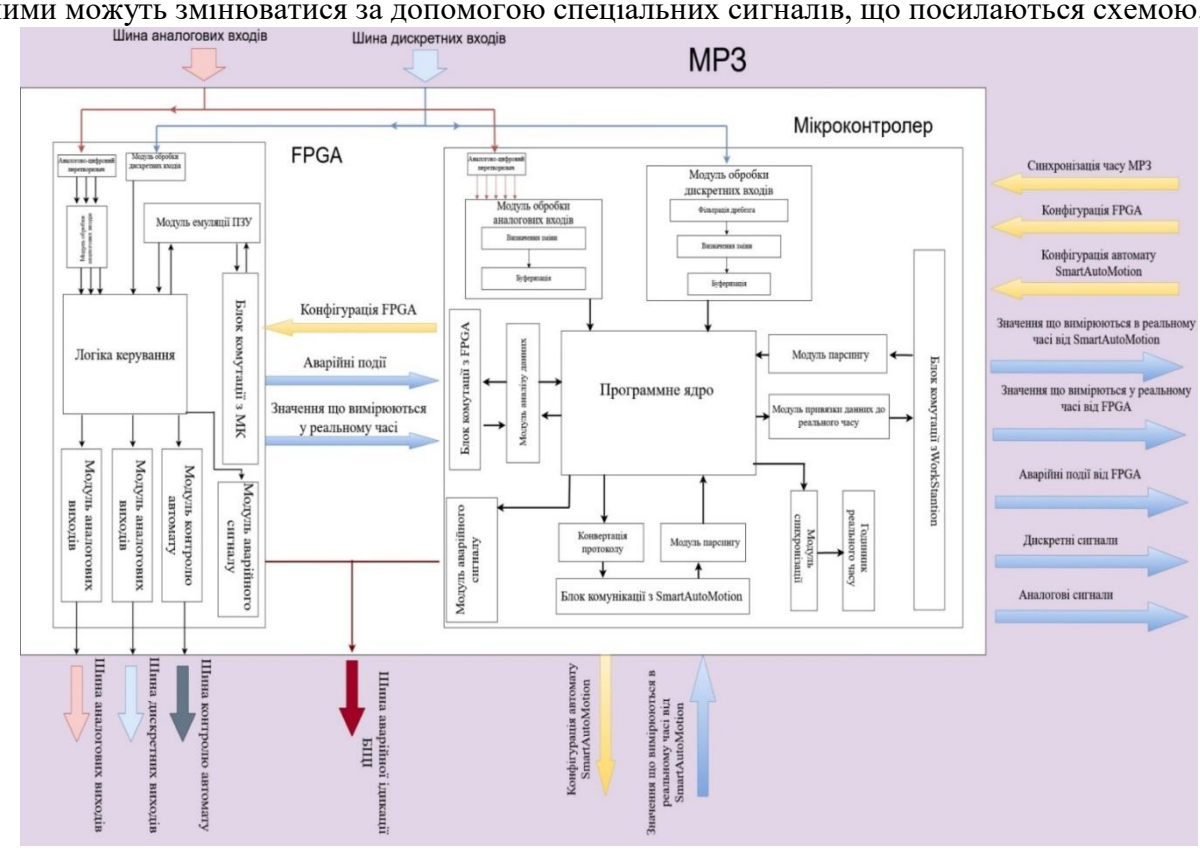


Рисунок 1 – Структурна схема системи

У деяких спеціалізованих інтегральних схемах (ASIC) використовуються логічні матриці, аналогічні до PLIS архітектурою, однак вони конфігуруються один раз у процесі виробництва, в той час як PLIS можна постійно перепрограмувати та змінювати топологію з'єднань в процесі використання. Однак така гнучкість вимагає істотного збільшення кількості транзисторів у мікросхемі.

Завдяки програмованому характеристикам, FPGA може пристосовуватися до великої кількості різних задач. Комплексні рішення, що складаються з пристроїв FPGA, сучасного програмного забезпечення та які налаштовані, на використання IP ядер для додатків, таких як:

- Аерокосмічний та захист - радіаційно-стійкий FPGA.
- Інтелектуальна власність для обробки зображень, генерації сигналів та часткової реконфігурації для SDR.
- ASIC прототипування - прототипування ASIC з FPGA дозволяє швидко та точно моделювати систему SoC та перевіряти вбудоване програмне забезпечення
- Аудіо - FPGA і цільові дизайнерські платформи дозволяють підвищити рівень гнучкості, прискорити час виходу на ринок і знизити загальні неповторні витрати на

інженерні технології (NRE) для широкого спектру аудіо-, комунікаційних та мультимедійних додатків.

- Автомобільна промисловість - Автомобільні рішення з кремнію та IP для систем шлюзу та допомоги водіям, комфорту, зручності та інформаційних розваг у транспортних засобах. - Дізнайтеся, як Xilinx FPGA дозволяє автомобільні системи

- Broadcast & Pro AV - Адаптуйте до швидких змін, що змінюються, і подовжуйте життєві цикли виробів за допомогою платформ для цільового дизайну та рішень для високопрофесійних професійних систем мовлення.

- Побутова електроніка - економічно ефективні рішення, що дають можливість наступним поколінням повнофункціональних споживчих додатків, таких як збірні телефони, цифрові дисплеї на плоскій панелі, інформаційні прилади, домашні мережі та житлові приставки.

- Центр обробки даних - Розроблений для високопропускної здатності, серверів з низькою затримкою, мережевих додатків та додатків для зберігання даних, щоб принести більш високу цінність у хмарні розгортання.

- Високопродуктивні обчислення та зберігання даних - рішення для мережевого зберігання даних (NAS), мережі зберігання даних (SAN), серверів та пристроїв зберігання даних.

- Промислові - FPGA та цільові дизайнерські платформи для промислового, наукового та медичного (ISM) дозволяють підвищити ступінь гнучкості, пришвидшити час виходу на ринок та знизити загальні неповторні витрати на інженерні технології (NRE) для широкого спектру застосувань, таких як промислові візуалізація та спостереження, промислова автоматизація та медичне обладнання для візуалізації.

- Медичні - для діагностичних, моніторингових та терапевтичних застосувань сімейства Virtex FPGA та Spartan® FPGA можна використовувати для задоволення діапазону потреб в інтерфейсі обробки, відображення та вводу/виводу.

- Безпека - Xilinx пропонує рішення, що відповідають розвиваючим потребам програм безпеки, від контролю доступу до систем спостереження та безпеки.

- Обробка відео та зображень - Xilinx FPGA та цільові дизайнерські платформи дозволяють підвищити рівень гнучкості, прискорити час виходу на ринок та знизити загальні неповторні витрати на інженерні технології (NRE) для широкого спектру застосувань для відео та зображень.

- Провідний зв'язок - комплексні рішення для перепрограмованої мережевої обробки пакетних лінійних карток, Framer/MAC, серійних задніх планок тощо.

- Бездротова комунікація - RF, базовий діапазон, з'єднання, транспортні та мережеві рішення для бездротового обладнання, відповідні стандартам, таким як WCDMA, HSDPA, WiMAX та інші.

Виходячи з того, що модуль FPGA не є модулем для розробки, будемо його розглядати як апаратний пристрі, який має певні властивості комутатора шини аналогових та дискретних пристроїв з можливістю налаштування кількості каналів, або ширини шини.

МРЗ — модуль релєйного захисту. Це головний, точки зору ТЗ. Його головними функціями є

- отримання з відповідної шини набору даних;
- обробка отриманих даних у реальному часі;
- формування пакетів передачі для CAN;
- конфігурація FPGA;
- синхронізація часу між блоками МРЗ;
- передача отриманих даних до сервера обробки керування та візуалізації(верхній рівень — ПОМ).

МРЗ складається з програмного ядра, яке базується(запрограмоване) на мікроконтролері серії ARM Cortex-M4-based STM32F446.

Пристрої STM32F446 засновані на високоефективному 32-бітному ядрі RISC ARM Cortex-M4, який працює на частоті до 180 МГц. Ядро Cortex-M4 має єдину точність блоку з плаваючою точкою (FPU), яка підтримує всі інструкції та типи обробки даних ARM з однією точністю по типах даних. У STM реалізовано повний набір інструкцій DSP та блок захисту пам'яті (MPU), який підвищує безпеку програми. Мікроконтролери STM32F446 містять вбудовані швидкодіючі пам'ять (флеш-пам'ять до 512 Кбайт, до 128 Кбайт SRAM), що збільшується до 4 Кбайт за допомогою резервної копії SRAM, а також широкий діапазон вдосконального введення/виведення та периферійних пристроїв, які підключені до двох шин APB, двох шин AHB та 32-бітної матриці шини AHB. Пристрій має три 12-бітні АЦП, два ЦАПи, RTC з низькою потужністю, дванадцять 16-бітових таймери загального призначення, включаючи два таймери ШІМ для керування двигуноми, два 32-бітові таймери загального призначення. Він також має стандартний та розширений інтерфейс зв'язку:

-чотирb I2C;

-чотири SPI;

- три I2S повністю симплексні;

- чотири USART плюс два UART;

- повна швидкість USB OTG та високошвидкісний USB OTG з повно -швидкісним (з ULPI), обидва із спеціалізованими силовими рейками, що дозволяють використовувати їх у всьому діапазоні потужності;

- два CAN;

- два послідовних аудіоінтерфейси SAI. Для досягнення точності аудіо-класу SAI можна запускати через спеціалізований внутрішній аудіо PLL;

- інтерфейс SDIO/MMC;

- інтерфейс камери; • HDMI-CEC; • приймач SPDIF (SPDIFRx);

- QuadSPI. Розширені периферійні пристрої включають SDIO, гнучкий інтерфейс управління пам’яттю (FMC), інтерфейс камери для датчиків CMOS.

Отримання даних у модулі MP3 микрнується через два порти — аналоговий та дискретний. Аналогові сигнали обробляються вбудованими АЦП.

Для прийому аналогових сигналів STM32F446 має три вбудовані 12-бітові аналого-цифрові перетворювачі. Кожен АЦП має до 16 зовнішніх каналів, які виконують перетворення в режимі одиночного зняття або сканування сигналу. У режимі сканування автоматичне перетворення здійснюється на вибраній групі аналогових входів.

Для прийому дискретних сигналів використовують стандартні порти введення/виведення. Порти введення/виведення загального призначення (GPIO) Кожен з GPIO-пінів може бути налаштований програмним забезпеченням як вихід ("push-pull" або "open-drain", з або/без підтягування або пониження), як вхід (плаваючий, з або/без підтягування або пониження), або як периферійна альтернативна функція. Більшість пінів GPIO поділяються цифровими або аналоговими альтернативними функціями. Всі реєстратори мають високий струм і мають вибір швидкості для кращого управління внутрішнім шумом, енергоспоживанням та електромагнітною емісією. Конфігурацію введення/виведення можна заблокувати, якщо потрібно, дотримуючись певної послідовності, щоб уникнути помилкового запису на введення/виведення Регістри швидкого введення/виведення, що дозволяють максимально встановлювати введення/ виведення до 90 МГц.

Для передачі даних на верній рівень використовується модуль контролера (bxCAN) CAN відповідає стандартам 2.0A та B(активний) з бітрейтом до 1 Мбіт/с. Вони можуть приймати і передавати стандартні кадри з 11-бітовими ідентифікаторами, а також розширені кадри з 29-бітовими ідентифікаторами. Кожен CAN має три поштові скриньки для передачі, отримують FIFOS з 3 ступенями та 28 спільних масштабованих банків фільтрів (усі вони можуть бути використані, навіть якщо використовується одна CAN). 256 байт SRAM виділяється для кожного CAN.

Уся система працюю у реальному часі. Це обумовленно тим, що система забезпечує захист роботи дуже небезпечного обладнання, яке пов'язано з безпекою життя не тільки особистості(обслуговуючого персоналу), але й з безпекою цілих екологічних регіонів і навіть країн.

Процеси обробки, формування , і передачі інформації мегамодулем, повинно забезпечуватися підмодулем системи – МРЗ. Щоб отримати відповідність сигнал-обробка-передача - реакція, потрібно, при здійсненні розробки програмно-апаратного модуля МРЗ передбачити real time обробки сигналу. Такі можливості надає мікроконтролеру STM вбудований RTC(rial time clock).

RTC, дозволяє резервне копіювання SRAM та регістри резервного копіювання Домен резервного копіювання включає в себе:

- Годинник реального часу (RTC)
- 4 Кбайт резервного копіювання SRAM
- 20 реєстрів резервного копіювання Час реального часу (RTC) - незалежний таймер/лічильник BCD. При цьому виділені регістри містять другу, хвилину, годину (через 12/24 години), тиждень день, дату, місяць, рік у форматі BCD (двійково кодований десятковій). Виправлення на 28, 29 (високосний рік), 30 та 31 день місяця виконуються автоматично.

RTC забезпечує програмований ALARM та програмовані періодичні переривання з пробудженням із режимів зупинки та очікування. Також доступне значення субсекунд у двійковому форматі. RTC працює, як зовнішній кристал, резонатор або внутрішній низькопотужний RC-генератор генератор 32,768 кГц, або високошвидкісний зовнішній годинник, розділений на 128. Внутрішній низькошвидкісний RC має типову частоту 32 кГц.

RTC можна калібрувати, використовуючи зовнішній вихід 512 Гц для компенсації будь-якого природного кварцового відхилення. Два регістри тривоги використовуються для генерації тривоги в певний час, а календарі поля можуть бути незалежно замасковані для порівняння тривоги. Для генерування періодичного переривання доступний 16-бітний програмований двійковий автоматичний датчика з програмованою роздільною здатністю, який дозволяє автоматично пробуджувати та періодичні надавати тривожні сигнали кожні 120 мкс, або кожні 36 годин. Для часового базового годинника використовується 20-бітний декодер. За замовчуванням генерується базовий час в 1 секунду з тактової частоти на 32,768 кГц. Резервна копія SRAM 4-кбайт є областю пам'яті EEPROM. Він може використовуватися для зберігання даних, які потрібно зберігати в режимі VBAT та в режимі очікування. Ця область пам'яті відключена за замовчуванням, щоб мінімізувати споживання електроенергії. Це можна ввімкнути програмним забезпеченням. Реєстри резервного копіювання - це 32-бітні регістри, які використовуються для зберігання 80 байт даних програм користувача, коли живлення VDD відсутнє. Реєстри резервного копіювання не скидаються системою, скидається живлення або коли пристрій прокидається з режиму очікування. Додаткові 32-бітні регістри містять програмовану тривогу під секунди, секунди, хвилини, години, день та дата. Як резервне копіювання SRAM, регістри RTC та резервного копіювання подаються через комутатор, який живиться або від джерела VDD, якщо він присутній, або від штифта VBAT.(У нашому випадку комутатором є FPGA).

Розробка структурної схеми

Виходячі з попереднього підрозділу, зрозуміло, головним елементомсистеми, яка розроблюється є окремий модуль МРЗ. Таких модулів може бути деяка кількість, що може бути обмежена ознаками RTC(rial time clock). Система обмежена не тільки проходженням даних, які передаються, формуються або передаються а, що є найголовнішим, виключним станом системи(ALARM)!

Прийнявши до уваги, що на верхньому рівні ми, апріорі, маємо операційну систему з не визначеним відношенням до проходження процесів(Windows, Unix(Linux), MacOs), то передача сигналів на рівні МРЗ повинна вирішуватися на рівні понять операційних систем реального часу(RTOS).

RTOS — визначають, що функції обробки даних повинні бути завершені у вказаному ліміті часу - невиконання цих умов, приведених до повної відтворення в роботі всієї системи.

Механізм роботи системи, що працює на регістації помилок релєйної системи, має в своєму розпорядженні пристосуванням функцій жорсткого реального режиму. Помилка реактора довго розвивається при зміненні розташування у зоні розщеплення уранового стрижня у відведений ліміт часу. Відкрита система, що знаходиться в цьому ліміті, може привести до повногозламу реактора, який можна уникнути завдяки застосування ідей RTOS.

Висновок. У статті розглянуто та проаналізовано, що при численних перевагах мікропроцесорних пристроїв, їх недоліки не є суттєвими. Впровадження мікропроцесорних технологій в підприємства електроенергетичної галузі доцільно і обґрунтовано безліччю незаперечних переваг. Сучасні АЕС потребують використання швидкодійних, надійних модулів релейного захисту. Завдяки саме цьому на науковому дослідженню, вдалося розробити програмне забезпечення, яке виконує свої функції діагностики краще аналогічних модулів.

Список літератури

1. Босько В.В. Анализ и сравнительное исследование перспективных направлений развития цифровых телекоммуникационных систем и сетей / Смирнов А.А., Босько В.В., Мелешко Е.В. // Системи обробки інформації. – Х.: ХУ ПС, 2008. – Вип.7(74). – С.120-123.
2. Босько В.В. Разработка методики оценки середнего времени обслуживания информационных пакетов в телекоммуникационной сети / Смирнов А.А., Босько В.В., Мелешко Е.В. // Системи управління, навігації та зв'язку. – Київ: ДП «Центральний науково-дослідний інститут навігації і управління», 2009. – Вип. 2(10). – С.162-165.
3. Босько В.В. Разработка математической модели процесса динамического управления маршрутизацией данных в телекоммуникационной сети / Смирнов А.А., Босько В.В. // Системи управління, навігації та зв'язку. – К.: ДП «ЦНДІ навігації і управління», 2009. – Вип. 3(11). – С.208-210.
4. Босько В.В. Разработка метода определения оптимального множества путей передачи информации в телекоммуникационной сети / Смирнов А.А., Босько В.В. // Збірник наукових праць. – Х.: ХУПС, 2009. – Вип. 3(21). – С.102-108.
5. В.В.Босько. Разработка метода прогнозирования поведения информационного потока в телекоммуникационной сети // Збірник наукових праць. Харківського університету Повітряних Сил: – Х.:ХУ ПС, – 2010.-Вип. 3 (25) .- С.126-130.
6. Босько В.В. Исследование особенностей построения современных телекоммуникационных систем и сетей / Смирнов А.А., Босько В.В. // Проблемы информатики и моделирования. Материалы восьмой международной научно-технической конференции 26-28 ноября. – Х.: НТУ "ХПИ", 2008. – С.54.
7. Босько В.В. Исследование влияния времени мониторинга телекоммуникационной сети на точность прогнозирования поведения трафика / Смирнов А.А., Босько В.В. // Перша міжнародна науково-практична конференція "Проблеми й перспективи розвитку IT-індустрії" м. Харків , 18-19 листопада 2009р. – С.198-200.
8. Босько В.В. Анализ математических моделей телекоммуникационной сети / Смирнов А.А., Босько В.В. // Проблемы информатики и моделирования. Материалы девятой международной научно-технической конференции 26-28 ноября. – Х.: НТУ "ХПИ", 2009. – С.52-53.
9. Босько В.В. Метод повышения оперативности передачи данных в телекоммуникационной сети / Смирнов А.А., Босько В.В. // Збірник тез доповідей науково-практичної конференції "Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку" 24-25 березня. – Х.: АВВ МВС України, 2010. – С.54.
10. Босько В.В. Динамическое управление процессом маршрутизации данных в телекоммуникационной сети / Смирнов А.А., Босько В.В. // Тези доповідей Міжнародної науково-практичної конференції м. Вінниця, Україна 19-21 травня 2010 року. – Вінниця: ВНТУ, 2010. – С.231-232.

УДК 004

Д. Будніков, магістр гр. КІ-18М-1,4
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ ПРОТИДІЇ ЗАГРОЗАМ КОРПОРАТИВНІЙ МЕРЕЖІ

У статті розроблено програмне забезпечення, яке призначено для системи протидії загрозам корпоративній мережі. Метою розробки є дослідження та програмна реалізація системи протидії загрозам корпоративній мережі. Об'єктом дослідження є процес протидії загрозам корпоративній мережі. Предметом дослідження є методи протидії загрозам корпоративній мережі. Методи дослідження базуються на методах захисту інформації, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи протидії загрозам корпоративній мережі. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення. Розроблено зручний інтерфейс користувача.
комп'ютерна інженерія, захисту інформації, корпоративна мережа

Постановка проблеми. Хочемо ми того чи ні, але з кожним роком хакери використовують усе більше витончені способи кібератак, а постраждати від них може будь-яка компанія – і міжнародний гігант, і невелике сімейне підприємство. Загальносвітовий збиток від кібернападів виміряється мільярдами доларів. Віруси не тільки б'ють по репутації компанії, але й порушують бізнес-процеси. Наприклад, японському автовиробникові Honda через атаку, яка відбулася в червні 2017 року, довелося припинити роботу заводу на цілу добу.

Як показало розслідування інцидентів, викликаних шифрувальниками WannaCry і Petya, віруси використовували ту саму уразливість у реалізації протоколу SMB в операційних системах Windows. Petya, що атакував компанії по усьому світі через місяць після WannaCry, наніс нітрохи не менший збиток, чим його попередник, із чого можна зробити вивід, що до рекомендацій з відновлення ПЗ й установці латок мало хто прислухався. Результат, думаю, усі бачили в заголовках ЗМІ.

Перші екземпляри вірусу найчастіше проникають у мережу через корпоративну пошту. Наприклад, відділ кадрів одержує листа з резюме у вкладенні. Співробітник HR-служби при всьому бажанні не зможе догадатися, заражене воно чи ні, тому що всі листи відправляються здобувачами з особистих адрес.

Зараження може відбуватися непомітно: вірус самостійно поширюється по мережі компанії через уразливі комп'ютери. Справа в тому, що трафік інспектується в основному тільки на ділянці «Інтернет – корпоративна мережа». Якщо вірус уже усередині, дослідження трафіку на погрози найчастіше не здійснюється.

Поширюючись неймовірно швидко, вірус може відразу паралізувати всі бізнес-процеси. В основному мету зловмисників – вимагання, але в шифрувальника є й інші неприємні наслідки: зупинка роботи промислового встаткування, банкоматів, кас у магазинах.

Якщо на комп'ютерах користувачів і серверах є уразливість, то через неї, як за запрошенням, за периметр можуть потрапити й інші погрози – наприклад, шпигунське ПЗ, що завдає шкоди компанії нишком, крадучи конфіденційні дані. Це знов-таки лише один з можливих сценаріїв. Уразливості є скрізь, навіть у самих пророблених програмах або операційних системах, а варіантів скористатися ними дуже багато.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи протидії загрозам корпоративній мережі.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи протидії загрозам корпоративній мережі.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем протидії загрозам корпоративній мережі.
– Дослідження системи протидії загрозам корпоративній мережі.
– Програмна реалізація системи протидії загрозам корпоративній мережі.

Об'єктом дослідження є процес протидії загрозам корпоративній мережі.

Предметом дослідження є методи протидії загрозам корпоративній мережі.

Методи дослідження базуються на методах захисту інформації, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Забезпечення надійного захисту корпоративної мережі – дуже складний процес, що являє собою безперервну й постійну послідовність дій по реалізації комплексу мір інформаційної безпеки.

Що можуть зробити компанії для захисту корпоративної мережі? Більшість експертів по безпеці рекомендують почати з ретельного відбору (у тому числі по етичних і моральних критеріях) співробітників, у завдання яких буде входити адміністрування мережі й, зокрема, створення й експлуатація підсистеми інформаційної безпеки корпоративної мережі. І хоча багато керівників думають, що самими широкими правами доступу до важливого для компанії даним володіють тільки вони разом з адвокатами й бухгалтерами, але це не так. Доступом до всіх конфіденційних матеріалів володіють адміністратори корпоративної мережі. А оскільки вони, як правило, не мають участь на паях у прибутках компанії, то являють собою одну із самих серйозних потенційних погроз для безпеки компанії. Тому цілком очевидно, що люди, що претендують на цю роботу, повинні бути ретельно перевірені.

Одне з останніх віянь моди – прийом на посаду адміністратора мережі колишніх хакерів. І дійсно, хто краще їх зможе підтримувати й тестувати безпека комп'ютерної мережі й давати необхідні рекомендації? Однак є й інша сторона медалі: надати привілейований доступ до конфіденційної інформації про структуру мережі й про місцезнаходження найбільш важливих даних сумнівної особистості, що, з одного боку, підкована технічно, а з іншого боку – не пристосована до серйозної й кропіткої роботи із забезпечення безпеки, – тут є, над чим подумати.

Варто враховувати, що фахівець із безпеки інформації відповідає за розробку, реалізацію й експлуатацію системи забезпечення інформаційної безпеки, спрямованої на підтримку цілісності, придатності й конфіденційності даних, накопичених у компанії. У його функції входить забезпечення й фізичної (технічні засоби, лінії зв'язку й віддалені комп'ютери), і логічної (самі дані, прикладні програми, операційна система) захисту інформаційних ресурсів.

Складність створення системи захисту інформації обумовлена тим, що дані можуть бути викрадені з комп'ютера (скопійовані), одночасно залишаючись на місці. До того ж цінність деяких даних полягає у володінні ними, а не в їхньому знищенні або зміні. При забезпеченні безпеки інформації необхідно приймати не тільки витрати на закупівлю й установку різних технічних або програмних засобів, але й питання кваліфікованого визначення розумних границь безпеки й відповідної підтримки системи в працездатному стані. Об'єктами зазіхань можуть бути як самі матеріальні технічні засоби (комп'ютери й периферія), так і програмне забезпечення й бази даних. Кожний збій роботи комп'ютерної мережі – це не тільки неприємності для працівників компанії й мережних адміністраторів: у міру розвитку технологій електронних платежів і безпаперового документообігу серйозний збій комп'ютерних мереж може паралізувати роботу цілих корпорацій і банків, що приведе

до значних збитків. Тому захист даних у комп'ютерних мережах стає однієї із самих гострих проблем.

Головним завданням, розв'язуваної на етапі проектування підсистеми інформаційної безпеки, є забезпечення безпеки інформації в комп'ютерних мережах, що припускає створення перешкод для будь-яких несанкціонованих спроб розкрадання або модифікації даних, переданих у мережі. У той же час дуже важливо зберегти такі властивості інформації, як доступність, цілісність і конфіденційність. Доступність інформації має на увазі забезпечення своєчасного й безперешкодного доступу користувачів до їхніх відомостей, що цікавлять. Цілісність інформації полягає в її існуванні в неспотвореному виді, тобто незмінному стосовно деякого фіксованого її стану. Конфіденційність припускає необхідність введення обмежень доступу до даної інформації для певного кола користувачів. Слід також зазначити, що такі області, як банківська й фінансова діяльність, державне керування, оборонні й спеціальні структури, вимагають спеціальних додаткових заходів безпеки даних і висувають підвищені вимоги до надійності функціонування інформаційних систем.

Перш ніж приступитися до створення підсистеми інформаційної безпеки мережі, необхідно розробити концепції й політики безпеки, які будуть прийняті в компанії і які нерозривно пов'язані із загальним планом її розвитку. Правильна політика безпеки дозволить не тільки врахувати всі вимоги по безпеці, але й оптимально використовувати фінансові засоби, необхідні для її реалізації. У політику безпеки повинні бути враховані всі складові інформаційної безпеки. У першу чергу потрібно визначити список об'єктів, на які можуть бути спрямовані погрози. Природно, у даний список повинні бути включені всі критично важливі вузли корпоративної мережі.

Необхідно провести аудита й аналіз існуючих і можливих зовнішніх і внутрішніх погроз, визначити їхні джерела й оцінити ризики. Ці відомості дозволять скласти реальне уявлення про існуючий і прогнозований ступінь уразливості корпоративної мережі, а також про потреби в захисті інформаційних ресурсів. Багато хто думають, що основна погроза виходить зовні – від зовнішніх, сторонніх осіб і організацій, від хакерів, які намагаються проникнути в мережу компанії й одержати доступ до її інформації й ресурсів. Але хто небезпечніше: хакер, що намагається проникнути в корпоративну мережу ззовні, або співробітник компанії, що вже має до неї доступ? До того ж зловмисник може знайти в компанії людини, нечистого на руку, або обдурити довірливого користувача, використовуючи різні психологічні прийоми. Витрачаючи величезні гроші на захист компанії, у жодному разі не можна забувати про небезпеку внутрішніх погроз.

За результатами проведеного аналізу можливих погроз визначаються методи й засоби виявлення ворожого впливу й захисту від відомих погроз, а також методи й засоби реагування при інцидентах. Необхідно пам'ятати, що збиток часто наноситься не через чийсь злий намір, а просто через елементарні помилки користувачів, які випадково псують або видаляють дані, украй важливі для компанії.

З урахуванням всіх обставин приймаються рішення про розробку й реалізацію комплексних проектів на базі широкого спектра систем і рішень, сполучення яких дозволяє забезпечити ефективний захист інформаційних ресурсів корпоративної мережі.

Одним з основних компонентів системи захисту корпоративної мережі є міжмережеві екрани, які забезпечують організацію захисного периметра, що захищає інформаційні ресурси організації від доступу ззовні й контролюючої процедури взаємодії користувачів корпоративної мережі із зовнішніми мережами, в основному з Інтернетом. Міжмережевий екран забезпечує рішення таких завдань, як захист локальної мережі від несанкціонованого доступу із зовнішніх мереж, безпечний доступ в Інтернет корпоративних користувачів, віддалене підключення користувачів до ресурсів корпоративної інформаційної системи. На критично важливі вузли корпоративної мережі можлива установка окремого міжмережевого екрана.

Антивірусні продукти забезпечують надійний захист серверів, робочих станцій, поштових систем і Інтернет-трафіку від поразки комп'ютерними вірусами.

Система організації захищеного віддаленого доступу користувачів до ресурсів корпоративної мережі надає можливість створення захищених Інтернет-каналів, реалізованих на базі технології побудови віртуальних приватних мереж, що забезпечує високий рівень безпеки корпоративного трафіку при невеликих фінансових витратах.

Системи виявлення вторгнень і системи аналізу захищеності ресурсів корпоративної мережі, що працюють у єдиному комплексі, забезпечують запобігання хакерських атак, дозволяють попереджати зовнішні й внутрішні хакерські атаки, контролюють минаючий трафік і процеси на ключових серверах мережі, дають можливість в автоматичному режимі блокувати атаки, виявляти й усувати уразливості в системі захисту корпоративної мережі.

Засоби керування політикою безпеки й захисти від несанкціонованого доступу реалізують комплексні рішення для організації доступу користувачів і адміністраторів до ресурсів корпоративної мережі, передбачають використання електронних ключів з унікальними персональними ідентифікаторами користувачів, електронних замків і інших засобів захисту серверів, робочих станцій і телекомунікаційного встаткування від несанкціонованого доступу.

Багато користувачів уважають, що для забезпечення надійного захисту цілком достатньо антивірусного програмного забезпечення, інші думають, що краще рішення – повне шифрування даних. Однак використання антивірусного ПЗ при його правильному настроюванні й експлуатації означає всього лише те, що віруси із загальновідомих списків з великою часткою ймовірності не потраплять в інформаційний захищаємий ресурс. Крім того, існує велика кількість програм, типу троянців і т.п., які не виявляються антивірусним програмним забезпеченням і можуть функціонувати на зараженому комп'ютері роками. Повне шифрування даних саме по собі теж не є панацеєю, тому що шифруєма стійкими алгоритмами важлива інформація може бути легко передана зловмисникові так званими клавіатурними шпигунами. У той же час варто враховувати, що система шифрування є одним із ключових (хоча й не єдиним!) елементів єдиної комплексної підсистеми інформаційної безпеки корпоративної мережі компанії.

Адміністраторові підсистеми безпеки варто мати на увазі те, що конфіденційна інформація компанії може бути послана співробітником компанії по електронній пошті. Для виявлення подібних фактів підсистема безпеки повинна включати засобу контролю вмісту поштових повідомлень.

А тепер більш детально розглянемо системи керування політикою безпеки й захисти від несанкціонованого доступу, засобу виявлення й запобігання вторгнень, а також інструменти аналізу захищеності ресурсів корпоративної мережі.

Система керування політикою безпеки й захисти від несанкціонованого доступу

Насамперед слід зазначити, що дана система не виконує функцій захисту від таких зловмисних дій, як використання побічних електромагнітних випромінювань і наведень, підслуховування, підглядання й т.п., – для протидії подібного роду порушенням повинен бути реалізований комплекс організаційно-технічних заходів щодо фізичного контролю (розміщення, охорона й т.п.) контрольованих вузлів корпоративної мережі. Основним же завданням системи керування політикою безпеки й захисти від несанкціонованого доступу є виявлення фактів несанкціонованих дій користувачів корпоративної мережі на основі збору й аналізу інформації про події, реєструємих на інформаційних ресурсах корпоративної мережі.

Дана система забезпечує моніторинг, контроль і збір інформації про дії легальних користувачів корпоративної мережі. Якщо за результатами аналізу зібраних даних виявляється факт несанкціонованих дій, система блокує подальші дії порушника й сповіщає адміністратора безпеки про дії користувача. Крім того, система контролює роботу застосунків, запущених на робочих станціях користувачів. Інформація про випадок порушенні політики безпеки записується в базу дані системи й може використовуватися для подальшого аналізу.

У завдання цієї системи входить збір інформації про наступні події:

– зміна файлової системи контрольованого вузла корпоративної мережі;

– використання зовнішніх пристроїв вводу-виводу (дисководів, USB-пристроїв і т.п.);

– запуск і зупинка процесів на контрольованому вузлі;

– локальна або віддалена реєстрація початку сеансу роботи користувача, а також завершення роботи користувачів;

– використання принтерів і інших периферійних пристроїв;

– ведення статистики використання мережних сервісів;

– зміна апаратної й програмної конфігурації контрольованого вузла.

Система керування політикою безпеки й захисти від несанкціонованого доступу має розподілену архітектуру й включає такі компоненти, як програмні сенсори, сервер керування сенсорами й консоль адміністратора. Програмні сенсори встановлюються на контрольовані вузли корпоративної мережі й забезпечують збір, фільтрацію й передачу параметрів зібраних подій серверу керування сенсорами. Сервер керування сенсорами здійснює зберігання й аналіз інформації про події, що надходять від сенсорів системи. Консоль адміністратора служить для централізованого керування сервером керування сенсорами й сенсорами системи, відображення результатів роботи системи й формування звітів.

Використання таких засобів захисту, як міжмережеві екрани, системи контролю доступу користувачів і т.п., не дає повної гарантії стійкості корпоративної мережі до атак. Будь-яке програмне або апаратне забезпечення не є зробленим, і в ньому є уразливості, що дозволяють зробити які-небудь дії в порушення встановленого порядку використання інформаційних ресурсів. Крім того, реагувати на несанкціоновану активність або спроби злому мережі в режимі реального часу практично неможливо, якщо ці функції виконуються вручну. Своєчасне виявлення спроб злому інформаційних ресурсів і оперативна реакція на ці дії дозволяють значно підвищити рівень захищеності мережі.

Система виявлення й запобігання вторгнень

Дана система дозволяє виявляти атаки й зловживання відносно вузлів корпоративної мережі компанії. Система може забезпечувати як захист конкретного вузла, так і цілого мережного сегмента. Основний принцип роботи системи виявлення й запобігання вторгнень полягає у виявленні й блокуванні мережних атак у корпоративній мережі на основі аналізу пакетів даних, що циркулюють у цій мережі, і в наступному виявленні аномалій мережного трафіку мережі. Система дозволяє з рівним ступенем ефективності виявляти й блокувати атаки з боку як зовнішніх, так і внутрішніх порушників.

Для виявлення вторгнень система використовує метод, заснований на виявленні сигнатур відомих атак, а також метод, що базується на аналізі поводження мережі. Метод, заснований на виявленні сигнатур, забезпечує виявлення атак за допомогою спеціальних шаблонів. Як сигнатура атаки можуть виступати рядок символів, семантичне вираження спеціальною мовою, формальна математична модель і ін., причому кожна сигнатура може бути співвіднесена з відповідною атакою порушника. При одержанні вихідних даних про мережний трафік корпоративної мережі система проводить їхній аналіз на відповідність певним шаблонам або сигнатурам атак, збереженим у постійно, що обновляється базі, даних системи. У випадку виявлення сигнатури у вихідних даних система фіксує факт виявлення мережної атаки й блокує її подальші дії. Перевагою сигнатурного методу є його висока точність.

Для виявлення нових типів атак у системі виявлення вторгнень реалізований метод, що заснований на аналізі поводження корпоративної мережі й використовує інформацію про штатний процес функціонування корпоративної мережі. Принцип роботи цього методу полягає у виявленні невідповідності між поточним режимом функціонування корпоративної мережі й моделлю штатного режиму роботи, закладеної в параметрах роботи методу. Будь-яка невідповідність розглядається як інформаційна атака. У випадку здійснення атаки, що може привести до виведення з ладу вузлів корпоративної мережі, можливе автоматичне завершення з'єднання з атакуючим вузлом, блокування облікового запису порушника (якщо

він є співробітником компанії) або реконфігурація міжмережевих екранів і маршрутизаторів таким чином, щоб надалі з'єднання з атакуючим вузлом були заборонені.

До складу системи виявлення й запобігання вторгнень входять наступні компоненти: мережні сенсори, серверні сенсори, датчики, сервер керування сенсорами, а також консоль адміністратора. Мережні сенсори, призначені для захисту об'єктів мережних сегментів корпоративної мережі, забезпечують перехоплення й аналіз усього мережного трафіку, переданого в рамках того сегмента, де вони встановлені. Серверні сенсори встановлюються на сервери корпоративної мережі й забезпечують захист певних мережних сервісів мережі. У числі таких сенсорів можуть бути серверні сенсори для поштових, файлових і Web-серверів, а також для серверів баз даних. На одному сервері корпоративної мережі може бути одночасно встановлено кілька типів сенсорів. Датчики виконують функції керування серверними й мережними сенсорами, а також функції забезпечення передачі інформації між сенсорами й сервером керування сенсорами. Сервер керування сенсорами забезпечує централізований збір, зберігання й аналіз інформації, що надходить від серверних і мережних сенсорів, і дає можливість виявлення розподілених мережних атак на основі аналізу отриманої інформації. Консоль адміністратора призначена для централізованого керування компонентами системи й відображення результатів роботи системи.

Повідомлення про виявлену атаку, як правило, формується у відповідності зі стандартом IDMEF (Intrusion Detection Message Exchange Format) і містить наступну інформацію:

- дата й час виявлення атаки;
- загальний опис атаки, включаючи можливі посилання на додаткові джерела інформації про виявлену атаку;
- символьний ідентифікатор атаки по класифікаторі CVE (Common Vulnerabilities Exposures, http://cve.mitre.org) або CERT (Computer Emergency Response Team, http://www.cert.org);
- рівень пріоритету виявленої атаки (низький, середній або високий);
- інформація про джерело атаки (IP-адреса, номер порту, доменне ім'я й ін.);
- інформація про об'єкт атаки (IP-адреса, номер порту, доменне ім'я й ін.);
- рекомендації з усунення уразливості, у результаті якої був зафіксований факт реалізації атаки.

База даних сигнатур атак системи виявлення й запобігання вторгнень повинна регулярно обновлятися.

Система аналізу захищеності корпоративної мережі

Система аналізу захищеності призначена для проведення регулярних, всебічних або вибіркових тестів з метою виявлення й усунення уразливостей програмно-апаратного забезпечення корпоративної мережі: мережних сервісів, операційних систем, прикладного програмного забезпечення, систем керування базами даних, маршрутизаторів, міжмережевих екранів, а також для перевірки наявності останніх модулів відновлення й т.п. При виявленні уразливостей система надає адміністраторові звіти, що містять докладний опис кожної виявленої уразливості, дані про їхнє розташування у вузлах корпоративної мережі й рекомендації з їхньої корекції або усунення.

До складу системи аналізу захищеності входять сканери безпеки, призначені для проведення заданої безлічі перевірок відповідно до параметрів, певними адміністратором безпеки; сервер зберігання результатів роботи системи; консоль адміністратора для централізованого керування системою.

Сканер безпеки являє собою програмний засіб для віддаленої або локальної діагностики різних елементів мережі на предмет виявлення в них уразливостей, використання яких може привести до комп'ютерних порушень. Основними користувачами таких сканерів є системні адміністратори й фахівці з безпеки. Сканери безпеки скорочують час, необхідне для пошуку уразливостей, за рахунок автоматизації операцій по оцінці

захищеності систем. Принципи роботи такого сканера полягає в тім, що основний модуль програми приєднується по мережі до віддаленого комп'ютера. Залежно від активних сервісів формуються перевірки й тести. Знайдена при скануванні кожного порту службова інформація рівняється з таблицею правил визначення мережних пристроїв, операційних систем і можливих уразливостей. На основі проведеного порівняння робиться вивід про наявність або відсутність потенційної уразливості.

Система аналізу захищеності вимагає постійної уваги й контролю. Будь-яка зміна конфігурації корпоративної мережі компанії, а також мережного програмного забезпечення повинне бути досліджене системою аналізу захищеності. Невідповідність у конфігурації може привести до збільшення кількості помилкових спрацьовувань, а також до появи дір у безпеці. Робота системи заснована на аналізі мережного трафіку з використанням методу сигнатур, тому система аналізу захищеності вимагає постійного відновлення бази уразливостей. Експлуатація даної системи має сенс тільки за умови, що вона розвивається разом з мережею, що вона захищає. Зрозуміло, що мається на увазі регулярне проведення тестів.

У цей час багато компаній, що займаються питаннями інформаційної безпеки (наприклад, Internet Security Systems і ін.), пропонують стратегію застосування описаних вище систем у складі єдиних комплексів, що дозволяють здійснювати централізоване керування інформаційною безпекою корпоративної мережі. За допомогою єдиного керування всіма компонентами підсистеми інформаційної безпеки корпоративної мережі, а також на основі збору й аналізу інформації від різних компонентів у режимі реального часу можна значно підвищити ефективність роботи адміністраторів безпеки, скоротити число співробітників відповідних служб і зменшити витрати на їхнє навчання.

Подібні системи дозволяють вести єдину базу даних шаблонів, варіантів реагування й відновлень для всіх компонентів підсистеми безпеки, автоматизувати рутинні завдання адміністраторів безпеки (відновлення сигнатур атак, сканування віддалених вузлів і т.д.), а також проводити всебічний аналіз різних подій шляхом кореляції даних від різноманітних засобів захисту.

У січні цього року, у зв'язку з наявністю широкого спектра антишпигунських програмних комплексів, компанії McAfee, Symantec, Trend Micro, ICSA Labs і Thompson Cyber Security Labs оголосили про реалізацію угоди по створенню методологій ідентифікації й тестування для технологій, що забезпечують протидію шпигунським програмам. Тестування продуктів буде засновано на стандартизованих, незалежних критеріях оцінки, а в середовищі виявлення й тестування будуть використовуватися загальні стандартні зразки. На думку учасників проекту, за рахунок використання стандартних метрик для оцінки третьою стороною, а також наявності загального стандарту для зразків можна буде порівнювати між собою характеристики продуктів, які колись із працею піддавалися виміру.

У сучасному світі неможливо повністю виключити погрозу, пов'язану з комп'ютерною безпекою, оскільки завжди найдуться люди, здатні знайти уразливі місця в системі й скористатися цим. Однак саме слабке місце – це люди. Змусьте їх зрозуміти, що безпека – це динамічний процес, це постійно розвивається, живуча за своїми законами система.

Розробка структурної схеми

Через практично повсюдну доступність широкополосного інтернету, більшість дій на пристроях виробляються через мережу, тому для 99% сучасних погроз саме мережа є транспортом, на якому доставляється погроза від джерела до мети. Звичайно, поширення шкідливого коду можливо за допомогою знімних носіїв, але даний спосіб у цей час використовується усе рідше й рідше, та й більшість компаній давно навчилися боротися з подібними погрозами.

Давайте спочатку намалюємо архітектуру класичної корпоративної мережі передачі даних у спрощеному й всьому зрозумілому виді.

Починається мережа передачі даних з комутатора рівня доступу. Безпосередньо до даного комутатора підключаються робочі місця: комп'ютери, ноутбуки, принтери,

багатофункціональні й різний рід інші пристрої, наприклад, бездротові крапки доступу. Відповідно встаткування у вас може бути багато, підключатися до мережі воно може в зовсім різних місцях (поверхах або навіть окремих будинках).

Звичайно, корпоративна мережа передачі даних будується по топології «зірка», тому взаємодія всіх сегментів між собою буде забезпечувати встаткування рівня ядра мережі. Наприклад, може використовуватися той же комутатор, тільки звичайно в більше продуктивному й функціональному варіанті в порівнянні з використовуваними на рівні доступу.

Сервери й системи зберігання даних звичайно консолідовані в одному місці й, з погляду мереж передачі даних, можуть підключатися як безпосередньо до встаткування ядра, так і можуть мати якийсь виділений для цих цілей сегмент устаткування доступу.

Далі в нас залишається встаткування для стику із зовнішніми мережами передачі даних (наприклад, Інтернет). Звичайно для цих цілей у компаніях використовуються такі пристрої, маршрутизатори, міжмережеві екрани, різного роду проксі-сервери. Вони ж використовуються для організації зв'язку з розподіленими офісами компанії й для підключення віддалених співробітників.

От така вийшла проста для розуміння й звичайна для сучасних реалій архітектура локально-обчислювальної мережі.

Давайте визначимо основні цілі й напрямки атак у рамках мережної взаємодії.

Найпоширеніша й проста мета атаки – це користувальницький пристрій. Шкідливе програмне забезпечення легко поширити в даному напрямку через контент на веб-ресурсах або через пошту.

Надалі зловмисник, одержавши доступ до робочої станції користувача, або може викрасти конфіденційні дані, або розвивати атаку на інших користувачів або на інші пристрої корпоративної мережі.

Наступна можлива мета атаки – це, звичайно ж, сервери. Одними з найвідоміших типів атак на опубліковані ресурси є DoS і DDoS атаки, які застосовуються з метою порушення стабільної роботи ресурсів або повної їхньої відмови.

Також атаки можуть бути спрямовані із зовнішніх мереж на конкретні опубліковані додатки, наприклад, веб-ресурси, DNS-сервери, електронну пошту. Також атаки можуть бути спрямовані зсередини мережі – із зараженого комп'ютера користувача або від зловмисника, що підключився до мережі, на такі додатки, як файлові кулі або бази даних.

Так само є категорія вибірних атак, і однієї із самих небезпечних є атака на саму мережу, тобто на доступ до неї. Зловмисник, що одержав доступ до мережі, може організувати наступну атаку фактично на будь-який пристрій, підключений до неї, а також потай одержувати доступ до будь-якої інформації. Що саме головне – успішну атаку подібного роду досить складно виявити, і вона не лікується стандартними засобами. Тобто фактично у вас з'являється новий користувач або, гірше того, адміністратор, про який ви нічого не знаєте.

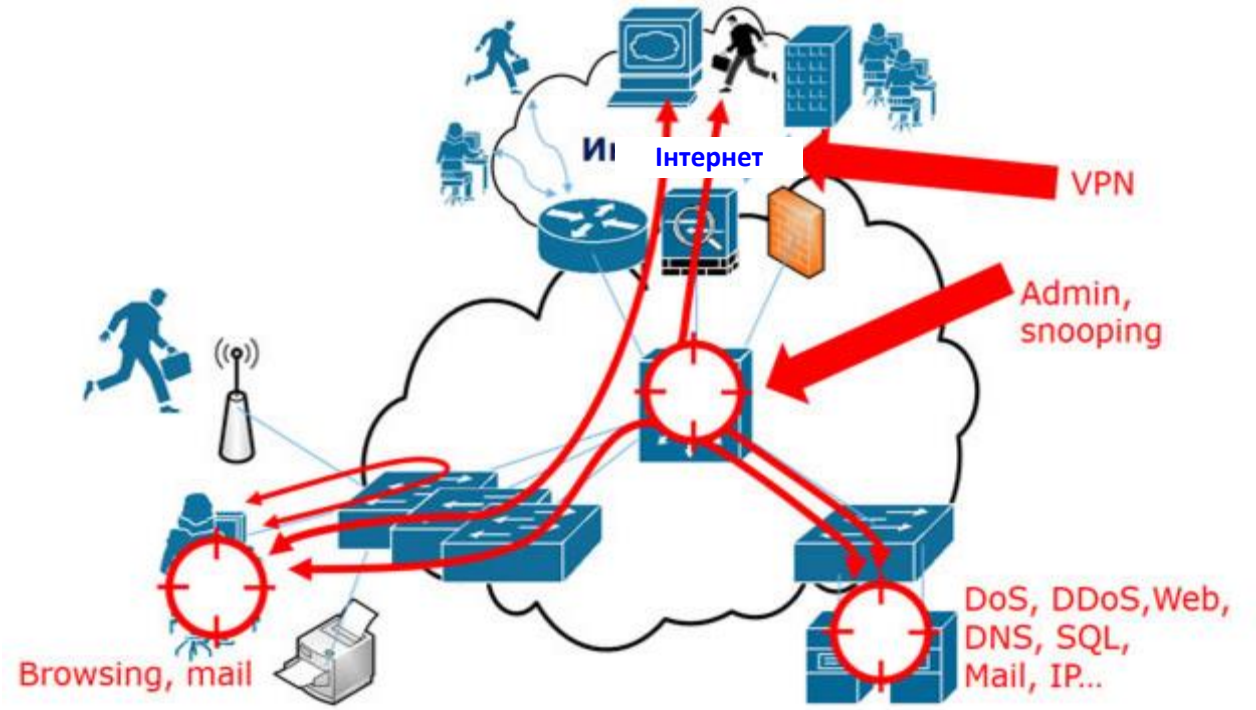


Рисунок 1 – Структурна схема системи

Ще метою атакуючих можуть бути канали зв'язку. Варто розуміти, що успішна атака на канали зв'язку не тільки дозволяє зчитувати передану по них інформацію, але й бути ідентичної по наслідках атаці на мережу, коли зловмисник може одержати доступ до всіх ресурсів локально обчислювальної мережі.

Для початку ми можемо представити загальносвітові практики й рекомендації з організації захисту корпоративної мережі передачі даних, а саме той набір засобів, що дозволить мінімальними зусиллями уникнути більшості існуючих погроз, так званий безпечний мінімум.

У даному контексті необхідно ввести термін «периметр безпеки мережі», тому що чим ближче до можливого джерела погрози ви будете здійснювати контроль, тим сильніше ви знижуєте кількість доступних для зловмисника способів атаки. При цьому периметр повинен існувати як для зовнішніх, так і для внутрішніх підключень.

У першу чергу, ми рекомендуємо убезпечити стик з публічними мережами, адже найбільша кількість погроз виникає від них. У цей час існує ряд спеціалізованих засобів мережної безпеки, призначених саме для безпечної організації підключення до мережі Інтернет.

Для їхнього позначення широко використовуються такі терміни як NGFW (Next-generation firewall) і UTM (Unified Threat Management). Ці пристрої не просто сполучать у собі функціонал класичного маршрутизатора, файрволла й проксі-сервера, але й надають додаткові сервіси безпеки, такі як: фільтрація по URL і контенту, антивірус і ін. При цьому пристрою найчастіше використовують хмарні системи перевірки контенту, що дозволяє швидко й ефективно перевіряти всі передані дані на наявність погроз. Але головне – це можливість повідомляти про виявлені погрози в ретроспективі, тобто виявляти погрози в таких випадках, коли заражений контент був уже переданий користувачеві, але інформація про шкідливість даного програмного забезпечення з'явилася у виробника пізніше.

Такі речі, як інспекція HTTPS трафіку й автоматичний аналіз застосунків, дозволяють контролювати не тільки доступ до конкретних сайтів, але й дозволяти/забороняти роботу таких застосунків як: Skype, Team Viewer і багатьох інших, а як ви знаєте, більшість із них давно працюють по протоколах HTTP і HTTPS, і стандартними мережними засобами їхню роботу просто так не проконтролювати.

На додаток до цього, у рамках єдиного пристрою ви можете одержати ще й систему запобігання вторгнень, що відповідає за припинення атак, спрямованих на опубліковані ресурси. Також ви додатково можете одержати VPN-сервер для безпечної віддаленої роботи співробітників і підключення філій, антиспам, систему контролю ботнетів, пісочницю й ін. Все це робить такий пристрій дійсно уніфікованим засобом мережної безпеки.

Якщо ваша компанія ще не використовує такі рішення, то ми дуже рекомендуємо почати ними користуватися прямо зараз, оскільки час їхньої ефективності вже наступило, і ми можемо із упевненістю сказати, що подібні пристрої довели свою реальну здатність боротися з більшою кількістю погроз, чого не було ще 5 років тому. Тоді подібні речі тільки вийшли на ринок, мали безліч проблем і були досить дорогими й низькоподуктивними.

Next-generation firewall

Зараз на ринку величезна кількість мережних пристроїв із заявленим подібним функціоналом, але дійсно ефективний захист здатні забезпечити лише одиниці. Це пояснюється тим, що лише обмежене число виробників мають засобу й дійсно вкладають їх в nonstop прооблення актуальних погроз, тобто постійно обновляють бази потенційно небезпечних ресурсів, забезпечують безперебійну підтримку рішень і т.д.

Багато партнерів будуть намагатися вам продати рішення, які вигідні їм для продажу, тому ціна рішення аж ніяк не завжди відповідає його реальній здатності протистояти погрозам. Особисто я рекомендую для вибору пристрою звернутися до матеріалів незалежних аналітичних центрів, наприклад, звітів NSS Labs. На мою думку, вони є більше точними й неупередженими.

Крім погроз із зовнішньої сторони, ваші ресурси можуть бути атаковані й зсередини. Так званий «безпечний мінімум», якому варто використовувати у вашій локально-обчислювальній мережі – це її сегментація на VLANи, тобто віртуальні приватні мережі. Крім сегментації, потрібне обов'язкове застосування політик доступу між ними хоча б стандартними засобами аркушів доступу (ACL), адже проста наявність VLAN у рамках боротьби із сучасними погрозами практично нічого не дає.

Окремою рекомендацією я позначу бажаність використання контролю доступу безпосередньо від порту пристрою. Однак при цьому необхідно пам'ятати про периметр мережі, тобто чим ближче до сервісів, яки захищаються, ви застосуєте політики – тим краще. В ідеалі такі політики варто вводити на комутаторах доступу. У таких випадках у якості самих мінімальних політик безпеки рекомендується застосовувати 4 прості правила:

- тримати всі незадіяні порти комутаторів адміністративно виключеними;
- не застосовувати 1й VLAN;
- використовувати аркуші фільтрації по MAC на комутаторах доступу;
- використовувати інспекцію ARP протоколу.

Відмінним рішенням буде застосовувати на шляху проходження передачі даних ті ж самі міжмережеві екрани із системами запобігання вторгнень, а також архітектурно використовувати демілітаризовані зони. Найкраще впровадити автентифікацію пристрою, що підключається, по 802. 1x протоколу, використовуючи для централізованого керування доступом до мережі різні AAA системи (системи автентифікації, авторизації й аккаунтингу). Звичайно ці рішення позначаються загальним серед виробників терміном NAC (Network Access Control). Приклад однієї з подібних комерційних систем – Cisco ISE.

Також зловмисниками можуть бути зроблені атаки на канали. Для захисту каналів варто використовувати сильне шифрування. Багато хто зневажають цим, а потім розплачуються за наслідки. Незахищені канали – це не тільки доступна для викрадень інформація, але й можливість атаки практично всіх корпоративних ресурсів. У наших замовників у практиці була чимала кількість прецедентів, коли відбувалися атаки на корпоративну телефонію шляхом організації зв'язку через незахищені канали передачі даних між центральним і віддаленим офісом (наприклад, просто використовуючи GRE тунелі). Компаніям приходили просто божевільні рахунки!

Бездротові мережі й BYOD

Тему віддаленої роботи, бездротових мереж і використання власних пристроїв я хотів би виділити окремо. По своєму досвіді можу сказати, що ці три речі – одна із самих більших потенційних дір у безпеці вашої компанії. Але при цьому вони є й одним із самих більших конкурентних переваг.

Якщо підійти до питання коротко, то я рекомендую або повністю забороняти використання бездротових мереж, віддалену роботу або роботу через власні мобільні пристрої, мотивуючи це корпоративними правилами, або надавати ці сервіси максимально проробленими з погляду безпеки, тим більше, що сучасні рішення надають можливість зробити це якнайкраще.

У плані віддаленої роботи вам можуть допомогти того ж самі Next Generation Firewalls або UTM пристрою. Наша практика показує, що є ряд стабільних рішень (туди входять Cisco, Checkpoint, Fortinet, Citrix), які дозволяють працювати з безліччю клієнтських пристроїв, при цьому забезпечуючи найвищі стандарти для ідентифікації віддаленого співробітника. Наприклад, використання сертифікатів, двофакторної авторизації, одноразових паролів, що доставляються по SMS або генеруємих на спеціальному ключі. Так само можна контролювати програмне забезпечення, установлене на комп'ютері, з якого виробляється спроба доступу, допустимо, на предмет установки відповідних відновлень або запущених антивірусів.

Якщо ви будуєте корпоративний Wi-Fi, то обов'язково проробляйте всі можливі аспекти безпеки, пов'язані з ним. Між іншим, Wi-Fi – це ціла окрема стаття доходів нашої компанії. Ми займаємося ними професійно: проекти по оснащенню бездротовим устаткуванням ТРК і ТЦ, бізнес-центрів, складів, у тому числі із застосуванням сучасних рішень, таких як позиціонування, виконуються в нас у режимі nonstop. І за результатами проведених нами радіо-обстежень ми в кожному другому офісі й складі знаходимо як мінімум по одному домашньому Wi-Fi роутеру, які підключали до мережі самі співробітники. Звичайно вони це роблять для власної зручності роботи, допустимо, у курилку з ноутбуком вийти або вільно переміщатися в межах кімнати. Зрозуміло, що ніяких корпоративних правил безпеки на таких маршрутизаторах не застосовувалося й паролі лунали добре знайомим колегам, потім колегам колег, що потім зашли на кава гостям і в підсумку доступ до корпоративної мережі мали практично всі, при цьому він був абсолютно неконтрольованим.

Звичайно, варто убезпечити мережа від підключення подібного встаткування. Основними способами це зробити можуть бути: використання авторизації на портах, фільтрація по MAC та ін. Знову ж, з погляду Wi-Fi, для мережі варто використовувати сильні криптографічні алгоритми й enterprise методи автентифікації. Але варто розуміти, що не всі enterprise методи автентифікації є однаково корисними. Наприклад, Android пристрою в деяких релізах програмного забезпечення можуть за замовчуванням ігнорувати публічний сертифікат Wi-Fi мережі, тим самим уможливлюючи атаки класу Evil twin. Якщо ж використовується метод автентифікації, такий як EAP GTC, то ключ у ньому передається у відкритому виді і його можна в зазначеній атаці цілком перехопити. Ми рекомендуємо в корпоративних мережах використовувати винятково автентифікацію за сертифікатом, тобто це TLS методи, але враховуйте, що вона значно збільшує навантаження на адміністраторів мережі.

Є ще спосіб: якщо в корпоративній мережі впроваджена віддалена робота, те можна підключені через Wi-Fi мережа пристрою змушувати використовувати ще й VPN клієнт. Тобто виділити Wi-Fi сегмент мережі в споконвічно недовірену область, і в підсумку вийде гарний робочий варіант із мінімізацією витрат на керування мережею.

Виробники enterprise рішень по Wi-Fi, такі як Cisco, Ruckus, що тепер Brocade, Aruba, що тепер HPE, крім стандартних рішень по організації Wi-Fi, надають цілий набір сервісів по автоматичному контролі безпеки бездротового середовища. Тобто в них цілком собі працюють такі речі як WIPS (Wireless intrusion prevention system). У даних виробників

реалізовані бездротові сенсори, які можуть контролювати весь спектр частот, тим самим дозволяючи відслідковувати в автоматичному режимі таки серйозні погрози.

Тепер торкнемося таких тем, як BYOD (Bring your own device – Принеси свій пристрій) і MDM (Mobile device management – Керування мобільними пристроями). Звичайно, будь-який мобільний пристрій, на якому зберігаються корпоративні дані, або яке має доступ до корпоративної мережі, є потенційним джерелом проблем. Тема безпеки для таких пристроїв стосується не тільки безпечного доступу до корпоративної мережі, але й централізованого керування політиками мобільних пристроїв: смартфонів, планшетів, ноутбуків, використовуваних поза організацією. Ця тема актуальна вже дуже давно, але тільки зараз на ринку з'явилися реально працюючі рішення, що дозволяють управляти різноманітним парком мобільної техніки.

На жаль, розповісти про їх у рамках даної роботи не вийде, але знайте, що рішення є й в останній рік ми випробовуємо бум впроваджень рішень MDM від Microsoft і MobileIron.

Перша рекомендація з нашої сторони для «безпеки в максимумі» – це ешелонування засобів інформаційної безпеки. Що це означає?

Один час в інтернеті була популярна картинка: на ній рекомендувалося для захисту мережі поставити один за одним міжмережеві екрани відомих виробників. Ми ні в якій мері не призиваємо робити вас так само, але, проте, частка істини тут є. Буде вкрай корисним мати мережний пристрій з аналізом вірусних сигнатур, а на робочих місцях уже встановлювати антивірус. Тим самим, ми одержуємо дві не заважають один одному системи захисту від шкідливого коду.

Існує ряд спеціалізованих засобів ІБ:

DLP

На ринку представлені спеціалізовані засоби інформаційної безпеки, тобто розроблені й спрямовані на рішення якоїсь конкретної погрози. У цей час популярними стають системи DLP (Data Loss Prevention) або запобігання витоку даних. Вони працюють як на мережному рівні, інтегруючись у середовище передачі даних, так і безпосередньо на серверах застосунків, робочих станціях, мобільних пристроях.

Ми трохи йдемо від мережної тематики, але погроза витоку даних буде існувати завжди. Особливо, дані рішення стають актуальними для компаній, де втрата даних несе комерційні й репутаційних ризики й наслідки. Ще 5 років тому впровадження DLP систем було трохи утруднене у виді їхньої комплексності й необхідності проведення процесу розробки для кожного конкретного випадку. Тому через їхню вартість багато компаній відмовлялися від даних рішень, або писали свої. У цей час ринкові системи досить напрацьовані, тому весь необхідний функціонал безпеки можна одержати прямо з «коробки».

На українському ринку комерційні системи в основному представлені виробником Infowatch і таки відомим MacAfee.

WAF

Через розвиток послуг інтернет комерції, а це інтернет-банкінг, електронні гроші, електронна торгівля, страхові послуги й т.д., останнім часом стали затребувані спеціалізовані засоби для захисту веб-ресурсів. А саме WAF – Web Application Firewall.

Даний пристрій дозволяє відбивати атаки, спрямовані на уразливості самого сайту. Крім вибірних DoS атак, коли сайт придушується легітимними запитами, це можуть бути атаки SQL injection, Cross site scripting та ін. Раніше такі пристрої здобувалися в основному банками, а в інших замовників вони були не затребувані, та й коштували дуже більших грошей. Для приклада – вартість робочого рішення починалася від 100 000$. Зараз на ринку представлена велика кількість рішень від відомих виробників (Fortinet, Citrix, Positive Technologies), від яких можна одержати працююче рішення по захисту вашого сайту за цілком собі осудні гроші (в 3-5 разів менше, ніж зазначена раніше сума).

Audit

Організації, що особливо ратують за власну безпеку, впроваджують засобу автоматизованого аудита. Дані рішення дорогі, але дозволяють винести ряд функцій адміністратора в область автоматизації, що вкрай затребувано для великого бізнесу. Такі рішення постійно здійснюють сканування мережі й виконують аудит всіх установлених операційних систем і застосунків на предмет наявності відомих дір у безпеці, своєчасності відновлень, відповідності корпоративних політик. Напевно, найвідоміші рішення в цій області не тільки в України, але й усьому світі – це продукти від Positive Technologies.

SIEM

Аналогічно SIEM рішення. Це системи, заточені на виявлення позаштатних ситуацій, що стосуються саме подій, пов'язаних з безпекою. Навіть стандартний набір з пари міжмережевих екранів, десятка серверів застосунків і тисячі робочих місць може генерувати десятки тисяч оповіщень у день. Якщо у вас більша компанія й ви маєте десятки прикордонних пристроїв, то розібратися в одержувані від них даних у ручному режимі стає просто неможливо. Автоматизація контролю логів, що збираються, одночасно із всіх пристроїв дозволяє адміністраторам і співробітникам ІБ діяти негайно. На ринку таки відомі рішення SIEM від Arcsight (входить у продукцію HPE) і Q-RADAR (входить у продукцію IBM).

Безумовно, при організації IT-безпеки підприємства не варто забувати й про адміністративний регламент. Користувачі й адміністратори повинні бути в курсі, що знайдені флешки використовувати на комп'ютері не можна, як не можна переходити по сумнівних посиланнях у листах або відкривати сумнівні вкладення. Дуже важливо при цей розповісти й пояснити, які посилання й вкладення є неперевіреними. У дійсності, не всі розуміють, що не треба зберігати паролі на стікерах, приклеєних до монітора або телефону, що потрібно навчитися читати попередження, які пишуть користувачеві додатка й т.д. Варто пояснити користувачам, що таке сертифікат безпеки й що означають повідомлення, пов'язані з ним. У цілому, необхідно враховувати не тільки технічну сторону питання, але й прищеплювати культуру використання корпоративних IT-ресурсів співробітниками.

Висновок. У статті розглянуто та проаналізовано програмне забезпечення, яке призначено для операційної системи протидії загрозам корпоративній мережі. В межах України в недостатній мірі представлені вітчизняні розробки в цій області. У роботі наведені теоретичне узагальнення й рішення наукового завдання дослідження методів протидії загрозам корпоративній мережі. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем протидії загрозам корпоративній мережі; Досліджена система протидії загрозам корпоративній мережі; На основі отриманих результатів досліджень створена програмна реалізація системи протидії загрозам корпоративній мережі. Розроблені під час виконання роботи алгоритми дозволяють успішно вирішувати завдання протидії загрозам корпоративній мережі. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки. Розроблене програмне забезпечення має простий, дружній та зручний інтерфейс користувача, що забезпечує легкість у освоєнні роботи програмного продукту, зручність у використанні, і не потребує особливих спеціальних знань. При створені програмного забезпечення було використано об’єктно-орієнтований підхід, що відповідає сучасним тенденціям у галузі розробки комерційних програмних систем. Програма реалізована на мові високого рівня Delphi XE8. Дана мова програмування дозволяє найбільш ефективно обробляти дані. Це дозволило мінімізувати строк розробки програмного забезпечення, і, як слід, зменшити витрати на його розробку. Запропоноване програмне забезпечення ділиться на загальне програмне забезпечення, що поставляється із засобами обчислювальної техніки й спеціальне програмне забезпечення, що спеціально розроблене для даної конкретної системи й включає програми, що реалізують її функції. Даються необхідні рекомендації з установки розробленого програмного забезпечення. Для

підвищення рівня безпеки запропоновано застосовувати алгоритм Blowfish.

Список літератури

1. Смирнов А.А. Анализ и сравнительное исследование перспективных направлений развития цифровых телекоммуникационных систем и сетей / А.А.Смирнов, В.В.Босько, Е.В.Мелешко // Системи обробки інформації. – Х.: ХУ ПС, 2008. – Вип.7(74). – С.120-123.
2. Смирнов А.А. Усовершенствование метода управления очередями в многопротокольных узлах телекоммуникационной сети / А.А.Смирнов, Е.В.Мелешко // Збірник тез та доповідей другої всеукраїнської науково-практичної конференції «Системний аналіз. Інформатика. Управління». Запоріжжя. Тези доповідей. Запоріжжя: КПУ, 2011.
3. Смирнов С.А. метод безопасной маршрутизации метаданных в облачные антивирусные системы / А.К. Дидык, С.А. Смирнов // Информационные технологии в управлении, образовании, науке и промышленности: монография / Под редакцией профессора В.С. Пономаренко. – Х.: Видавець Рожко С.Г., 2016. – 566 с.
4. Смирнов С. А. Сравнительные исследования математических моделей технологии распространения компьютерных вирусов в информационно-телекоммуникационных сетях / Мохамад Абу Таам Гани, А. А. Смирнов, А. В. Коваленко, С. А. Смирнов // Системи обробки інформації: зб. наук. праць. – Х.: ХУПС, 2014. – Вип. 9(125). – 105-110.
5. Смирнов С. А. Математическая модель интеллектуального узла коммутации с обслуживанием информационных пакетов различного приоритета / Мохамад Абу Таам Гани, А. А. Смирнов, Н. С. Якименко, С. А. Смирнов // Збірник наукових праць Харківського університету Повітряних Сил. – Харків: ХУПС, 2014. – Вип. 4 (41). – С. 48-52.
6. Смирнов С. А. Исследование показателей качества функционирования интеллектуальных узлов коммутации в телекоммуникационных системах и сетях / Мохамад Абу Таам Гани, А. А. Смирнов, Н. С. Якименко, С. А. Смирнов // Наука і техніка Повітряних Сил Збройних Сил України: наук. журн. – Х.: ХУПС, 2014. – № 4(17). – С. 90-95.
7. Смирнов С. А. Усовершенствованный алгоритм управления доступом к «облачным» телекоммуникационным ресурсам / Мохамад Абу Таам Гани, А. А. Смирнов, Н. С. Якименко, С. А. Смирнов // Системи обробки інформації: зб. наук. праць. – Х.: ХУПС, 2015. –Вип. 1(126). – С. 150-153.
8. Smirnov S.A. Method of controlling access to intellectual switching nodes of telecommunication networks and systems / A.A. Smirnov, Mohamad Abou Taam, S.A. Smirnov // International Journal of Computational Engineering Research (IJCER). – **Volume 5, Issue 5. –** India. Delhi. – 2015. – P. 1-7.
9. Смирнов С. А. Анализ и исследование методов управления сетевыми ресурсами для обеспечения антивирусной защиты даннях / Мохамад Абу Таам Гани, А. А. Смирнов, С. А. Смирнов // Системи озброєння і військова техніка: наук. журн. – Х.: ХУПС, 2015. – № 3(43). – С. 100-107.
10. Смирнов С. А. Исследование эффективности метода управления доступом к облачным антивирусным телекоммуникационным ресурсам / Мохамад Абу Таам Гани, А. А. Смирнов, С. А. Смирнов // Наука і техніка Повітряних Сил Збройних Сил України: наук. журн. –Х.: ХУПС, 2015. –№ 3(20). – С. 134-141.
11. Смирнов С. А. Комплекс gert-моделей технологии облачной антивирусной защиты телекоммуникационной системы / А. А. Смирнов, А. К. Дидык, А. Н. Дреев, С. А. Смирнов // Безпека інформації: наук. – практ. журн. – К.: НАУ, 2015. – Т. 21, № 3. – С. 251-262.

УДК 004

В. Варченко, магістр гр. КІ-18М-1,4
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ ПРОЕКТУВАННЯ АРХІТЕКТУРИ WI-FI МЕРЕЖ ДЛЯ ОПЕРАТОРІВ ТЕЛЕКОМУНІКАЦІЙНИХ ПОСЛУГ

У статті розроблено програмне забезпечення, яке призначено для системи проектування архітектури Wi-Fi мереж для операторів телекомунікаційних послуг. Метою розробки є дослідження та програмна реалізація системи проектування архітектури Wi-Fi мереж для операторів телекомунікаційних послуг. Об’єктом дослідження є процес проектування архітектури Wi-Fi мереж для операторів телекомунікаційних послуг. Предметом дослідження є методи проектування архітектури Wi-Fi мереж для операторів телекомунікаційних послуг. Методи дослідження базуються на методах теорії телекомунікації, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи проектування архітектури Wi-Fi мереж для операторів телекомунікаційних послуг. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення
комп’ютерна інженерія, проектування мереж, Wi-Fi

Постановка проблеми. В Україні нарешті «пішли» великі проекти по впровадженню Wi-Fi – у першу чергу вони реалізуються операторами зв'язку. Крім того, будуються мережі Wi-Fi високої щільності, які стають особливо актуальними.

За два останніх роки (з 2015 по 2017 рік) число операторських хот-спотів Wi-Fi збільшилося на 35% – до 83 тис. штук. Дохід же від послуг на ринку операторського Wi-Fi виріс ще значніше: з 1,4 до 3,4 млрд грн., незважаючи на стагнацію телекомунікаційного ринку в цілому. Цей ріст зв'язаний у першу чергу з державними проектами (B2G), на які доводиться 58% доходів. Частка в доходах B2B становить 39%, а от у сегменті B2C (3% доходів) поки ніхто заробляти не навчився.

Якщо в 2015 році приблизно третина хот-спотів (29%) компанії розгортали й експлуатували самостійно, то цього року цей показник знизився до 19%. Зв'язуємо це як з розвитком мереж Wi-Fi операторами, так і зі змінами в регулюванні: усе менше компаній готові самостійно вирішувати технічні проблеми ідентифікації користувачів, як того вимагає законодавство.

Найбільше число хот-спотів Wi-Fi (67%) установлене в Києві. Явне домінування столичного сегмента вказує на відносну незрілість ринку, розвиток якого повинне супроводжуватися збільшенням частки регіонів.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи проектування архітектури Wi-Fi мереж для операторів телекомунікаційних послуг.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи проектування архітектури Wi-Fi мереж для операторів телекомунікаційних послуг.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем проектування архітектури Wi-Fi мереж для операторів телекомунікаційних послуг.

– Дослідження системи проектування архітектури Wi-Fi мереж для операторів телекомунікаційних послуг.

– Програмна реалізація системи проектування архітектури Wi-Fi мереж для операторів телекомунікаційних послуг.

Об'єктом дослідження є процес проектування архітектури Wi-Fi мереж для операторів телекомунікаційних послуг.

Предметом дослідження є методи проектування архітектури Wi-Fi мереж для операторів телекомунікаційних послуг.

Методи дослідження базуються на методах теорії телекомунікації, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Швидкість і щільність – головне в Wi-Fi

Було проведене бліцопитування для виявлення актуальних для українських замовників напрямків розвитку бездротових мереж передачі даних. Найбільш важливим виявився розвиток систем високої щільності, ледве менше голосів одержало підвищення швидкості передачі даних. Два інших запропонованих варіанти відповіді – адаптація до вимог Інтернету речей (IoT) і реалізація засобів аналітики – вибрали значно менше число фахівців.

Як приклад мережі з низькою щільністю приводимо інфраструктуру на складі, де є 30 точок доступу й усього 10 активних клієнтів. У цьому випадку проектування мережі (вибір місця установки точок доступу) визначається завданням забезпечення покриття території. Протилежний приклад об'єкта, де необхідна мережа HD, – конференц-зал, у якому можуть збиратися кілька сотень людей. Для покриття всієї площі такого залу цілком достатньо однієї точки доступу, однак вона не зможе обслужити навіть сотню клієнтів, тому традиційний підхід до проектування не годиться.

Багато компаній уже наступили на граблі, розгорнувши «звичайні» мережі Wi-Fi: коли в зоні покриття однієї точки доступу виявлялася сотня людей [з мобільними пристроями], така мережа «лягала». За оцінкою експертів, саме показник 50-100 активних клієнтів на одну точку доступу є тією границею, починаючи з якої має сенс говорити про рішення високої щільності.

Представимо ряд загальних рекомендацій із проектування й побудови мереж Wi-Fi високої щільності. Ключовими факторами завжди є планування радіосистеми й вибір антен. Якою би функціональністю не володіла система, при поганому радіопокриті нічого не допоможе. У системах HD, потрібні маленькі стільники зі спрямованими антенами.

Малий розмір стільники гарантує високу швидкість і ефективність (низька частка повторних передач), а спрямовані антени – мінімізацію інтерференції між зонами, що обслуговуються точками доступу, які працюють на одному частотному каналі. При виборі місця розміщення й орієнтації антени повинна завжди забезпечуватися пряма видимість всіх клієнтів, а для рівномірного розподілу клієнтських пристроїв між точками доступу не слід допускати ні занадто «яскравих», ні білих плям.

Сама Cisco пропонує кілька варіантів спрямованих антен з різними діаграмами. Крім того, в арсеналі компанії є точки доступу (моделі 3800), до яких можна підключити дві різні антени для роботи в одному частотному діапазоні (5 Ггц), але на різних каналах. Таке комбінування антен дозволяє забезпечити оптимальне формування зони обслуговування.

Інша рекомендація фахівця Cisco – використовувати якнайменше ідентифікаторів SSID. На кожний SSID точка доступу раз в 100 мс відправляє спеціальне повідомлення Beacon, що анонсує її присутність. Розмір цього повідомлення в середньому 180 байт. При чотирьох SSID, настроєних на точці доступу, відсилання сигнальних повідомлень при швидкості 1 Мбіт/с займають до 70% ефірного часу. Звичайно досить двох SSID на мережу: наприклад, один ідентифікатор для співробітників, що проходять автентифікацію за допомогою механізму 802.1x, інший – для гостей, що входять через Web-сайт. Крім того, підтримку мінімальних швидкостей варто відключити, тому що саме на таких швидкостях пересилаються сигнальні повідомлення. Так, у розглянутому вище прикладі із чотирма SSID при швидкості 12 Мбіт/с частка «з'їдається» службовими повідомленнями пропускної здатності зменшується до 6%.

Наступна рекомендація від Cisco пов'язана з відключенням наявної на об'єкті мережі. Перехід на єдину БЛОМ із високою щільністю дає масу переваг, у тому числі підвищення ефективності використання частотного ресурсу. Частка керуючого трафіку звичайно скорочується з 30-40% до менш 1% ефірного часу, що залишає більше ресурсів для корисного трафіку.

Ще одна рада – максимально спростити підключення користувачів до мережі. Справа в тому, що підключений пристрій генерує набагато менше службового трафіку (Probe Request), чим непідключене, котре постійно шукає, куди йому підключитися, відправляючи на кожному каналі запити з усіма відомими йому SSID. Ідеальний варіант – технологія Hotspot 2.0, що забезпечує «прозоре» підключення, що не вимагає від користувача взагалі ніяких дій. Відносно простий спосіб надає й Web-автентифікація. А от необхідність перегляду при підключенні до мережі декількох рекламних роликів може дратувати користувача, що знижує частку підключень.

Ворогами мереж Wi-Fi високої щільності, крім сторонніх ТД, є перешкоди, походження яких не пов'язане з Wi-Fi. Відеокамери, бездротові аудіосистеми, освітлювальне встаткування, піротехнічні й інші системи можуть займати частоту Wi-Fi (2,4 Ггц). Подібні джерела перешкод можуть повністю «убити» мережа Wi-Fi. Методи боротьби зрозумілі: треба або виключити джерела перешкод, або перемінити частоти.

Крім загальних рекомендацій, кожний виробник пропонує власні ноу-хау, що спрощують побудову мереж HD. Так, наприклад, Ruckus відома рядом технологій, які значно підвищують ефективність роботи мережі Wi-Fi у режимі високої щільності. Це, зокрема, алгоритм BeamFlex, що забезпечує формування точкою доступу унікальних діаграм спрямованості для кожного окремого клієнта відповідно до особливостей радіосереди в цей момент часу в даному місці. Крім того, антени ТД Ruckus працюють в обох полярізаціях (вертикальної й горизонтальної), що гарантує більше якісну взаємодію зі смартфонами й планшетами, орієнтація яких у просторі щодо антен точки доступу постійно міняється.

Аналітика Wi-Fi

Ті ж самі службові повідомлення, які можуть викликати негативний ефект, знижуючи ефективність роботи мереж Wi-Fi, виявляються надзвичайно корисними для одержання різних аналітичних даних. Пристрої Wi-Fi постійно посилають запити Probe Request, у яких утримуються їх (пристроїв) унікальні MAC-адреси. Це дозволяє відстежити появу конкретного пристрою в зоні обслуговування даної точки доступу й одержати відповіді на питання: що за апарат використовується, коли він уперше з'явився в даній зоні, як часто вертається в неї й т.д. А вимір сили сигналу дає можливість обчислити координати пристрою й визначити, як воно переміщається. Ця інформація може виявитися корисної для торгових центрів, транспортних вузлів та ін., оскільки дозволяє довідатися, скільки людей проходять повз дану зону (наприклад, магазина), скільки заходять у неї, як довго там затримуються, звідки приходять, куди йдуть і т.д.

Найпростіший варіант – установлення факту присутності клієнта Wi-Fi у даній зоні. У цьому випадку координата пристрою не визначається. Для визначення присутності просто виміряється рівень сигналу від пристрою Wi-Fi (RSSI) і фіксується його знаходження в межах покриття даної зони. При цьому звичайно задається якийсь граничний рівень сигналу, щоб виключити користувачів, що перебувають за межами зони, що цікавить.

Координати пристрою звичайно обчислюються по методу тріангуляції. Відстань від ТД до клієнта розраховується по потужності отриманого сигналу. Дані від однієї точки доступу дозволяють визначити, що пристрій може перебувати на окружності розрахункового радіуса. Коли пристрій перебуває в межах видимості двох точок доступу, можна встановити лінію, на якій воно перебуває. У випадку трьох і більше – розрахувати місце знаходження (у точці перетинання трьох окружностей). Точність такого методу залежить від кількості й розташування точок доступу й становить 5-10 м.

Періодичність оправлення запитів Probe Request залежить від моделі конкретного мобільного пристрою, однак з урахуванням прагнення виробників підвищити час автономної

роботи пристроїв спостерігається тенденція до зниження частоти відправлення Probe Request. Деякі пристрої генерують такі запити раз у дві хвилини. Це занадто великий інтервал, щоб відслідковувати переміщення людини з потрібним рівнем деталізації. Cisco розробила спеціальну технологію FastLocate, що дозволяє відслідковувати трафік і одержувати інформацію частіше: 6-8 разів у мінуту. Цього досить, щоб установити маршрут переміщення клієнта. Для реалізації алгоритму FastLocate використовується спеціальний модуль сканування, установлюваний у точки доступу Cisco 3600 і 3700.

Ще одна з розробок Cisco для поліпшення збору аналітичних даних – Cisco Hyperlocation. Однойменний модуль містить масив з 32 антен, що надівається на ТД і дозволяє визначити кут, під яким перебуває пристрій щодо точки доступу (Angle of Arrival, AoA). При застосуванні методу тріангуляції виходять не три плями, а три вектори, що підвищує точність визначення координат до 1-3 м. Крім того, знання потужності сигналу RSSI і кута AoA дає можливість оцінити, де перебуває пристрій, навіть при наявності однієї точки доступу.

Особливістю модуля Hyperlocation є убудована підтримка Bluetooth Low Energy (BLE). Як і Wi-Fi, технологію BLE можна використовувати для фіксації факту знаходження пристрою в зоні «чутності» мітки iBeacon. Такі мітки коштують зовсім недорого, однак вони мають потребу в періодичній заміні батарейок, до того ж мітка легко може бути безконтрольно перенесена в інше місце. Рішення Hyperlocation з убудованою міткою iBeacon позбавлено таких недоліків.

Технологія BLE може використовуватися для примусової доставки по каналі Bluetooth різних повідомлень на, що перебувають поруч із міткою пристрою. Крім того, для передачі повідомлень можуть бути задіяні технології RFID і NFC.

Для реалізації функцій по зборі аналітичних даних, крім інфраструктури Wi-Fi, у випадку вибору рішення Cisco необхідний ще сервер CMX (Connected Mobile Experience), де властиво й накопичуються дані. Дане рішення користується все більшою популярністю: у світі вже більше 2100 замовників розгорнули системи аналітики на базі CMX, три проекти реалізовані в Україні.

Wi-Fi як помічник/конкурент мережам стільникового зв'язка

Одним з напрямків розвитку мереж Wi-Fi є їхнє використання для розвантаження (off-load) мереж стільникового зв'язка. Кілька років назад ця тема активно обговорювалася, але до реальних проектів справа не дійшла. Головна причина в тому, що основні інвестиції операторів стільникового зв'язка були спрямовані на розвиток мереж 4G/LTE. Забезпечувані цими мережами високі швидкості передачі даних, поряд з їх невисокою поточною завантаженістю, і сьогодні дозволяють операторам стільникового зв'язка відкладати питання про впровадження рішень для розвантаження. Однак, на думку багатьох експертів, уже найближчим часом це питання стане актуальним.

Більше того, у перспективі мережі Wi-Fi можуть не тільки «допомагати» мережам стільникового зв'язка, але й, «вийшовши» на вулицю, конкурувати з ними. Число хот-спотів Wi-Fi, які знаходяться поза приміщеннями (outdoor) в Україні за останні два роки виросло з 14,9 до 21,9 тис. штук, так що тепер на них доводиться 27% всіх установлених хот-спотів. Дуже активно розвиваються проекти міського Wi-Fi. Всі частіше міські адміністрації звертаються до операторів із проханням покрити мережею Wi-Fi тимчасово або постійно різні території: місця проведення масових заходів, парки, зупинки суспільного транспорту та ін. Москва тут також стає прикладом для наслідування: слідом за столицею керівництво інших міст прагне створювати зручний інформаційний простір для взаємодії з городянами й гістьми.

Провідні виробники систем Wi-Fi мають у своєму арсеналі готові рішення для реалізації схем розвантаження. Так, наприклад, самий продуктивний контролер Ruckus – модель SCG-200, що підтримує до 10 тис. точок доступу (при розгортанні кластера контролерів з резервуванням 3+1 число підтримуваних точок доступу зростає до 30 тис.), – виконує функції не тільки контролера мережі Wi-Fi, але й шлюзу для інтеграції з ядром

(core) мереж стільникового зв'язка. Така інтеграція створює умови для розвантаження мережі стільникового зв'язка шляхом передачі «важкого» трафіку даних через Wi-Fi відразу в Інтернет.

Однак амбіції оператора мережі Wi-Fi можуть не обмежуватися тільки допомогою в розвантаженні стільникових мереж. Усе більше операторів по усьому світі будують плани стати повноцінними віртуальними операторами стільникового зв'язка (Full MVNO). Відмінність від звичної моделі MVNO полягає в тому, що оператор Full MVNO має у своєму розпорядженні практично всю інфраструктуру, необхідну для надання послуг стільникового зв'язка, – за винятком лише базових станцій. І передові виробники істотно доробили свої технічні рішення в справі реалізації Full MVNO.

Так, компанія Brocade (якої, нагадаємо, тепер належить Ruckus) пропонує віртуалізовану реалізацію функціонала ядра EPC (vEPC), що може бути інтегрований з мережею Wi-Fi. Як відзначає Олексій Зайцев, в vEPC є всі елементи класичного ядра EPC, включаючи засобу для зберігання користувальницьких даних і формування SIM-Карт. При цьому розгортання цієї системи незрівнянно простіше, ніж традиційного ядра EPC. Із завданням, як затверджує фахівець Ruckus, може легко впоратися один інженер.

Згодом «повноцінні» MVNO можуть почати будувати й власні мережі радіодоступу, якщо, звичайно, це виявиться більш вигідним ніж розвиток мереж Wi-Fi.

Розробка структурної схеми

З появою в нашім житті мережі Інтернет, люди стали придумувати всі нові й витончені способи з'єднання із всесвітньою павутиною. Зараз dial-up модем викликає ностальгічну посмішку, а користувачі уриваються в мережу Інтернет на більших швидкостях, використовуючи бездротові технології.

На сьогоднішній день існує велика кількість протоколів для такої передачі даних і одним із сам зручних, популярних і цікавих є Wi-Fi.

Назва Wi-Fi розшифровується як Wireless Fidelity і дивно переводиться – бездротова відданість.

Технології Wi-Fi є самими перспективними в області комп'ютерного зв'язку.

Користуватися таким зв'язком дуже зручно й просто, от кілька переваг підключення до мережі за такою технологією:

– мобільність – ви одержуєте Інтернет, де вам зручно;

– немає проводів, немає сигналу зайнято, вам варто тільки включити свій пристрій, будь те ноутбук, комунікатор або смартфон і ви миттєво виявіться в мережі Інтернет;

– висока швидкість передачі даних – до 11 Мбіт/с;

– простота використання;

– користуватися таким з'єднанням зручно й вигідно хоч де, навіть у роумінзі.

У цей час у багатьох більших містах активно розробляється й запускається безліч проектів по організації мереж Wi-Fi у місцях великого скупчення користувачів телефонів, комунікаторів, смартфонів, і ноутбуків. І називається таке місце « Хот-спот» – точка доступу, що дозволяє користувачам підключитися до мережі Інтернет практично там, де вони цього хочуть – 24 години на добу й всі 7 днів у тиждень.

Наприклад, на вулицях деяких міст США «ростуть» гарні чотирьохметрові пластикові квіти. І завдання цих незвичайних квітів складається не тільки в прикрасі вулиці, але ще й для доступу користувачів в Інтернет-Простір.

Величезний розмір пелюстків це сонячні батареї, таким чином, виробляється електрика для роботи пристроїв. Одна така квітка може підключати до мережі до 10 чоловік. Біля квітів розташовані зручні крамнички, а якщо у вас сіл акумулятор, то зарядити його ви зможете прямо там же. Усе передбачено для відпочинку людей і для роботи техніки.

Так що, тепер щоб поспілкуватися в мережі із друзями або знайти необхідну інформацію зовсім не обов'язково шукати Інтернет-Кафе й комп'ютер. Досить просто мати портативний бездротовий пристрій з убудованим інтерфейсом Wi-Fi і знайти унікальне місце – « Хот-спот». До речі, більшість таких місць провайдери надають користувачам

абсолютно безкоштовно. Будь-який бажаючий може помандрувати по мережі й не платити за це ні копійки.

WiFi ідеально пасує сучасним користувачам, які люблять бути в курсі того, що відбувається у світі й хочуть залишатися на зв'язку завжди.

Власники кафе, готелів, кінотеатрів, спортивних і торгових центрів стурбована: обов'язкова авторизація в публічних Wi-Fi мережах може поставити хрест на доступному Інтернеті й «упустити» число клієнтів і середній чек на 10-15%.

Бізнесу пропонується законне рішення проблеми й додаткові можливості для просування бренда.

Послуга являє собою рішення «під ключ» проблеми Wi-Fi авторизації. Ваші відвідувачі одержать елементарний механізм авторизації в мережі, а ви – дотримання закону без шкоди для бізнесу.

Wi-Fi хот-спот – це:

– якісний технічний супровід. Програма авторизації розроблена фахівцями, тому ви завжди можете розраховувати на грамотну консультацію й оперативну допомогу;

– лояльність клієнтів. Вибір між закладом з відкритим Wi-Fi і закладом, де не можна безкоштовно вийти в Інтернет, очевидний;

– гнучкі налаштування системи. Послуга Хот-спот передбачає вибір зони дії Wi-Fi, стандартного шаблона сторінки авторизації або індивідуального, обмеження по кількості й тривалості одночасних сесій;

– рішення маркетингових завдань. Ви зможете не тільки збирати розширену статистику про користувачів, але й розміщати на стартовій сторінці авторизації гарячі пропозиції й анонси заходів.

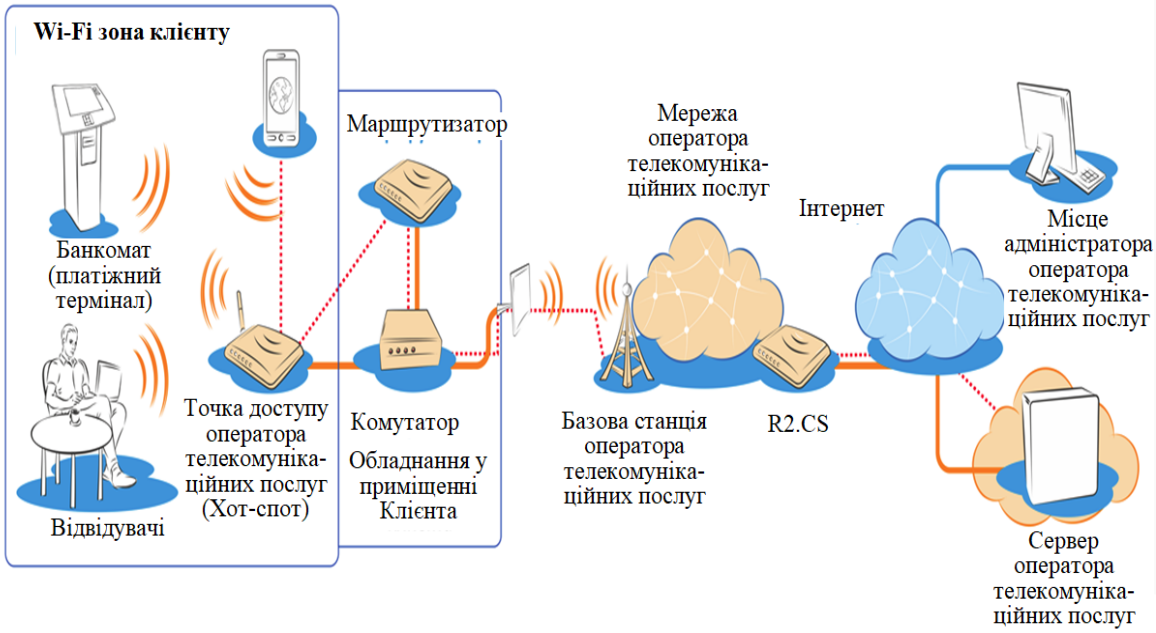


Рисунок 1 – Структурна схема системи

Висновок. У статті розглянуто та проаналізовано програмне забезпечення, яке призначено для системи проектування архітектури Wi-Fi мереж для операторів телекомунікаційних послуг. В межах України в недостатній мірі представлені вітчизняні розробки в цій області. У роботі наведені теоретичне узагальнення й рішення наукового завдання дослідження методів проектування архітектури Wi-Fi мереж для операторів телекомунікаційних послуг. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем проектування архітектури Wi-Fi мереж для операторів телекомунікаційних послуг; Досліджена система проектування архітектури Wi-Fi мереж для операторів телекомунікаційних послуг; На основі отриманих результатів

досліджень створена програмна реалізація системи проектування архітектури Wi-Fi мереж для операторів телекомунікаційних послуг. Розроблені під час виконання роботи алгоритми дозволяють успішно вирішувати завдання проектування архітектури Wi-Fi мереж для операторів телекомунікаційних послуг. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки. Розроблене програмне забезпечення має простий, дружній та зручний інтерфейс користувача, що забезпечує легкість у освоєнні роботи програмного продукту, зручність у використанні, і не потребує особливих спеціальних знань. При створені програмного забезпечення було використано об'єктно-орієнтований підхід, що відповідає сучасним тенденціям у галузі розробки комерційних програмних систем. Програма реалізована на мові високого рівня Embarcadero Delphi 10.2 Tokyo. Дана мова програмування дозволяє найбільш ефективно обробляти дані. Це дозволило мінімізувати строк розробки програмного забезпечення, і, як слід, зменшити витрати на його розробку. Запропоноване програмне забезпечення ділиться на загальне програмне забезпечення, що поставляється із засобами обчислювальної техніки й спеціальне програмне забезпечення, що спеціально розроблене для даної конкретної системи й включає програми, що реалізують її функції. Даються необхідні рекомендації з установки розробленого програмного забезпечення. Для підвищення рівня безпеки запропоновано застосовувати алгоритм Діффі-Хеллмана.

Список літератури

1. Босько В.В. Анализ и сравнительное исследование перспективных направлений развития цифровых телекоммуникационных систем и сетей / Смирнов А.А., Босько В.В., Мелешко Е.В. // Системи обробки інформації. – Х.: ХУ ПС, 2008. – Вип.7(74). – С.120-123.
2. Босько В.В. Разработка методики оценки середнего времени обслуживания информационных пакетов в телекоммуникационной сети / Смирнов А.А., Босько В.В., Мелешко Е.В. // Системи управління, навігації та зв'язку. – Київ: ДП «Центральний науково-дослідний інститут навігації і управління», 2009. – Вип. 2(10). – С.162-165.
3. Босько В.В. Разработка математической модели процесса динамического управления маршрутизацией данных в телекоммуникационной сети / Смирнов А.А., Босько В.В. // Системи управління, навігації та зв'язку. – К.: ДП «ЦНДІ навігації і управління», 2009. – Вип. 3(11). – С.208-210.
4. Босько В.В. Разработка метода определения оптимального множества путей передачи информации в телекоммуникационной сети / Смирнов А.А., Босько В.В. // Збірник наукових праць. – Х.: ХУПС, 2009. – Вип. 3(21). – С.102-108.
5. В.В. Босько. Разработка метода прогнозирования поведения информационного потока в телекоммуникационной сети // Збірник наукових праць. Харківського університету Повітряних Сил: – Х.:ХУ ПС, – 2010.-Вип. 3 (25) .- С.126-130.
6. Босько В.В. Исследование особенностей построения современных телекоммуникационных систем и сетей / Смирнов А.А., Босько В.В. // Проблемы информатики и моделирования. Материалы восьмой международной научно-технической конференции 26-28 ноября. – Х.: НТУ "ХПИ", 2008. – С.54.
7. Босько В.В. Исследование влияния времени мониторинга телекоммуникационной сети на точность прогнозирования поведения трафика / Смирнов А.А., Босько В.В. // Перша міжнародна науково-практична конференція "Проблеми й перспективи розвитку IT-індустрії" м. Харків , 18-19 листопада 2009р. – С.198-200.
8. Босько В.В. Анализ математических моделей телекоммуникационной сети / Смирнов А.А., Босько В.В. // Проблемы информатики и моделирования. Материалы девятой международной научно-технической конференции 26-28 ноября. – Х.: НТУ "ХПИ", 2009. – С.52-53.
9. Босько В.В. Метод повышения оперативности передачи данных в телекоммуникационной сети / Смирнов А.А., Босько В.В. // Збірник тез доповідей науково-практичної конференції "Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку" 24-25 березня. – Х.: АВВ МВС України, 2010. – С.54.
10. Босько В.В. Динамическое управление процессом маршрутизации данных в телекоммуникационной сети / Смирнов А.А., Босько В.В. // Тези доповідей Міжнародної науково-практичної конференції м. Вінниця, Україна 19-21 травня 2010 року. – Вінниця: ВНТУ, 2010. – С.231-232.

УДК 657

Т. Вербовіцька, магістр гр. ООУ-18мз-1,9
О. Сибірцева, магістр гр. ООУД-18М-1,9
Б. Шитик, магістр гр. ОО-18М-1,4
Центральноукраїнський національний технічний університет

ОБЛІКОВЕ ЗАБЕЗПЕЧЕННЯ ЯК ОСНОВА ФОРМУВАННЯ ЗВІТНОСТІ ПІДПРИЄМСТВА

У статті розглянуто облікове забезпечення як основа формування звітності. Доведено, що звітність підприємства є повноцінною продукцією облікової системи, яка пройшла всі стадії обробки. З'ясовано, що на якість фінансової звітності також впливають суб'єкти, відповідальні за реалізацію професійного судження – фінансовий менеджмент або головні бухгалтери. Обґрунтовано необхідність перегляду нинішньої моделі звітності внаслідок зміни методів ведення бізнесу, підходів до генерування підприємствами своєї вартості та умов ведення бізнесу, що обумовлює і зміни в обліковому забезпеченні.

фінансова звітність, облікове забезпечення, система бухгалтерського обліку, процесний підхід, обліковий інформаційний ресурс, обліковий (бухгалтерський) продукт

Подальший розвиток системи бухгалтерського обліку насамперед пов'язаний із розвитком потреб користувачів облікової інформації. З появою необхідності виділення нових видів показників бухгалтерської звітності з'являється необхідність удосконалення теоретико-методологічних аспектів функціонування облікової системи. Саме тому питання облікового забезпечення формування звітності набувають актуальності.

Теоретичні питання формування звітності і методичні підходи до її складання досліджували у своїх працях вітчизняні вчені: М. Білуха, Ф. Бутинець, Ю. Верига, С. Голов, В. Жук, О. Канцуров, Г. Кірейцев, М. Коцупатрий, М. Корягін, М. Кужельний, А. Кузьмінський, Ю. Кузьмінський, Т. Кучеренко, П. Куцик, Г. Лютова, В. Палій, М. Пушкар, В. Савчук, Н. Селіванова, В. Сопко, Л. Сук, Н. Ткаченко, В. Швець, І. Яремко та ін. За визначеним напрямком суттєвими є також роботи провідних зарубіжних дослідників: Л.А. Бернстайна, М.Ф. Ван Бреди, П.Ф. Друкера, В.Ф. Палія, Л. Петришин, Д. Панков, В. Пантелеєв, Ф. Сафанова, Я.В. Соколова, Е.С. Хендріксена, Ч. Хоргрена.

Результати досліджень учених-економістів характеризуються глибиною теоретичних висновків, значущістю висвітлених питань і узагальнень та становлять значний вклад у розвиток вітчизняної системи обліку та звітності. Проте потребують подальшого дослідження питання облікового забезпечення формування фінансової звітності.

В останні роки для удосконалення бухгалтерського обліку використовується значна кількість наукових методів і теорій, внаслідок чого відбувається поступове наближення методології наукових досліджень в сфері бухгалтерського обліку із дослідженнями в економічних, соціальних, поведінкових та інших видах наук. Всі подібні спроби можна об'єднати в два основні підходи – міждисциплінарний, що передбачає використання в облікових дослідженнях методології інших наук (інформатики, соціології, психології, лінгвістики тощо) та міждисциплінарний, що базується на використанні методології досліджень, яка може застосовуватись в будь-яких науках (системний аналіз, синергетика тощо).

Такою міждисциплінарною спробою дослідження бухгалтерського обліку є використання процесного підходу, згідно якого облікова система розглядається в якості окремого бізнес - процесу, результатом функціонування якого є створення інформаційного продукту у вигляді бухгалтерської звітності.

Відповідно, одержані на виході із системи показники бухгалтерської звітності розглядаються основним результатом організації і функціонування бухгалтерського обліку.

Однією із перших серед вітчизняних вчених, хто привернув увагу можливості розуміння системи обліку як окремого бізнес-процесу, була проф. Н. М. Малюга. На її думку, система бухгалтерського обліку виступає забезпечувальною ланкою у системі управління, тому вона призначена впорядкувати вхідну та вихідну інформацію (свій продукт) відповідно до потреб управління [4, с.33]. Відповідно, під бухгалтерським продуктом автором розуміється вся вихідна інформація, яка надається обліковою системою, тобто не лише бухгалтерська звітність, а й інші джерела інформації – узагальнюючі документи, облікові регістри тощо.

Дещо іншого підходу дотримується М. А. Проданчук, який розглядає бухгалтерський продукт як сукупність технологічних засобів, методів та процедур, які реалізують інформаційний ресурс за рахунок синергічного ефекту, від використання якого очікується прийняття ефективних управлінських рішень, що сприятимуть отриманню економічних вигод. Отже, в основі продукту бухгалтерського обліку є облікова інформація, знання та обліковий інформаційний ресурс, які мають свою вимірність, вартість, корисність та якість, використання яких у бізнес-процесах підприємства сприятиме прийняттю ефективних управлінських рішень [6]. Таку ж позицію займають проф. С. О. Левицька та К. О. Іващенко, які вважають предметом та результуючим продуктом системи обліку обліковий інформаційний ресурс, під яким, в свою чергу, розуміються дані про факти господарської діяльності, які розглядаються як інформація системи обліку за результатами процесів аналізу об'єктів, їх оцінки, реєстрації та узагальнення, що підтверджується відповідними первинними документами, регістрами та формами звітності [3, с. 66]. Таким чином, авторами вводяться в науковий обіг два нових поняття – "обліковий інформаційний ресурс" та "обліковий (бухгалтерський) продукт". Під першим розуміються бухгалтерські дані, що обробляються за допомогою облікового інструментарію, а під другим – вихідна облікова інформація, зокрема, бухгалтерська звітність.

Розгляд системи бухгалтерського обліку як певного виробничого процесу, результатом функціонування якого є створення інформаційного продукту, базується на організаційно-технічному структуруванні системи управління підприємством (рис. 1.1).

На даному етапі розвитку бухгалтерського обліку, що характеризується тенденціями гармонізації та стандартизації облікової практики, важливе значення має проблема обґрунтування набору критеріїв та норм, на основі яких має бути побудована система правил ведення бухгалтерського обліку на підприємстві.

Одним із способів їх виокремлення є розгляд бухгалтерської звітності як інформаційного продукту, що характеризується певним рівнем якості. У контексті даного підходу зрозумілим є класичне твердження, що стандартизація будь-яких бізнес-процесів, зокрема, і облікових процедур, є одним із найбільш вагомих інструментів підвищення якості продукту, який створюється системою.

Світова бухгалтерська наукова спільнота, декларуючи позицію, що в умовах сьогодення система бухгалтерського обліку виступає основним інформаційним джерелом для прийняття управлінських рішень, апріорі на перший план висуває проблему забезпечення якості облікової інформації, що надається користувачам для прийняття рішень. Тому сьогодні якість бухгалтерської інформації стала "порядком денним" для бухгалтерської професії у всьому світі. Як відмічає з цього приводу Т. Д. Поплаухіна, в умовах розширення впливу інформаційного простору на функціонування господарського об'єкта, адміністративна та оперативна діяльність суб'єктів господарювання все більше залежить від якості використовуваної інформації.

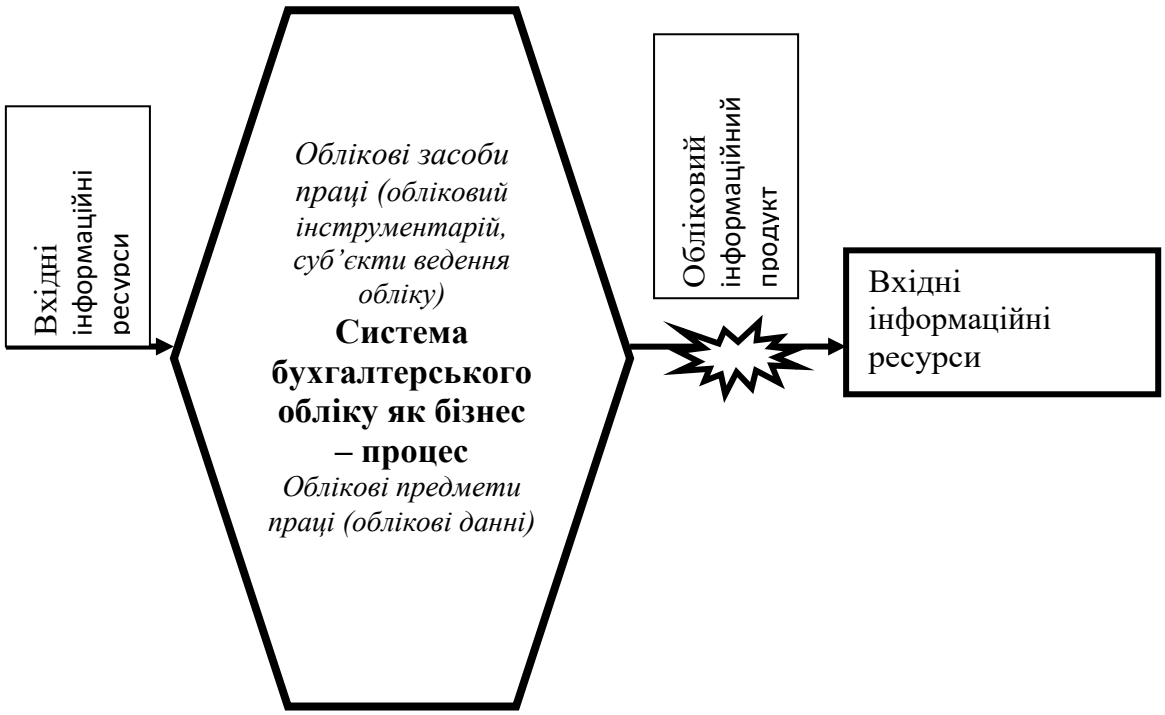


Рисунок 1.1 - Система бухгалтерського обліку якінформаційний бізнес-процес

Інформаційне забезпечення, створення і використання інформаційних каналів – необхідний компонент будь-якого менеджменту. Для формування інформаційної бази прийняття будь-яких видів рішень і організації діяльності особливе значення має якість облікової інформації, підвищення якої – це найважливіша умова підвищення ефективності вироблюваних, прийнятих і реалізованих управлінських рішень [7, с. 202]. Такої ж позиції дотримується О. С. Соколова, відмічаючи, що якість облікової інформації має першорядне значення для учасників бізнес-процесу, оскільки саме вона визначає життєздатність майбутніх стратегічних рішень [8, с. 232].

Підвищення рівня якості облікової інформації, що надається зовнішнім користувачам для прийняття інвестиційних та позикових рішень в цілому сприятиме підвищенню ефективності функціонування ринку капіталу.

Серед вчених відсутня єдність в поглядах стосовно того об'єкта, якість якого має оцінюватись та враховуватись при оприлюдненні облікової інформації. Окрім того, значна кількість дослідників одночасно використовує декілька понять в якості синонімів, наприклад, поняття якості облікової інформації та якості бухгалтерської звітності, не проводячи розмежування між ними та не розкриваючи їх суть.

Проблематику використання концепції якості в бухгалтерському обліку також можна досліджувати в контексті системи його нормативного регулювання. Як зазначає з цього приводу К. Хеллстром, сьогодні якість в бухгалтерському обліку розглядається в контексті облікових стандартів та їх характеристик (оскільки облік фіксує відповідні аспекти фірми та особливості її діяльності), застосування облікових стандартів підприємствами (ступеня використання реалізованих в стандартах альтернатив), вимог до розкриття інформації (обрана облікова політика може бути недостатньо зрозумілою, якщо вона не розкрита належним чином), оцінки інвесторами бухгалтерської інформації. Згідно такого підходу виділяються дві основні групи факторів, які впливають на якість бухгалтерського обліку. Перша група факторів пов'язана зі специфікою облікової методології, що створює можливість для прояву професійного судження бухгалтера при визнанні та оцінці об'єктів обліку. При цьому облік повинен бути організованим і вестись таким чином, щоб фінансова звітність була достовірною і неупередженою. Друга група факторів пов'язана з поінформованістю користувачів фінансової звітності про рівень її якості. Тобто, навіть за умови надання користувачам високоякісної фінансової звітності, якщо вони проінформовані

про це, їх оцінка може бути суб'єктивною, що значно вплине на прийняття ними відповідних рішень. Таким чином, інформування про рівень якості фінансової звітності забезпечує взаємозв'язок між обліковими показниками та їх реальним сприйняттям з боку користувачів облікової інформації.

За О. С. Соколовою слід проводити оцінку якості облікових показників, що передбачає визначення досяжності системою облікових показників заданого рівня критеріїв [8, с. 232]. Під обліковими показниками автор розуміє інформацію, що генерується системою бухгалтерського обліку, якість якої має бути оцінена з метою створення адекватних передумов для забезпечення її контролю.

Корягін М зазначає, що американські дослідники Д. Ебоді, Дж. Хьюз та Дж. Лю розглядають якість прибутку як показник, що вимірюється за допомогою аномальних нарахувань, які виступають в якості постійної для інформаційної асиметрії, впливаючи на вартість капіталу [1]. За підходом авторів слід визначати не лише якісь фінансової звітності, як певного інтегрованого набору звітів, а безпосередньо слід оцінювати якість прибутку, як основного її показника. Якість прибутку визначається за допомогою розрахунку відхилень між грошовими потоками і прибутком підприємства, що є досить корисним для інвесторів, оскільки дозволяє їм побачити відмінність між реальною економічною картиною підприємства та її бухгалтерською моделлю, що одержується завдяки застосуванню принципу нарахування, який дозоляє відображати в обліку і звітності доходи і витрати у момент їх виникнення, незалежно від часу надходження і сплати грошей.

На нашу думку, найбільш доцільним є використання поняття "якість в бухгалтерському обліку" стосовно бухгалтерської звітності, зокрема, фінансової звітності, яку можна вважати повноцінною продукцією облікової системи, яка пройшла всі стадії обробки.

Слід зазначити, що на якість фінансової звітності також впливають суб'єкти, відповідальні за реалізацію професійного судження – фінансовий менеджмент або головні бухгалтери. Існування можливості здійснення вибору методів обліку із представлених в стандартах альтернатив надає їм можливість впливати на показники, від яких залежить якість фінансової звітності. З метою підвищення її рівня власники повинні забезпечити належний стан корпоративного управління компанією, що в кінцевому випадку сприятиме залученню додаткового капіталу, збереженню акціонерів та побудові дієвої системи внутрішнього контролю.

При аналізі шляхів покращання якості фінансової звітності не слід виключати роль суб'єктів, які одночасно виступають користувачами та особами, що встановлюють рівень її якості.

Підвищення рівня освіченості та компетентності аналітиків, менеджменту та інших суб'єктів прийняття рішень на основі фінансової звітності – рівня їх апперцепції, теж можна вважати одним із таких шляхів. Як відмічав з цього приводу проф. Я. В. Соколов, ефективність облікової системи прямо пропорційна рівню апперцепції її користувачів. Облік може бути найдосконалішим, але він стане дійсно досконалим лише в тому випадку, якщо люди, що використовують його дані, будуть настільки ж досконалі [7, с. 243- 244]. Виходячи з чого можна констатувати, що фінансова звітність стане досконалою та високоякісною лише в тому випадку, коли паралельно зі змістовним удосконаленням фінансової звітності відбуватиметься підвищення рівня апперцепції вітчизняних користувачів фінансової звітності.

Досить нестандартний підхід до удосконалення якості фінансової звітності пропонує Л. Н. Кузнецова. Такий підхід теж можна віднести до удосконалення організаційних аспектів формування фінансової звітності, однак, на особливу увагу заслуговують пропозиції автора стосовно шляхів удосконалення організації обліку і складання звітності, в основі яких покладено застосування мотиваційного механізму. Зокрема, автором пропонується запровадження національної премії якості в сфері бухгалтерського обліку шляхом розробки індикаторів, що враховуватимуть облікову специфіку, яка має здійснюватись в розрізі наступних категорій підприємств:

– підприємства, що надають професійні послуги (аудиторські, консалтингові, аутсорсингові тощо);

– спеціалізовані видавництва з бухгалтерського облікута інтернет-ресурси;

– навчальні заклади, що здійснюють підготовку спеціалістів з бухгалтерського обліку;

– бухгалтерські служби юридичних осіб [2, с. 79-80].

Практична реалізація наведених Л. Н. Кузнецовою пропозицій дозволить не лише визначити суб'єктів ведення обліку і суб'єктів, що сприяють удосконаленню бухгалтерської професії, а також дозволить ідентифікувати пріоритетні напрями удосконалення бухгалтерського обліку, що забезпечуватимуть підвищення якісного рівня фінансової звітності. За результатами проведеного дослідження можна побудувати наступну модель якісної взаємодії між обліковою системою та користувачами облікової інформації (рис. 1.2).

Ця модель (рис. 1.2) дозволяє пояснити, в якому контексті є можливим розгляд питань, присвячених проблематиці якості фінансової звітності.

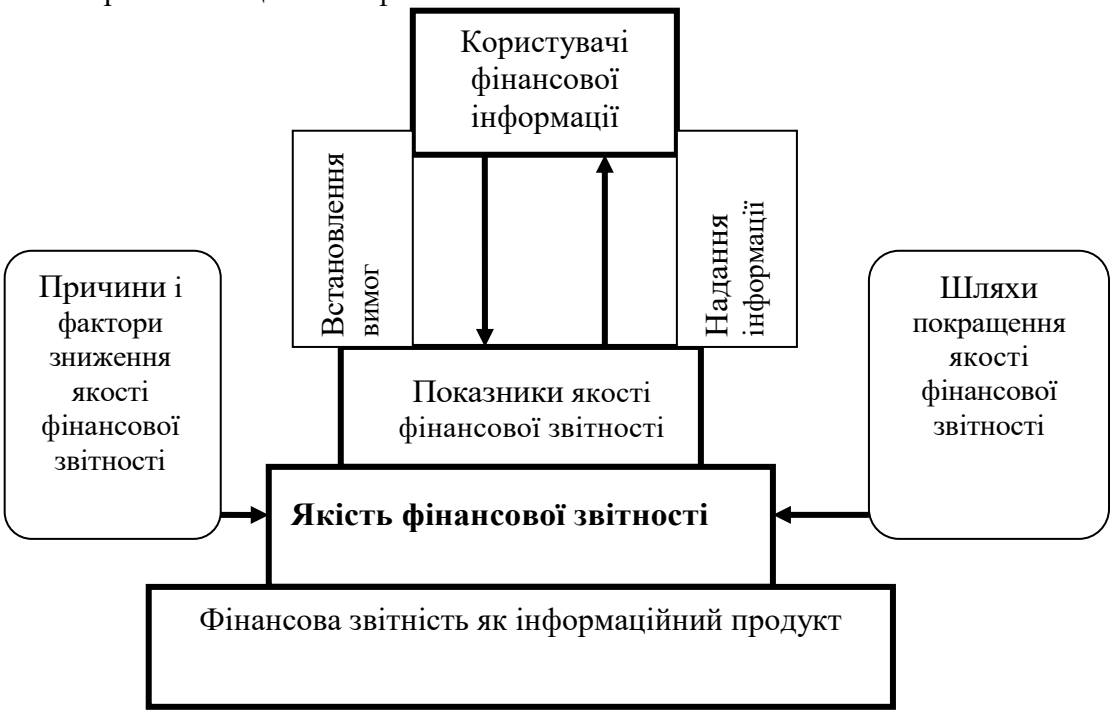


Рисунок 1.2 - Модель взаємодії бухгалтерського обліку як бізнес-процесу та користувачів облікової інформації

Отже, розуміння бухгалтерського обліку як окремого бізнес-процесу передбачає можливість розгляду фінансової звітності як облікового інформаційного продукту, що створюється із відповідним рівнем якості. На якість фінансової звітності впливає ряд об'єктивних і суб'єктивних факторів, вплив яких можна нівелювати шляхом підвищення змістовного наповнення фінансової звітності та проведення формально-організаційних заходів.

Одним із основних критеріїв відмінності між обліковими даними та інформацією є здатність приймати управлінські рішення. Тому саме показники фінансової звітності, що використовуються для прийняття рішень є кінцевим інформаційним продуктом, який необхідний внутрішнім та зовнішнім користувачам. Окремі показники фінансової звітності теж недоцільно розглядати в якості облікового продукту, оскільки для прийняття управлінських рішень слід мати комплексну картину про стан та результати діяльності підприємства, що неможливо зробити за допомогою одного або декількох показників.

Дану тезу також підтверджує поява тенденції доповнення показників фінансової звітності нефінансовими показниками, які дозволяють надати користувачам інформацію про

“приховані” фактористворення / руйнування вартості, що не потрапляють до складу об’єктів облікового спостереження, які визначаються чинними національними та міжнародними обліковими стандартами.

Сьогодні серед вчених немає єдиного підходу стосовно набору критеріїв, на основі яких визначається рівень якості фінансової звітності. Крім того, сьогодні бухгалтерська звітність не повинна концентрувати свою увагу лише на діяльності підприємства та його мікрозовнішньому середовищі, а також повинна сприяти наданню відповіді на актуальні проблеми функціонування соціально-економічних систем, у тому числі на нагальні соціальні, екологічні та управлінські проблеми.

Зокрема, в дискусійному документі Комітету з міжнародної інтегрованої звітності (IIRC) “До інтегрованої звітності. Об’єднуючи вартість у XXI столітті” було чітко обґрунтовано необхідність перегляду нинішньої моделі звітності внаслідок зміни методів ведення бізнесу, підходів до генерування підприємствами своєї вартості та умов ведення бізнесу. Ці зміни є взаємозалежними і відображають наступні тенденції: глобалізація; зростання політичної діяльності у всьому світі у відповідь на фінансову, управлінську та інші кризи; завищені очікування корпоративної прозорості та підзвітності; фактичний і перспективний дефіцит ресурсів, зростання кількості населення і екологічні проблеми. Для врахування всіх цих змін генерування лише фінансової звітності або додаткової нефінансової звітності в розрізі окремих аспектів діяльності підприємства (соціальних, екологічних, інноваційних тощо) вже є недостатнім, оскільки користувачам потрібна дещо ширша (не про об’єкти обліку, а про фактори створення і руйнування вартості) і по- іншому (більш цілісно) структурована інформація для прийняття рішень. Тому існуюча облікова система та парадигма звітності, яка формується на її основі, мають бути трансформовані, щоб забезпечити усунення подібних “прогалин” та забезпечити адекватність бухгалтерського обліку сучасним соціально- економічним реаліям.

Вихідна інформація є цінним ресурсом для системи прийняття рішень на всіх рівнях внутрішнього та зовнішнього середовища, регулюючи формування та реалізацію керівного впливу, що позначається на організації господарської діяльності підприємств та оптимізації взаємовідносин між групами користувачів управлінської інформації.

Список літератури

1. Корягін М. В., Куцик П. О. Проблеми та перспективи розвитку бухгалтерської звітності [Текст] : монографія / М. В. Корягін, П. О. Куцик. – Київ : Інтерсервіс, 2016. – 276 с.
2. Кузнецова Л. Н. Совершенствование методики и методологии бухгалтерского учета на основе премии качества / Л. Н. Кузнецова // Вестник Адыгейского государственного университета. Экономика. – Майкоп : изд-во АГУ. – 2010. – Вып. 3(66). –С. 73-82.
3. Левицька С. О. Обліковий інформаційний ресурс: теоретичний аспект / С. О. Левицька, К. О. Іващенко // Зимові читання, присвячені видатним вченим в галузі бухгалтерського обліку, аналізу і контролю : збірник тез Одинадцятої Всеукраїнської наукової Internet- конференції ЖДТУ. – 2013. – С. 65-68.
4. Малюга Н. М. Бухгалтерський облік в Україні: теорія й методологія, перспективи розвитку : [монографія] / Н. М. Малюга. – Житомир : ЖДТУ, 2005. – 548 с.
5. Поплаухина Т. Д. Качество учетно-аналитической информации как научная категория / Т. Д. Поплаухина // Актуальные вопросы экономики и управления : материалы междунар. науч. конф. (г. Москва, апрель 2011 г.). – Т. I. – М. : РИОР, 2011. – С. 202-205
6. Проданчук М. А. Продукт бухгалтерського обліку у системі прийняття управлінських рішень / М. А. Проданчук // Ефективна економіка. – 2014. – № 7. – [Електронний ресурс]. – Режим доступу : http://www.economy.nayka.com.ua/?op=1&z=3203
7. Соколов Я. В. История бухгалтерского учета : [учебник] / Я. В. Соколов, В. Я. Соколов. – [2-е изд., перераб. и доп.]. – М., 2006. – 274 с.
8. Соколова Е. С. Методы оценки качества учетной информации / Е. С. Соколова // Экономические науки. – 2009. – № 5(54). – С. 293-299.

УДК: 633.31

І. Вечірко, магістр гр. АГ-18М-1,9
В. Резніченко, канд. с.-г. наук, доц.
Центральноукраїнський національний технічний університет

ВПЛИВ МІКРОДОБРИВ НА ПРОДУКЦІЙНИЙ ПРОЦЕС ЛЮЦЕРНИ

Проаналізовано вплив мікроелементів на проходження вегетаційного періоду у сільськогосподарських культур. Встановлено вплив передпосівної обробки та підживлення хелатних мікродобрив, у різні фази росту та розвитку люцерни, на урожайність зеленої маси досліджуваної культури
люцерна, мікродобрива, урожайність, зелена маса.

Для нормального росту та розвитку сільськогосподарських культур, в тому числі і бобових трав, недостатньо лишень задовольнити їхні базові потреби у азоті, фосфорі, калії, кальції, магнії та сірці, а також важливі мікроелементи.

Роль мікроелементів в мікродобривах багатогранна, але нажаль недооцінена, адже недолік мікроелементів в життєзабезпеченні сільськогосподарських культур є такою ж важливою проблемою, як і відсутність потрібної кількості азоту, фосфору або калію, оскільки всі елементи живлення взаємозв'язані.

Для вирощування високих і сталих врожаїв сільськогосподарських культур поряд з біоелементами (C, H, O, N, P, K, Ca, Mg, S) важливе значення в живленні рослин мають ще близько 18 елементів, передусім – B, Mn, Cu, Zn, Co, Mo. Оскільки вміст цих елементів у рослинах і ґрунтах досить малий (0,01-0,001 % у перерахунку на суху речовину), їх називають мікроелементами, а добрива, що їх містять – мікродобривами. Для отримання високих повноцінних врожаїв сільськогосподарських культур необхідно враховувати їх вимоги до мікроелементного складу живильного середовища.

Мікроелементи входять до складу ферментативних систем, покращують обмін речовин, сприяють нормальному перебігу фізіологічних та біохімічних процесів, впливають на процес фотосинтезу.

Під дією мікроелементів зростає стійкість рослин до хвороб, несприятливих умов навколишнього середовища, покращується засвоєння макроелементів з ґрунту та добрив [1].
Їх вміст у рослинах становить не більше тисячної частки відсотка, але це не знижує їх цінність для рослин. Нестача мікроелементів зумовлює порушення фізіологічних процесів організму рослини і як наслідок зниження врожаю та погіршення його якості. Поєднання різних мікроелементів утворює різні види мікродобрив.

Дія мікроелементів на фізіологічні процеси пояснюється їх вмістом у ферментах, вітамінах, гормонах та інших біологічно активних речовинах. За оптимального забезпечення рослин мікроелементами пришвидшуються їх розвиток і достигання насіння, підвищується стійкість до хвороб і шкідників, знижується дія проти зовнішніх несприятливих чинників – посухи, низьких і високих температур повітря та ґрунту. На відміну від пестицидів мікроелементи підвищують імунітет рослин.

Не достатня кількість елементів живлення на початкових етапах, може не мати візуальних проявів, але це призводить до значного зменшення врожайності культури, оскільки біохімічні процеси пригнічені дефіцитом елемента [2].
Перш за все, мікроелементи життєво важливі для рослин і чинять пряму дію на організм, їх специфічний біохімічний вплив не можна замінити іншими речовинами. Без них рослина не може ні рости, ні завершити деякі метаботичні цикли. Їх нестача обов'язково має бути

компенсована, лише тоді можна отримати якісну продукцію, яка відповідає оптимальному вмісту для певного сорту цукрів, амінокислот, вітамінів.

Ще донедавна мікроелементи застосовували в так званій сольовій формі, тобто у вигляді неорганічний солей металів, що мають цілий ряд недоліків (токсичність, шкідливість для ґрунту, засвоєння рослинами лише на 20-30 %). В теперішній час на зміну солям прийшли хелати мікроелементів – складні органічні комплексні сполуки, які забезпечують високий рівень засвоєння елементів живлення (на 90-95 %), швидку ліквідацію дефіциту мікроелементів в період вегетації, зменшення норми внесення мікроелементів, і відповідно підвищення рівня рентабельності рослинницької продукції.

Існує декілька форм хелатів на основі яких виробляються мікродобрива: ЕДТА, ДТПА, ДБТА, ЕДДА, ОЕДФ, НТФ. Найбільш поширеною формою є ЕДТА.

Добрива із вмістом неорганічних солей мікроелементів, не в змозі забезпечити рослину бажаною кількістю елементів, в зв’язку з низьким відсотком засвоєння. Окрім цього, вони є токсичними для рослин і можуть визвати опіки листової пластини. Мінеральні солі за своєю ефективністю поступаються хелатним з'єднанням мікроелементів. Хелати отримують шляхом з'єднання мікроелементів і органічних кислот з утворенням сполук - хелатів. Такі сполуки розчинні у воді та повністю засвоюються рослинами. При поглинанні мембрана клітини розпізнає цей комплекс як речовину, споріднену біологічним структурам.

Бобові культури добре реагують своєю продуктивністю на позакореневе підживлення молібденом, бором, марганцем, цинком, магнієм та сіркою. Особлива роль у мінеральному живленні бобових належить молібденові, який поліпшує азотний обмін та фіксацію атмосферного азоту бульбочковими бактеріями [3].

Мікродобрива є одним із основних факторів, що впливають на продуктивність люцерни [4].

Тому, в наших дослідженнях ми звернули увагу, як впливали мікродобрива на урожайність зеленої маси люцерни (табл.1).

Таблиця 1-Вплив мікродобрив на урожайність зеленої маси люцерни, (т/га)

Обробка насіння	Позакореневе відживлення	2018 р	2019 р	середнє
Авангард-Молібден	Контроль (без підживлення)	6,54	5,49	6,02
	Підживлення у фазі 2-3 трійчастих листків	7,07	6,19	6,63
	Підживлення у фазі кінець бутонізації-цвітіння	8,46	7,22	7,84
Квантум-бобові	Контроль (без підживлення)	7,89	6,76	7,33
	Підживлення у фазі 2-3 трійчастих листків	8,37	7,74	8,06
	Підживлення у фазі кінець бутонізації-цвітіння	10,22	9,18	9,70
Реаком-СР-бобові	Контроль (без підживлення)	9,17	6,46	7,82
	Підживлення у фазі 2-3 трійчастих листків	10,67	9,07	9,87
	Підживлення у фазі кінець бутонізації-цвітіння	13,48	11,75	12,62

Як, показали наші дослідження показники урожайності зеленої маси люцерни у 2018 році були вищими у порівнянні до показників урожайності 2019 року, оскільки гідротермічні показники в 2019 році були менш сприятливими для розкриття біологічного потенціалу досліджуваної культури.

На варіантах, де використовували мікродобрива Авангард-Молібден за передпосівної обробки насіння та за підживлення забезпечили найнижчу урожайність у порівнянні до інших варіантів досліду, та відповідно забезпечило в середньому на контролі (без підживлення) – 6,02 т/га; за підживлення у фазі 2-3 трійчастих листків – 6,63 т/га, що перевищувало контроль на 0,61 т/га; а за підживлення у фазі кінець бутонізації-цвітіння – 7,84 т/га, що перевищувало контроль та перше підживлення на 1,82 та 1,21 т/га, відповідно.

Як, показали наші дослідження, на варіантах за використання мікродобрива Квантум-бобові показники урожайності люцерни, в середньому по роках, були вищими до попередніх в межах 17- 19 %.

Також, в наших дослідженнях ми звернули увагу, як впливали мікродобриво Реаком-СР-бобові на урожайність зеленої маси люцерни.

Встановлено, що досліджувана культура сформувала максимальну урожайність за передпосівної обробки та підживлення Реаком-СР-бобові. Так, на варіантах за передпосівної обробки та (без підживлення), забезпечило в середньому по роках, урожайність зеленої маси 7,82 т/га, що перевищувало аналогічні варіанти за використання Авангард-Молібден було вище на 23,1%, а Квантум-бобові на 6,3%.

За підживлення у фазі 2-3 трійчастих листків досліджуваний показник склав 9,87 т/га, що був вищий від контролю на 2,05 т/га, тоді як на аналогічних варіантах за використання Авангард-Молібден було вище на 32,8%, а Квантум-бобові на 18,3%.

На варіантах за підживлення у фазі кінець бутонізації-цвітіння урожайність зеленої маси склала 12,62 т/га, що було вищим від контролю на 4,8 т/га, тоді як на аналогічних варіантах за використання Авангард-Молібден було вище на 37,9 %, а Квантум-бобові на 23,1%.

Отже, мікродобрива мали позитивний вплив на урожайність зеленої маси люцерни. Встановлено, що оптимальні умови утворилися на варіантах за використання мікродобрива Реаком-СР-бобові та забезпечило найвищу урожайність за передпосівної обробки насіння та підживлення у фазі кінець бутонізації-цвітіння, що в середньому по роках досліджень склало в межах 12,62 т/га.

Список літератури

1. Городній М.М. Агрохімія. – К.: Арістей, 2008. – 936с.
2. Лісовал А.П., Макаренко В.М., Кравченко С.М. Система застосування добрив. – К.: Вища школа, 2002. – 317с.
3. Власюк П.А. Биологические элементы в жизнедеятельности растений.- К.: Наук.думка.-1969
4. Шешела Т.А. Вплив мікроелементів на урожайність насіння люцерни в умовах зрошення //Т.А. Шишела – Землеробство - №7 – 2009 – с.45.

УДК 004

В. Вороний, магістр гр. КІ-18М-1,4
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ПОБУДОВАНОЇ НА ОСНОВІ РІШЕНЬ AXIS

У статті розроблено програмне забезпечення, яке призначено для системи забезпечення безпеки побудованої на основі рішень Axis. Метою розробки є дослідження та програмна реалізація системи забезпечення безпеки побудованої на основі рішень Axis. Об’єктом дослідження є процес забезпечення безпеки побудованої на основі рішень Axis. Предметом дослідження є методи забезпечення безпеки побудованої на основі рішень Axis. Методи дослідження базуються на методах теорії кодування, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи забезпечення безпеки побудованої на основі рішень Axis. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

комп’ютерна інженерія, відеонагляд, Axis

Постановка проблеми. Цього року компанія Axis відзначає 20-річчя появи першої мережної камери – Axis NetEye 200. У порівнянні з функціоналом сучасних камер відеоспостереження, її характеристики – 1 кадр у секунду з розв'язною здатністю CIF (352 на 288 пікселів) – можна назвати допотопними. Першопрохідникам далеко не завжди вдається удержатися на лідерських позиціях, але Axis продовжує залишатися як технологічним, так і ринковим лідером. Незважаючи на багаторазово зрослу в останні роки конкуренцію, Axis як і раніше є найбільшим світовим виробником мережних відеокамер.

Торік майже 90% акцій Axis було придбано японською компанією Canon (близько 11% належить хедж-фонду Elliott Management), і новий власник пообіцяв, що міняти в її діяльності нічого не буде. Скоріше, навпаки: для розвитку власної лінійки камер відеоспостереження Canon вирішила запозичити в Axis стратегії, які дозволили останній домогтися успіху. Більше того, питання просування цих камер на європейському й американському ринках Canon передала Axis.

На дослідження й розробки компанія витрачає 15% свого доходу. За даними звіту за 2017 рік, у її портфелі налічується 150 різних продуктів, а за рік представлено 30 нових. Як головні цілі називаються щорічний 20-процентний ріст оберту й перетворення в провідного постачальника мережних рішень безпеки.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи забезпечення безпеки побудованої на основі рішень Axis.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи забезпечення безпеки побудованої на основі рішень Axis.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем забезпечення безпеки побудованої на основі рішень Axis.
– Дослідження системи забезпечення безпеки побудованої на основі рішень Axis.
– Програмна реалізація системи забезпечення безпеки побудованої на основі рішень Axis.

Об'єктом дослідження є процес забезпечення безпеки побудованої на основі рішень Axis.

Предметом дослідження є методи забезпечення безпеки побудованої на основі рішень Axis.

Методи дослідження базуються на методах теорії кодування, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Мережні камери становлять основу пропозиції Axis, тим більше що цей ринок продовжує рости. Модельний ряд регулярно обновляється (до 25% щорічно), і вибір продуктів став настільки великим, що тримати в пам'яті характеристики всіх моделей уже неможливо. Із всіх новинок згадаємо лише дві, представлені цієї восени: Axis Q 6155-E і Axis Q1659.

Купольна поворотна камера Axis Q 6155-E оснащена лазером, за допомогою якого вимірюється відстань до об'єкта, що дає можливість прискорити процес фокусування й одержати більше чітку картинку. Це дозволило Axis вирішити одну з основних технічних завдань, з якими доводиться зіштовхуватися при використанні PTZ-камер. Крім цього, чіткість зображення забезпечується за рахунок застосування нового поліпшеного сенсора й традиційних технологій Axis, зокрема Lightfinder.

Одним з результатів входження до складу Canon стала поява камер Axis з оптикою Canon. Так, нова мережна камера Axis Q1659 з розв'язною здатністю 20 Мпікс має високоякісну світлочутливу матрицю й об'єктив Canon EF/ EF-S. Застосування цих компонентів дозволило поліпшити якість передачі кольору, контрастність і деталізацію навіть при самому складному освітленні. Залежно від поставлених завдань, на камеру можна встановити кожної із семи різних об'єктивів EF/ EF-S, які завдяки використовуваній системі кріплення легко замінити.

У контексті відеоспостереження не можна не згадати й зовсім новий для Axis продукт – 16-портовий комутатор Axis T8516 з підтримкою PoE+. Як затверджується, він оптимізований для рішень відеоспостереження.

Для замовників інтерес представляють не характеристики камер, а можливості рішення, створеного на їхній основі. При цьому замовники хотіли б знати, у скільки все це їм обійдеться. Axis почала спробу проаналізувати сумарних витрат на прикладі реального проекту, що передбачає установку 1500 відеокамер для міського відеоспостереження.

Відповідно до наведених розрахунків, за 10 років витрати складуть 17 млн доларів (на оплату праці співробітників центра керування відеоспостереженням знадобиться ще 10-11 млн доларів). На апаратне й програмне забезпечення, включаючи мережні комутатори, мережу зберігання, систему зберігання й ПЗ для керування відеоспостереженням, а також на оснащення диспетчерського пункту доводиться лише 49% від загальної суми.

У такому масштабному проекті зменшення витрат навіть на кілька відсотків приведе до значної економії. Так, застосування фірмової технології стиску потоку Zipstream дозволяє знизити вимоги до пропускної здатності мережі і ємності сховищ для відеозаписів. Як затверджують в Axis, у випадку цілодобового охоронного відеоспостереження можна вдвічі зменшити навантаження на мережу й СЗД. Але якщо навіть виходити з більше консервативної оцінки в 25%, тільки за рахунок скорочення займаної ємності зберігання можна зменшити ТСО на 3%, а це по 300 доларів на камеру.

Установка якісних камер дозволяє знизити витрати на їхню експлуатацію, зокрема на заміну при виході з ладу. Як затверджують співробітники компанії, посилаючись на замовників, відеокамери Axis виходять із ладу в 4-5 разів рідше, ніж устаткування конкурентів. Таким чином, якби в проекті використовувалися менш надійні камери, витрати на їхнє обслуговування виросли б з 800 тис. до 2 млн 300 тис. доларів.

Стабільна робота пристроїв дозволила істотно скоротити витрати по технічному обслуговуванню проекту – зокрема, уникнути численних виїздів фахівців, тому що відповідно до вимог замовника заміну треба було здійснювати протягом п'яти днів, а об'єкти були розосереджені по всій території країни.

Тим часом багато інсталяторів систем відеоспостереження недостатньо інформовані про правову сторону проблеми, хоча незаконна установка відеокамери може загрожувати карним переслідуванням.

Крім схованого спостереження, забороняється використання камер з винесеною зіницею (pin hole), що працюють при низької освітленості (менш 0,01 люкс) і закамуфльованих під побутові предмети. До того ж необхідно вказувати, для чого буде здійснюватися відеоспостереження. Використання записів в інших цілях, відмінних від заявлених, є правопорушенням. Відеоспостереження може вестися тільки на виробничому місці, при цьому необхідно попереджати про це працівників, а згода на подібний контроль вони повинні давати в письмовому виді. Крім того, строк зберігання відеозаписів варто чітко визначити.

Запису відеоспостереження не є персональними даними, однак, якщо для ідентифікації використовується розпізнавання осіб, мова вже піде про біометричні персональні дані. Їхня обробка можлива тільки за згодою суб'єкта й теж у писемній формі (за винятком випадків забезпечення безпеки й обороноздатності держави). Таким чином, застосування відеоаналітики в роздрібних магазинах для виявлення зловмисників буде незаконним, якщо використовувана база ведеться без санкції компетентних органів.

Компанія Axis Communications представляє лінійку надкомпактних і недорогих модульних камер AXIS FA, а також три новинки в серії AXIS P13, які здійснюють зйомку зі швидкістю до 30 к/с у розв’язній здатності 4K і 5 мегапікселів і забезпечують високий ступінь деталізації навіть на більших територіях.

Камери AXIS серії FA

Модульні камери серії AXIS FA складаються із блоків: основного блоку AXIS FA54, оптичного блоку AXIS FA1105 зі стандартним об'єктивом, оптичного блоку AXIS FA1125 із

точковим об'єктивом і купольним оптичним блоком AXIS FA4115 з варіофокальним об'єктивом. Кожний із блоків можна придбати окремо. Використовуючи пристрою цієї серії, можна створити економічну малопомітну систему, що забезпечує внутрішнє відеоспостереження за чотирма прилеглими приміщеннями на базі всього одного основного блоку. Основний блок AXIS FA54 може транслювати потокове відео з повною частотою кадрів і розв'язною здатністю HDTV 1080p відразу із чотирьох підключених оптичних блоків, використовуючи одну IP-адресу. У процесі зйомки використовується технологія широкого динамічного діапазону Forensic WDR, що дозволяє розглянути погано освітлені й об'єкти, що рухаються. Крім того, блок AXIS FA54 підтримує розширені засоби відеоаналізу й обладнаний HDMI-виходом для підключення до монітора відеоспостереження або екрану в торговельному залі, що робить систему ідеальним рішенням для магазинів. Завдяки невеликому розміру оптичні блоки можна вмонтувати в різні поверхні, конструкції й пристрої, а також непомітно встановити на рівні очей, наприклад, у входу в будинок. Оптичні блоки поставляються з 8-метровим кабелем для підключення до основного блоку AXIS FA54. При необхідності можна придбати 15-метровий кабель.

Виносні оптичні блоки займають зовсім мало місця й зливаються з елементами інтер'єра, дозволяючи здійснювати малопомітне відеоспостереження. Камери серії AXIS FA є дуже вигідним рішенням, оскільки дозволяють контролювати кілька ділянок з використанням однієї високопродуктивної системи».

Новинки в серії AXIS P13

Мережні камери для внутрішньої (AXIS P1367) і зовнішньої (AXIS P 1367-E і AXIS P 1368-E) установки поповнили вже зарекомендувала себе серію стаціонарних камер AXIS P13, що ідеально підходить для відеоспостереження за міськими об'єктами, транспортом і торговельними точками. Завдяки поліпшеним показникам світлочутливості, якості зображення й частоти кадрів камери можна використовувати для спостереження за великими відкритими площадками з низькою освітленістю, такими як залізничні перони, людні міські зони або паркування, у розв'язній здатності до 4K.

Камера AXIS P1367/-E підтримує об'єктиви CS і i-CS, а AXIS P 1368-E з розв'язною здатністю 4K у стандартні комплектації поставляється з об'єктивом i-CS. Камери AXIS P 1367-E і AXIS P 1368-E призначені для зовнішнього відеоспостереження – вони оснащені інноваційною механічною платформою, що спрощує доступ до рознімань і кабелів і залишає більше місця для змінних об'єктивів. Убудовані рейки збільшують універсальність камери й дозволяють установити могутніші об'єктиви, що забезпечують велику деталізацію зображення.

Полегшені камери AXIS P 1367-E і AXIS P 1368-E є повноцінними вуличними камерами. Не просто помістили камеру в корпус: ми з нуля розробили камеру зовнішнього відеоспостереження із кріпленням CS-mount. Нам удалося створити універсальну, гнучку систему відеоспостереження, що дозволяє використовувати як варифокальні об'єктиви, так і коридорний формат Axis, призначений для клієнтів, які віддають перевагу вертикальному зображенню й не хочуть витрачати дорогоцінний трафік і місце на екрані.

Тепловізійні технології

Тепловізійні технології відрізняються надійністю виявлення об'єктів і низьким відсотком помилкових спрацьовувань, однак дотепер високоякісні тепловізійні камери були недоступні для малих організацій по економічних причинах.

Нова тепловізійна мережна камера AXIS P 1280-E для внутрішнього й зовнішнього спостереження має гнучке модульне виконання, завдяки чому тепловізійний блок можна розміщати в обмежених просторах. Камера поставляється в комплекті із широким набором приналежностей для монтажу на стіну або стелю, а також для установки заподлицо. Тепловізійна мережна камера AXIS P1290 для відеоспостереження в приміщеннях виконана в малопомітному купольному корпусі.

Камери здатні виявляти об'єкти й надавати візуальне підтвердження для забезпечення безпеки людей і майна в самих різних умовах. Камери оснащені убудованими засобами

аналізу відеоданих, у тому числі системою AXIS Video Motion Detection, що подає сигнал тривоги при виявленні руху в заданій області. Крім того, камери підтримують платформу AXIS Camera Application Platform, сумісну із широким спектром сторонніх додатків.

Там, де конфіденційність приватних осіб має першорядне значення – наприклад, у школах і інтернатах – тепловізійні камери фіксують інциденти, не розкриваючи особистості людей. Нові камери не тільки аналізують відеодані, але й можуть подавати сигнали тривоги, наприклад, при падінні пацієнта, щоб працівники могли негайно почати необхідні дії.

Розробка структурної схеми

Фіксовані корпусні відеокамери Axis несуть чітке послання потенційним порушникам: "Подумайте гарненько. За вами спостерігають". Це пов'язане з тим, що в камер фіксований, добре помітний кут огляду, тому легко зрозуміти, куди спрямована камера, і це дозволяє реєструвати події в точно певній області. У нашім портфелі фіксованих корпусних відеокамер є камери зі змінними об'єктивами CS-mount.

Модульні камери Axis можна розмістити практично в будь-якому місці, і вони будуть украй малопомітні. Їх можна встановлювати в обмежених просторах, вбудовувати в банкомати й використовувати навіть в автобусах і поліцейських автомобілях. Вони оптимально підходять для малопомітного відеоспостереження зі звуковим супроводом і аналітичними додатками. Вони також припускають мінімальні витрати, якщо потрібно розмістити кілька камер на невеликій території.

Модульні камери оснащуються оптичним блоком, з'єднаним кабелем з основним блоком, що є пристроєм обробки даних. Оптичний блок (щоскладається з об'єктива й матриці) можна розташувати там, де необхідно, а основний блок – там, де є місце. Для організації малозатратного відеоспостереження декількох розташованих поблизу зон до чотирьохканального основного блоку можна підключити до чотирьох оптичних блоків.

Щоб одержати оптимально відповідній вашій вимогам сполучення апаратних компонентів, можна придбати основні й оптичні блоки окремо. Можна також придбати заздалегідь укомплектовані модульні камери в зборі.

Будь-який варіант розміщення камер компанії Axis забезпечує найбільшу область спостереження із всіх можливих: монтаж на стінах, стовпах або колонах дозволяє одержати панорамний огляд на 360° з вертикальним кутом огляду 135°.

У камерах передбачена як дуже швидка, так і зверхповільна швидкість повороту й нахилу, що при необхідності дозволяє операторам відразу знайти потрібне місце, а в противному випадку – переглядати плавне оглядове відео. Спеціально розроблена конструкція цих пристроїв є надійної, міцної й призначена для будь-яких погодних умов.

Камери Axis можна встановити різними способами; крім того, вони оснащені SFP-слотами для передачі даних на більші відстані за допомогою оптоволоконних модулів, що забезпечує економію засобів. Резервне підключення до мережі можливо як за допомогою мережного роз’єму RJ45, так і SFP.

Повнофункціональні фіксовані камери Axis у циліндричному корпусі, що мають привабливу ціну, готові до роботи відразу ж після одержання. Маючи невеликий розмір і витончений дизайн, вони чудово вписуються в будь-яке середовище. Убудована ІЧ-підсвічування й висока якість відео означають, що вони здатні цілодобово виконувати важливу роботу із захисту вашого об'єкта як усередині приміщень, так і на вулиці.

Фіксовані купольні камери Axis – це компактні рішення з кожухом купольного типу. Вони відмінно вписуються в будь-який інтер'єр і не залучають уваги. Купол не тільки захищає камеру від ударів і спроб змінити напрямок огляду або розфокусувати зображення, але й маскує напрямок огляду. Ми пропонуємо широкий вибір фіксованих купольних моделей для зовнішньої й внутрішньої установки, що працюють удень і вночі в будь-яких умовах.

Бортові камери Axis спеціально призначені для схованого, ефективного відеоспостереження в поїздах, вагонах метрополітену, автобусах, машинах екстрених служб. Ці високоміцні камери, захищені від пилу й вологи, пристосовані до жорстких умов

експлуатації, де вони можуть піддаватися вібрації, поштовхам, ударам, перепадам температури.

Функція активного оповіщення про несанкціоновані дії в сполученні із продуманою конструкцією забезпечує надійний захист від спроб порушити працездатність камери, наприклад, покрити її об'єктив фарбою з пульверизатора, змінити її орієнтацію або розбудувати фокус, тому бортові камери Axis прекрасно підходять для установки там, де вони можуть бути піддані зовнішньому впливу.

За рахунок панорамуваня, нахилу й зума мережні PTZ-камери Axis забезпечують широкий огляд у сполученні із чудовою деталізацією зображення всього з однієї камери. Неперевершена якість зображення й можливість збільшити масштаб дозволяють перевіряти виявлені в системі безпеки події. Результатом є максимальний захист при мінімальних витратах.

Камери оснащені різними інтелектуальними функціями й можуть переміщатися в передвстановлені положення й автоматично збільшувати масштаб у відповідь на виявлені події. Крім того, їх можна з легкістю інтегрувати в систему з іншими камерами.

Пропозиція в області мережних PTZ-камер містить у собі особливо міцні моделі, що підходять для експлуатації в найсуворіших кліматичні й інших умовах.

Тепловізійні мережні камери Axis, що ідеально доповнюють собою будь-яку професійну систему охоронного IP-відеоспостереження, дозволяють забезпечити надійну охорону певної зони або периметра навіть у повній темряві.

Тепловізійні мережні камери Axis формують зображення, засноване на тепловому випромінюванні, що виходить від будь-якого об'єкта, автомобіля або людини. Завдяки цьому камери можуть працювати в повній темряві, передаючи зображення, що дозволяють операторам виявляти підозрілі події й реагувати на них цілодобово й без вихідних.

Якщо потрібно надійне цілодобове відеоспостереження 7 днів у тиждень із малою кількістю помилкових спрацьовувань, то вибір природно падає на тепловізори.

Оскільки в живих об'єктів, наприклад, людей, температура тіла звичайно відрізняється від фонової температури, те тепловізори відмінно справляються з виявленням людей при самих різних обставинах. Крім того, температура таких об'єктів як автомобілі теж відрізняється від температури навколишнього середовища, що також спрощує їхнє виявлення.

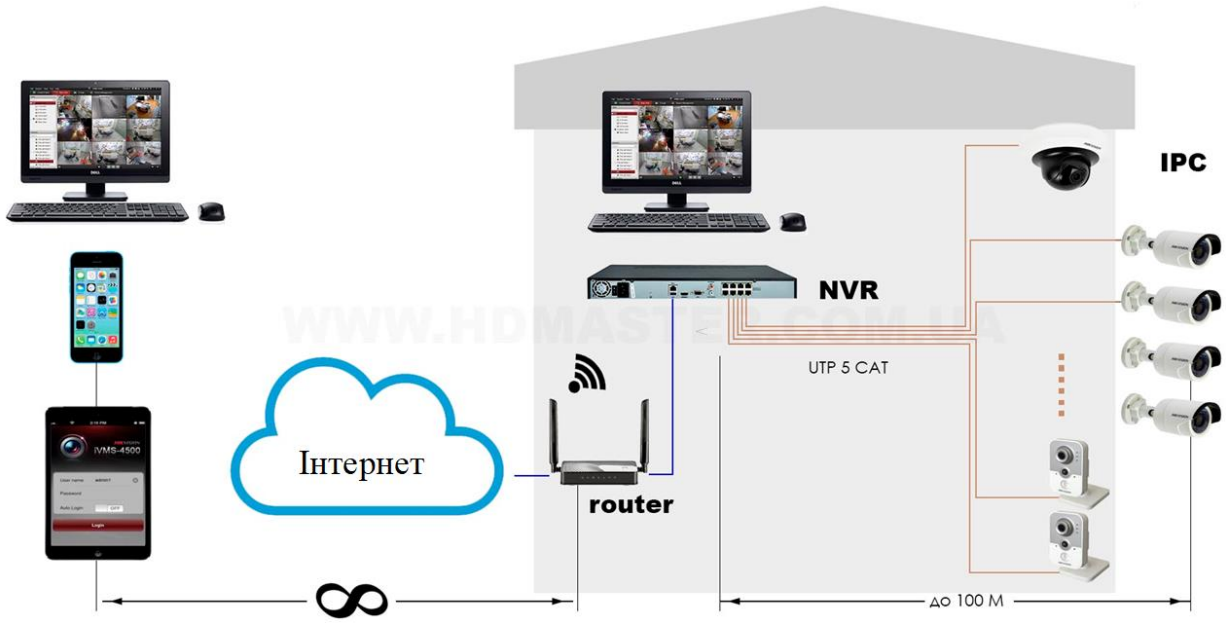


Рисунок 1 – Структурна схема системи

Тепловізори можуть застосовуватися в самих різних областях, де потрібне забезпечення безпеки – наприклад, це може бути захист периметра навколо промислових

об'єктів, аеропортів і електростанцій. Можливості тепловізорів роблять їхніми коштовними інструментами при проведенні пошуково-рятувальних операцій.

Деякі тепловізори, які в компанії Axis називаються камерами з температурною сигналізацією, можуть визначати абсолютні значення температур. Серед іншого їх можна застосовувати для моніторингу виробничих процесів або як сигнальний пристрій при виникненні пожежі або для контролю роботи холодильників у супермаркетах.

Компанія Axis пропонує тепловізори обох типів: серія тепловізорів AXIS Q19, які оптимальні для виявлення об'єктів при забезпеченні безпеки, і серія камер з температурною сигналізацією AXIS Q29, здатних визначати абсолютні значення температур.

І тепловізори, і камери Axis з температурною сигналізацією забезпечують ті ж можливості, що й інші мережні камери Axis, а саме: засобу відеоаналітики, розроблена в компанії Axis технологія Zipstream, Power over Ethernet (PoE), передача звуку й стандартизовані способи стиску відео.

Убудовані інтелектуальні функції камери, доповнені засобами аналізу зображень, дозволяють створити рішення, у якому система відеоспостереження автоматично виконує аналіз знятого відеоматеріалу. Мережні тепловізори поширюють результати такого аналізу на інші камери в IP-системі, що підвищує ефективність і масштабованість застосовуваного рішення.

У підсумку, мережні тепловізори дають упевненість у надійному виявленні й реєстрації об'єктів, людей і інцидентів сім днів у тиждень у цілодобовому режимі. У сполученні із засобами аналізу зображень тепловізори допомагають знизити кількість фіктивних тривог і зменшити витрати на створення системи за рахунок того, що для охорони тої ж території потрібно менше камер.

Користувальницькі сценарії

Здатність тепловізорів виявляти людей, автомобілі й тварин можна також використовувати при проведенні пошуково-рятувальних операцій, коли, наприклад, у портовій акваторії потрібно знайти людей, що впали у воду, або допомогти пожежникам побачити щось крізь дим, або сприяти поліції в переслідуванні злочинців. Широкий набір різних об'єктивів дозволяє використовувати тепловізори де завгодно – від відеоспостереження на більших парковочних територіях до охорони по периметрі довгих огорож.

Тепловізори як невидима огорожа для захисту периметра

Мережні тепловізори є ефективним засобом захисту периметра. Завдяки їм часто вдається створити економічне рішення, у якому відеоспостереження на більших відстанях забезпечують усього кілька камер, здатних виявляти людей на фоновому зображенні. Якщо людина перетинає огорожу, то менеджер служби безпеки одержує зображення для перевірки на свій інтелектуальний пристрій.

За рахунок малої кількості фіктивних тривог тепловізори дозволяють керівникам служби безпеки знизити витрати, оскільки скорочується кількість випадків, що вимагають реагування з боку їхнього персоналу. Тепловізори також можна використовувати для перевірки тривог – наприклад, щоб переконатися, що тривога від детектора руху була дійсно викликана людиною. Знаючи це, співробітники служби безпеки можуть більш ефективно діяти для запобігання дорогих наслідків актів вандалізму або злочинів.

Виявлення людей заради їхньої безпеки

За допомогою тепловізорів можна підвищити безпека перебування в потенційно небезпечних обмежених просторах, наприклад, у тунелях, на переїздах і залізничних коліях, що допомагає запобігти нещасним випадкам.

Як і будь-яка інша камера, тепловізор або камера з тепловою сигналізацією збирає електромагнітне випромінювання, що формує зображення. Але звичайна камера працює в діапазоні видимого світла, тобто випромінювання з довжинами хвиль приблизно від 400 до 700 нанометрів (0,4-0,7 мкм), а тепловізор призначений для реєстрації випромінювань, у яких довжина хвилі більше, ніж у видимого світла. Тепловізори в основному працюють або в

діапазоні середніх довжин хвиль ІЧ-випромінювання (MWIR), тобто приблизно 3-5 мкм, або в діапазоні довгохвильового ІЧ-випромінювання (LWIR), що охоплює область 8-14 мкм.

Найбільша відмінність випромінювань у діапазонах MWIR і LWIR від більше короткохвильового випромінювання полягає в тому, що MWIR- і LWIR-випромінювання в основному є що випускається, а не відбиваним. Тепловізори можуть реєструвати випромінювання, що випускається. Можливість побудови теплових зображень заснована на тому, що всі об'єкти – як органічні, так і неорганічні – випускають інфрачервоне випромінювання, характеристики якого залежать від температури об'єкта. Оскільки випромінювання йде від самого об'єкта, те видиме світло не впливає на роботу тепловізора, а виходить, він може функціонувати при будь-якому освітленні – як удень, так і вночі.

Існують два основних типи датчиків, якими оснащуються тепловізори: більше зроблені охолоджувані датчики (застосовувані в основному для військових і наукових цілей) і менш дорогі неохолоджувані датчики. Тепловізори Axis ставляться до неохолоджуваних пристроїв, у яких застосована так звана технологія виробництва мікроболометрів, призначена для використання в LWIR-діапазоні.

Здатність випромінювати поглинену енергію називається випромінювальною здатністю (e). Всі матеріали в тім або іншому ступені мають випромінювальну здатність, значення якої лежить у діапазоні від 0 до 1. Людська шкіра поглинає все падаюче на неї випромінювання й має значення e, приблизно рівне 1 (~ 0,97), у той час як матеріали з більше сильною здатністю, що відбиває, будуть мати менші значення e.

Теплове випромінювання об'єкта також залежить від його температури – чим гаряче об'єкт, тим інтенсивніше він випускає термічне випромінювання. Людина не бачить це випромінювання, але почуває його, наприклад, підходячи до багаття або входячи в сауну. Чим більше різниця температур, тим вище контраст одержуваного зображення й тем краще видний об'єкт.

Теплові зображення іноді асоціюються з яскравими, насиченими квітами, що може здатися трохи дивним, якщо врахувати, що камера працює за межами спектра видимого світла. Це пояснюється тим, що кольори створюються в результаті цифрової обробки й вибираються з так званих псевдокольорів або колірних палітр. Кожний колір або відтінок палітри відповідає певній температурі; при цьому білий і червоний кольори позначають, як правило, більше високі температури, а зелений, синій і фіолетовий – більше низькі. Причина використання колірних позначень є чисто практичної, оскільки людське око краще сприймає різні колірні відтінки, чим різні відтінки сірого.

Тепловізори не тільки добре працюють у темряві, але є незамінним засобом для виявлення людей і об'єктів при цілодобовому відеоспостереженні в будь-яких умовах, навіть якщо людина одягнена в костюм, що маскує. По можливостях виявлення об'єктів тепловізори набагато перевершують звичайні камери в різних непростих погодних умовах – наприклад, коли йде сніг або під час туману.

Варто мати на увазі, що на теплові датчики поширюються експортні обмеження, тому необхідно заздалегідь проконсультуватися в місцевих органах контролю за експортом, щоб не було порушень чинного законодавства.

Висновок. У статті розглянуто та проаналізовано програмне забезпечення, яке призначено для системи забезпечення безпеки побудованої на основі рішень Axis. В межах України в недостатній мірі представлені вітчизняні розробки в цій області. У роботі наведені теоретичне узагальнення й рішення наукового завдання дослідження методів забезпечення безпеки побудованої на основі рішень Axis. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем забезпечення безпеки побудованої на основі рішень Axis; Досліджена система забезпечення безпеки побудованої на основі рішень Axis; На основі отриманих результатів досліджень створена програмна реалізація системи забезпечення безпеки побудованої на основі рішень Axis. Розроблені під час виконання роботи алгоритми дозволяють успішно вирішувати завдання забезпечення безпеки побудованої на основі рішень Axis. Проведено аналіз предметної галузі в ході якого

були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки. Розроблене програмне забезпечення має простий, дружній та зручний інтерфейс користувача, що забезпечує легкість у освоєнні роботи програмного продукту, зручність у використанні, і не потребує особливих спеціальних знань. При створені програмного забезпечення було використано об'єктно-орієнтований підхід, що відповідає сучасним тенденціям у галузі розробки комерційних програмних систем. Програма реалізована на мові високого рівня Delphi 10.2 Tokyo. Дана мова програмування дозволяє найбільш ефективно обробляти дані. Це дозволило мінімізувати строк розробки програмного забезпечення, і, як слід, зменшити витрати на його розробку. Запропоноване програмне забезпечення ділиться на загальне програмне забезпечення, що поставляється із засобами обчислювальної техніки й спеціальне програмне забезпечення, що спеціально розроблене для даної конкретної системи й включає програми, що реалізують її функції. Даються необхідні рекомендації з установки розробленого програмного забезпечення. Для підвищення рівня безпеки запропоновано застосовувати алгоритм DSA.

Список літератури

1. Дреев А.Н. Использование неравномерного распределения единичных битов для дополнительного сжатия SPIHT кода / А.Н. Дреев, А.А. Смирнов // Информационные системы в управлении, образовании, промышленности: монография. Под редакцией профессора В.С. Пономаренко. – Х.: Вид-во ТОВ «Щедра садиба плюс», 2014. – С. 498.
2. Дрєєв О.М. Дослідження впливу шляху розгортки на ступінь ентропійного стиснення цифрового зображення / О.М. Дрєєв, О.В. Слюсар // Збірник наукових праць Кіровоградського національного технічного університету. Техніка в сільськогосподарському виробництві, галузеве машинобудування, автоматизація. Випуск 21. – Кіровоград: КНТУ. – 2008 – С. 115-118.
3. Дрєєв О.М. Метод розвантаження телекомунікаційного сервера за рахунок кешування зображень / О.М. Дрєєв // Збірник наукових праць Кіровоградського національного технічного університету. Техніка в сільськогосподарському виробництві, галузеве машинобудування, автоматизація. Випуск 25. Ч. І. – Кіровоград: КНТУ. – 2012 – С. 419-424.
4. Дрєєв О.М. Метод прогнозування завантаженості серверу телекомунікаційної мережі / О.М. Дрєєв, О.А. Смірнов, Є.В. Мелешко, О.В. Коваленко // Системи обробки інформації. Випуск 3(101) Том 2. – Х.: ХУПС. – 2012. – С. 181-188.
5. Дрєєв О.М. Оцінка якості стиснення зображень на основі дискретного перетворення Хартлі / О.В. Коваленко, О.П. Доренський, О.М. Дрєєв // Системи озброєння і військова техніка. Науковий журнал 2(34) – Х.: ХУПС – 2013. С. 99-102.
6. Дрєєв О.М. Дослідження впливу ступеня стиснення зображень на оперативність їх доставки у телекомунікаційній системі / О.А. Смірнов, О.М. Дрєєв, О.П. Доренський // Збірник наукових праць "Системи обробки інформації". – Випуск 8(115). – Х.: ХУПС – 2013. – С. 234-239.
7. Дреев А.Н. Сравнение битовых плотностей при использовании различных методов кодирования информации / А.Н. Дреев, А.А. Смирнов // Системи обробки інформації, 2014, випуск 2 (118), том 2 – Харків: ХУПС – 2014. С 64-66.
8. Дрєєв О.М. Моделювання впливу інтенсивності трафіку на оперативність доставляння інформації / О.М. Дрєєв // Науково-виробничій журнал "Зв'язок". – Київ: ДУТ, 2014. – № 2 (108) С. 24-29.
9. Дреев А.Н. Повышение вероятности доставки сообщений в телекоммуникационных системах и сетях для обеспечения информационной безопасности / А.Н. Дреев, А.А. Смирнов //«Безпека інформації» Том 21, №1 2015 р. – Київ: НАУ – 2015. – С. 22-28.
10. Дрєєв О.М. Узагальнення вейвлету Хаара / О.М. Дрєєв, Г.М. Дрєєва // Збірник тез доповідей Комбінаторні конфігурації та їх застосування, 15-16 жовтня 2010 р. – Кіровоград – С. 58

УДК 004

В. Гаморя, магістр гр. КІ-18М-1,4
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ ПРОМИСЛОВОГО ІНТЕРНЕТУ РЕЧЕЙ

У статті розроблено програмне забезпечення, яке призначено для системи промислового інтернету речей. Метою розробки є дослідження та програмна реалізація системи промислового інтернету речей. Об'єктом дослідження є процес промислового інтернету речей. Предметом дослідження є методи промислового інтернету речей. Методи дослідження базуються на методах теорії промислового інтернету речей, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи промислового інтернету речей. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

комп'ютерна інженерія, промисловий інтернет речей

Постановка проблеми. Експерти по-різному оцінюють поточний стан Промислового Інтернету речей (IoT) в Україні. Для великих вітчизняних промислових підприємств IoT – це поки екзотика.

Насправді по зрілості цифрових бізнес-моделей і рівню їхньої реалізації промисловість і енергетика навіть у розвинених країнах перебувають далеко не на першому місці. До лідерів у частині цифрової трансформації відносяться медіакомпанії й торговельні підприємства. Далі випливають транспорт і охорона здоров'я. Більше складні процеси й більша база успадкованого встаткування істотно утрудняють впровадження нових моделей і технологій на промислових і енергетичних підприємствах. Проте необхідність цифрової трансформації підприємств уже назріла. Традиційні технології вичерпали потенціал росту й підійшли до межі ефективності. Ключове питання для нашої промисловості полягає в тім, чи готова вона до нового бізнес-моделям, які стають можливими завдяки таким технологіям, як IoT, предиктивне й подійне керування.

Починаючи з 2000 року 52% компаній зі списку Fortune Global 500 уже випробували на собі руйнівний вплив цифрових технологій. Не встигши вчасно зорієнтуватися й впровадити нові технології, ці компанії втратили свої позиції на ринку. Згідно із прогнозом, по тимі ж причинам 50% лідерів ринку поступляться свої провідні позиції в найближчі 10 років.

Від візіонерства в області IoT і інтелектуального виробництва треба більш сміливо переходити до реальних проектів. Він уважає, що всі потрібні для цього технології або вже доступні, або з'являться протягом найближчих декількох років. Інструментів багато, а використовуються вони мало.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-58] було виявлено певні прогалини у забезпеченні системи промислового інтернету речей.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи промислового інтернету речей.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

- Огляд існуючих систем промислового інтернету речей.
- Дослідження системи промислового інтернету речей.
- Програмна реалізація системи промислового інтернету речей.

Об'єктом дослідження є процес промислового інтернету речей.

Предметом дослідження є методи промислового інтернету речей.

Методи дослідження базуються на методах теорії промислового інтернету речей, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Багато технологій для надійної й ефективної взаємодії промислових «речей» уже існують.

Швидко ставши надзвичайно популярним, термін «Інтернет речей» (Internet of Things, IoT) породив різні «похідні». Найчастіше вони пропонуються замість термінів, що існували багато років, щоправда, при цьому описувані ними рішення й процеси наповнюються новими змістом і можливостями. Так, замість ІБ (інтелектуальний будинок) всі частіше зустрічається абревіатура BIoT (Building Internet of Things) – «Інтернет речей у будинку». А замість АСУ ТП (автоматизована система керування технологічним процесом) деякі « філологи-технократи» пропонують термін IoT (Industrial Internet of Things). На українську мову його можна перевести як «Промисловий Інтернет речей» або просто «Промисловий Інтернет».

Загальноприйняте визначення, що ж таке Промисловий Інтернет речей, поки не сформувалося. У цьому контексті слід зазначити дві ініціативи, які багато в чому визначають два підходи: європейськ і американський (сподіваюся, незабаром буде вироблений і наш, український).

Європейський підхід базується на народженій у Німеччині концепції «Індустрія 4.0» (Industry 4.0), хоча в багатьох інших європейських країнах є свої схожі програми з іншими назвами. Згідно Industry 4.0, ми, точніше європейська економіка, перебуваємо на порозі четвертої промислової революції. Перша революція (80-і роки XVIII століття) була пов'язана з механізацією виробництва завдяки винаходу парових двигунів. З початком масового застосування електроенергії на заводах наступила друга – індустріалізація (початок XX століття). Застосування електроніки для автоматизації виробництва привело до третьої промислової революції – по суті, вона викликана впровадженням систем АСУ ТП (50-е роки XX століття). Властиво четверта революція – «розумні» підприємства – насправді є продовженням третьої. Її знакові моменти – впровадження кіберфізичних систем і перехід до персоналізованого виробництва.

Кіберфізична система

Є безліч докладних визначень кіберфізичних систем, але саме істотне в них – це наявність двостороннього зв'язку між фізичними процесами й керуючими програмами (обчислювальними засобами). Елементи такої системи можуть перебувати як поруч, наприклад в одній виробничій зоні, так і далеко друг від друга, а взаємодія між ними – здійснюватися на всіх стадіях «життєвого циклу» (планування, виробництво, експлуатація, ремонт, утилізація). Збір і аналіз інформації, що збирається, можуть служити безлічі цілей: діагностика стану, прогнозування необхідності тих або інших змін, автоматичне настроювання, адаптація та ін.

Класичний приклад кіберфізичної системи – інфраструктура Smart Grid, у якій дані, що збираються з різних вузлів електромережі, використовуються програмними засобами керування для коректування роботи цих вузлів з метою підвищення надійності й ефективності.

Інший приклад – підключений автомобіль, стан різних елементів якого постійно контролюється як локально, самою системою керування, так і віддалено, наприклад із сервісного центра. Різні події, скажемо стирання гальмової колодки, приведуть як до зміни настроювань системи гальмування, так і до формування замовлення на випуск нових колодок для заміни. Нові запчастини надійдуть на сервіс, і одночасно власник буде проінформований про необхідність заміни.

За океаном теж замислюються про майбутнє промислового виробництва. В 2014 році компанії General Electric, AT&T, Cisco, IBM і Intel створили Консорціум Промислового Інтернету (Industrial Internet Consortium, IIC), що сьогодні нараховує вже 170 членів. З погляду членів цього консорціуму, Промисловий Інтернет виходить далеко за рамки виробничих підприємств. Як приклади реалізації цієї концепції на офіційному сайті IIC

приводяться безпілотні автомобілі, здатні безпечно переміщатися до крапки призначення без водіїв; системи вилученого збору різних медичних показників, що дозволяють контролювати стан пацієнтів лікарем дистанційно; обладнані «розумними» датчиками системи водопостачання, керування паркуваннями й інші системи інтелектуального міста. Таким чином, якщо концепція Industry 4.0 фокусується на виробничій сфері, то в сфері інтересів Консорціуму Промислового Інтернету – не тільки властиво виробництво, але й медицина, транспорт, сільське господарство, комунальні послуги та ін.

У цьому розділі ми сконцентруємося на обговоренні інфраструктурної проблематики Промислового Інтернету речей у його європейському розумінні – тобто на виробничій сфері.

«Речі» у промисловості

У промисловому IoT основними різновидами «речей», які треба підключати до мережі, є різні типи датчиків (сенсорів) і приводів. Ці пристрої з однієї сторони мають інтерфейс із комунікаційною мережею, а з іншого боку – інтерфейс, що забезпечує фізичну взаємодію із процесом, що потрібно відслідковувати. Завдання датчиків і сенсорів – збір інформації. Вони можуть фіксувати різні фізичні характеристики (температуру й вологість, тиск і різні зусилля, напругу й силу струму, витрата газу й рівень рідини), присутність різних речовин (хімічні й біосенсори), а також фізичні події (наприклад, зміна й переміщення об'єктів). Сенсори всі частіше інтегруються безпосередньо в мікросхеми.

Крім сенсорів, у мікросхеми можуть вбудовуватися й приводи, призначення яких – контроль за фізичними об'єктами й керування ними. Такі інтегровані рішення називають мікроелектромеханічними системами (МЕМС). Прикладами подібних пристроїв, що поєднують у собі мікроелектронні й мікромеханічні компоненти, є акселерометри й гіроскопи. Класичні ж приклади приводів – це мотори, що переміщають різні об'єкти; клапани, що відкривають і закривають канали надходження рідини або газу; електричні перемикачі. Приводи звичайно мають механічний, гідравлічний, пневматичний або електричний компонент для виконання необхідних функцій, а також електронний блок керування.

Комунікаційний інтерфейс – зовсім необхідний компонент пристрою IoT. Це може бути провідний або бездротової інтерфейс. Основним кандидатом на універсальну технологію проводовий зв'язка є Ethernet. У випадку бездротового підключення це може бути Wi-Fi, а також безліч інших технологій. Але, незалежно від того, яка технологія використовується на канальному й фізичному рівнях, пристрій повинне безпосередньо підтримувати протокол IP, щоб інтегруватися в інфраструктуру IoT. Крім того, найважливішою умовою використання пристрою IoT є наявність засобів безпеки. IP – це відкритий протокол, тому такі засоби повинні бути інтегровані в пристрій споконвічно.

Із проводами або без

Традиційно в промислових мережах переважна більшість підключень були провідними. Однак останнім часом бездротові технології використовуються усе ширше. Частіше їх застосовують для некритичних додатків, таких як конфігурування й моніторинг, передача додаткових даних, підтримка додатків мобільних співробітників.

Однієї з важкорозв'язних проблем застосування радіотехнологій є поділюване середовище передачі (використання загального частотного діапазону), що може привести до неможливості передачі даних, якщо всі частотні канали виявляться зайнятими. Крім того, радіозв'язок піддається негативному впливу електромагнітних перешкод, які у виробничих цехах можуть бути досить істотними. Випадкова втрата пакетів також досить типова для багатьох радіосистем. Якщо для офісних мереж це прийнятно, то для критично важливих промислових рішень потрібна передача даних без втрат.

Одним з напрямків удосконалювання радіотехнологій з метою їхнього застосування на виробництві є розробка ефективних технологій захисту від статичної електрики. Використання бездротової мережі з ніздрюватою топологією дозволяє знизити затримку й час реконфігурації мережі, а алгоритмів паралельної передачі – виключити втрати пакетів. У

мережах «розумних» фабрик майбутнього бездротові технології будуть використовуватися досить широко, хоча основу, як і раніше, складуть провідні рішення.

За межами локальної мережі

Мережі Промислового Інтернету речей по визначенню не можуть бути обмежені периметром того або іншого підприємства. Важливе значення мають взаємодія зі зробленим продуктом («річчю») на етапі його експлуатації, а також доступ до хмарних сервісів, які можуть бути реалізовані в ЦОДах, розкиданих по усьому світі. Тому територіально розподілена інфраструктура – ключова характеристика Промислового Інтернету.

Якщо говорити про бездротові технології, на даний момент для підключення речей до Інтернету найбільше активно використовуються мережі стільникового зв'язка. Причому розвиток останніх у рамках організації 3GPP іде саме в напрямку адаптації до потреб IoT. У рамках розробки систем покоління 5G зміна структури кадру дозволить на порядок скоротити затримку (у порівнянні із системами LTE) – до 1 мс. Крім того, спеціальні рішення розробляються для низькошвидкістного підключення великої кількості пристроїв при збільшеній зоні покриття.

Але, оскільки наявні технології стільникового зв'язка створювалися для обслуговування людей, а не речей, вони погано адаптовані для IoT (висока вартість, проблеми з покриттям та ін.). Тому активно розвиваються й альтернативні бездротові технології, у тому числі для розподілених мереж з низьким енергоспоживанням (Low-power Wide-area Network, LPWAN), які будуть працювати на частотах загального користування.

Одна з технологій для LPWAN розроблена французькою компанією Sigfox, причому відповідна мережа вже розгорнута по всій Франції – для чого, як затверджується, вистачило 1200 базових станцій. На відміну від мереж GSM, рішення на базі технології Sigfox дешевше, споживають набагато менше електроенергії й працюють на великих відстанях.

Інший приклад перспективної технології для побудови мереж LPWAN – LoRa, що просувається організацією LoRa Alliance. Радіус покриття базової станції LoRaWAN може досягати 90 км.

Розробка структурної схеми

Еволюція АСУ ТП

Як улаштовані сучасні системи промислової автоматизації? Їх можна розділити на кілька рівнів. Безпосередньо «у поле», наприклад у цеху підприємства, розташовуються різні сенсори, датчики й приводи. Далі треба рівень контролю – наприклад, програмувальні логічні контролери (ПЛК; англ. PLC), які, властиво, збирають інформацію з датчиків і управляють приводами. Рівень керування процесами формують системи класу SCADA (Supervisory Control And Data Acquisition) і MES (Manufacturing Execution System). Нарешті, на вершині піраміди – системи планування ресурсів підприємства (Enterprise Resource Planning, ERP), які, як правило, працюють на серверах, розташованих у корпоративних центрах обробки даних (ЦОДи).

Що зміниться в цій структурі з реалізацією концепції Industry 4.0? Нижній рівень (з датчиками, приводами й іншими виконавчими механізмами) збережеться, однак число пристроїв на цьому рівні експоненційно виросте. Крім того, що навіть більш важливо, пристрою цього рівня будуть наділятися все більшим інтелектом. Вони стануть частиною кіберфізичних систем і будуть здатні автономно виконувати багато функцій. Більшість же функцій, які в сьогоднішніх системах реалізуються пристроями вищестоящих рівнів, будуть переноситися на високопродуктивні сервери, які будуть розташовуватися в серверних кластерах, ЦОДах або хмарах.

Технології віртуалізації – поділ реалізованих програмним способом конкретних функцій і встаткування, на якому вони виконуються, – уже стали реальністю у світі IT, проникнуть і в системи промислової автоматизації. Переваги нової структури в тім, що загальна кількість керуючих систем скоротиться, що спростить сам процес керування. Крім того, ефективність використання ресурсів підвищиться, а засобів буде потрібно менше.

Масова реалізація описаного вище підходу в системах промислової автоматизації поки ще гальмується рядом невирішених проблем. Більша їхня частина зв'язана саме з мережною інфраструктурою: низькою продуктивністю передачі даних, недостатньою надійністю, непередбаченими затримками між пристроями польового рівня й обслуговуючих їхніх серверів. Однак на рішення цих проблем кинуті кращі сили багатьох виробників, що вселяє оптимізм.

Інфраструктура для IOT

Як уже говорилося, кількість підключених пристроїв на «розумних» фабриках майбутнього стане значно більше, ніж на сучасних виробництвах. Обсяги даних, що збираються, також кардинально збільшаться. Тому необхідні технічні рішення, здатні забезпечити підключення великої кількості різних пристроїв просто й ефективно, при виконанні вимог до продуктивності, безпеці й надійності. На думку більшості експертів, що домінують у минулому пропрієтарні шини поступляться місцем універсальним мережам Ethernet. Для безшовного зв'язку як між елементами в рамках одного підприємства, так і з об'єктами «зовнішнього миру» будуть використовуватися стандартні Інтернет-протоколи, тому й говорять про Промисловий Інтернет.

Адаптація традиційних мережних рішень до вимог Промислового Інтернету йде по декількох напрямках. Одна з тенденцій – спрощення кабельної системи. Типові системи Gigabit Ethernet задіють всі чотири пари провідників мідножильної СКС. Однак уже розроблений стандарт Ethernet (1000 Base-T1) для передачі гігабітного трафіку по однієї кручений парі – правда, з деякими обмеженнями по відстані. Системи Fast Ethernet також можуть працювати по одній парі (100 Base-T1), причому при стандартній дальності.

Інший важливий момент, що не залежить від того, використовується провідний або бездротовий зв'язок, – це зниження розмірів пристроїв і скорочення енергоспоживання. Прогрес в області напівпровідникової техніки дозволяє робити усе більше компактні структури, забезпечувати більш високий ступінь інтеграції й скорочувати енергоспоживання. Так, системи Wi-Fi з низьким споживанням можуть використовуватися для підключення невеликих датчиків, що одержують живлення від убудованих акумуляторних батарей. Радіотехнологій з низьким енергоспоживанням багато, але використання Wi-Fi дозволяє побудувати однорідну мережну інфраструктуру, у якій кадри Ethernet і протокол IP будуть застосовуватися «від краю до краю».

Для багатьох застосувань у промисловості необхідна гарантована затримка при передачі даних. Причому такі гарантії можуть знадобитися не тільки при зв'язку об'єктів у межах виробничої зони або підприємства, але й при взаємодії з об'єктами поза підприємством. У цей час існує ряд протоколів реального часу, які здатні забезпечити тверді гарантії по затримці в мережі Ethernet. Але жоден із цих протоколів не є стандартом Ethernet.

Для роботи в режимі реального часу можуть використовуватися різні технології – наприклад, протокол Precision Time Protocol (PTP), що забезпечує синхронізацію годин, убудованих у мережні пристрої. Цей протокол уже активно застосовується в багатьох мережах. Організація IEEE постійно працює над удосконалюванням PTP, в 2016 році повинен бути прийнятий стандарт уже на третю версію цього протоколу. Досягненню стабільної низької затримки сприяють також підвищення пропускної здатності каналів зв'язку й застосування алгоритмів пріоритезації трафіку усередині комутаторів. Очевидно, що чим більше широка смуга пропущення доступна, тим нижче ймовірність того, що комутатор блокує той або інший пакет.

За стандарт на Ethernet реального часу в рамках комітету IEEE 802.1 відповідає група Time Sensitive Networking (TSN). Її завдання – стандартизація детермінованого варіанта Ethernet, настільки необхідного для багатьох промислових застосувань. Коротенько технічний концепт TSN можна викласти в такий спосіб:

– Протокол резервування пропускної здатності відповідає за виділення необхідних ресурсів у мережі.

– Формувачі ресурсів Time-Aware Shaper усередині комутаторів використовують визначені тимчасові слоти для контролю потоку пакетів, якому необхідно передавати в реальному часі.

– Технологія превентивного витиснення (Frame Preemption) низькопріоритетних потоків забезпечує гарантовану передачу пакетів з високим пріоритетом без затримок.

Робота над першими стандартами TSN повинна бути завершена в 2018році.

Зі збільшенням числа підключених до мережі пристроїв і підвищенням значимості її безперебійної роботи кардинально міняються вимоги до її адміністрування й експлуатації. Дотепер величезний обсяг пов'язаних з мережами робіт виконується вручну. Проектування мережі, інсталяція встаткування, його конфігурування, тестування, моніторинг роботи, технічне обслуговування, пошук і усунення несправностей – все це вимагає величезних людських і фінансових ресурсів. У майбутніх мережах IoT частка ручної праці повинна істотно скоротитися. Це необхідно, зокрема, тому, що при збільшенні числа підключених пристроїв у сотні й тисячі разів стане фізично неможливо, наприклад, налаштовувати кожний окремий пристрій.

Засоби автоматичного конфігурування мережного встаткування, керування мережею та ін. активно розвиваються. Вони не тільки заощаджують час і ресурси, але й дозволяють істотно знизити ймовірність помилок, пов'язаних з людським фактором. Однак роботи тут ще непочатий край.

Обмежений обсяг статті не дозволяє докладно розглянути всі аспекти, пов'язані з розвитком технологій для інфраструктури Промислового Інтернету. Відзначу, що ключове значення мають питання забезпечення безпеки таких рішень. Відказостійкість мереж – також надзвичайно важливий аспект. Жорсткі умови експлуатації підвищують імовірність ушкодження тих або інших елементів мережних структур, при цьому наслідку простою промислової мережі можуть мати величезний негативний ефект. У деяких випадках такий простій взагалі неприпустимий, тому що може привести до катастроф і масової загибелі людей. На даний момент існує чимало механізмів, що забезпечують гаряче резервування мережних елементів і гарантуюче продовження роботи навіть у випадку ушкодження частини вузлів і каналів зв'язку. Такі механізми активно розвиваються й повинні обов'язково використовуватися в промислових мережах.

На якій стадії свого розвитку сьогодні перебуває Промисловий Інтернет речей? Безумовно, він уже існує тією чи іншою мірою – у вигляді систем автоматизації виробництва. На багатьох підприємствах безліч пристроїв підключені до мереж промислових зон, взаємодія між речами здійснюється й на далеких відстанях. Але цей тільки початок. Як уже говорилося, зі збільшенням кількості підключених пристроїв, реалізацією кіберфізичних систем Промисловий Інтернет речей вийде на новий рівень

Що стосується інфраструктурних рішень, багато технологій для надійної й ефективної взаємодії промислових «речей» також уже існують. Однак чимало й пробілів, які необхідно заповнити. Наскільки швидко й продуктивно будуть вирішені цей завдання, багато в чому залежить від фінансових засобів, які будуть спрямовані на ці мети. А обсяги фінансування, у свою чергу, будуть визначатися тими економічними перевагами, які дасть широкомасштабне розгортання Промислового Інтернету.

Ключові технології

Технології ідентифікації й відстеження

Технології ідентифікації й відстеження, застосовувані в IoT, включають системи RFID, штрихкоди й інтелектуальні датчики. Проста RFID-система складається з RFID-зчитувача й RFID-мітки. Завдяки здатності цієї системи до виявлення й відстеження пристроїв і фізичних об'єктів вона всі частіше використовується в промислових галузях, таких як логістика, керування ланцюгами поставок, служба моніторингу здоров'я [2, 15]. Інша перевага системи RFID полягає в надані точної інформації в режимі реального часу про підключені пристрої, що дозволяє скоротити витрати на робочу силу, спростити бізнес-

процеси, підвищити точність інформації про встаткування й у підсумку поліпшити загальну економічну ефективність.

На даний момент розвиток технологій RFID фокусується на наступних аспектах [2, 3, 4, 15]:

1) активні RFID-системи з розширеним спектром передачі;

2) технологія керування RFID-додатками [3, 4].

Також існує багато можливостей для розвитку RFID-додатків [16]. Наприклад, RFID-технологія може бути інтегрована з WSN для кращого виявлення «речей» і спостереження за ними в режимі реального часу. сенсорні технології, Що Розвиваються бездротові інтелектуальні, такі як електромагнітні датчики, біосенсори, убудовані датчики, датчики тегів, незалежні теги й сенсорні пристрої, надалі посприяють впровадженню й розгортанню виробничих служб і додатків. За допомогою інтеграції даних, отриманих інтелектуальними датчиками за допомогою RFID, можуть бути створені могутніші додатки IoT, які підходять для індустріального середовища.

Комунікаційні технології в IoT

Реалізація «Інтернету речей» може містити безліч електронних апаратів, мобільних пристроїв і промислового встаткування. Різним «речам», які можна підключити до мережних і комунікаційних технологій, відповідають різні способи комунікації, з'єднання по мережі, обробки й зберігання даних, а також пропущення електроенергії. Наприклад, багато хто смартфони вже зараз мають якісний зв'язок, багатими мережними можливостями й способами обробки й зберігання даних, а в моніторах серцевого ритму спостерігаються лише обмежені можливості комунікації й обчислень.

«Інтернет речей» містить у собі ряд гетерогенних мереж, таких як WSN, бездротові ніздрюваті мережі, WLAN і т.п. Вони допомагають «речам» в IoT обмінюватися інформацією. Мережний шлюз у стані полегшити комунікацію або взаємодію різних пристроїв за допомогою Інтернету, а також може використовувати свою «мережу знань» для локального виконання алгоритмів оптимізації, що дозволяє застосовувати його при обробці безлічі складних аспектів комунікації в мережі [16].

В «речей» можуть бути різні вимоги до якості сервісу (QoS-вимоги, англ. quality of service – якість обслуговування, якість сервісу) по продуктивності, енергоефективності й безпеки. Приміром, багатьом пристроям для роботи потрібні акумулятори, і тому зниження енергоспоживання є для них однією з головних проблем. Навпроти, для пристроїв з постійним живленням поліпшення енергозбереження найчастіше не є першочерговим завданням. IoT також значно виграє від використання існуючих протоколів Інтернету, таких як IPv6, оскільки це дозволить прямо звертатися до будь-якого числа необхідних «речей» через Інтернет [1, 7, 8]. Основні комунікаційні протоколи й стандарти містять у собі радіочастотну ідентифікацію RFID (наприклад, ISO 18000 6c EPC Class 1 Gen 2), NFC, IEEE 802.11 (WLAN), IEEE 802.15.4 (ZigBee), IEEE 802.15.1 (Bluetooth), мультихоп-бездротові датчики й ніздрюваті мережі, малопотужні бездротові персональні просторові мережі IETF (6LoWPAN), межмашині з'єднання (M2M), а також традиційні IP-технології (IP, IPv6 і т.д.).

Мережі для IoT

Для бездротових мереж існує досить багато шарів пересічних протоколів, наприклад бездротові датчики й приводні мережі (WSAN) або ad-hoc-мережі (AHNs) [13]. Однак вони повинні бути перероблені, перш ніж підійдуть для застосування в «Інтернеті речей». Причина в тім, що «речі» в IoT часто мають досить різноманітні можливості комунікацій і обчислень, а також різними вимогами до якості сервісу (QoS). Вузли в WSN, як правило, мають схожі вимоги до встаткування й мереж зв'язку. Крім того, у мережі IoT для підтримки обміну інформацією використовується Інтернет, але на відміну від WSN і AHN Інтернет не потрібно «включати», щоб забезпечити з'єднання.

Керування сервісами в IoT

Керування сервісами в «Інтернеті речей» пов'язане з їхньою реалізацією і якістю, які відповідають потребам користувачів і додатків. Сервіс-орієнтовану архітектуру (англ.

Service-oriented Architecture, SOA) можна використовувати для інкапсуляції послуг, приховуючи деталі їхньої реалізації, наприклад використовувані протоколи [17]. Це дає можливість розділити компоненти в системі й, отже, сховати гетерогенність від кінцевих користувачів. Сервіс-орієнтована архітектура «Інтернету речей» дозволяє додаткам використовувати різнорідні об'єкти, такі як сумісні сервіси [5].

Більше того, динамічний характер додатків «Інтернету речей» жадає від його послідовного надання надійних послуг. Ефективна сервіс-орієнтована архітектура може мінімізувати негативні наслідки, викликані переміщенням пристрою або відмовою батареї. Гарним прикладом є OSGi-платформа (Open Services Gateway Initiative – специфікація динамічної модульної системи й сервісної платформи для Java-додатків) [18], що застосовує динамічну сервіс-орієнтовану архітектуру (dynamic SOA architecture) для розгортання інтелектуальних сервісів. Із цією метою OSGi використовується в різних контекстах – наприклад, для мобільних додатків, плагінів, серверів додатків і т.д. В «Інтернеті речей» композиція сервісів на базі OSGi-платформи може бути реалізована за допомогою Apache Felix iPoJo [19].

Сервіс являє собою збір даних, а також режими, які необхідні, щоб виконати певну функцію, обслужити пристрій або його частини. Сервіс може надаватися різними способами: так, він може посилатися на інші первинні або вторинні сервіси й/або на набір характеристик сервісу. Сервіси можна розділити на два типи: первинні й вторинні. Перші виконують первинні функції у вузлі IoT, і їх можна розглядати як основні компоненти сервісу, які можуть бути включені в інший сервіс. Другі можуть надавати допоміжні функції для основного сервісу або інші додаткові послуги. Сервіс може володіти одним або декількома ознаками, які визначають структури даних, дозволу, дескриптори та інші атрибути сервісів [11, 13]. У сервіс-орієнтованом IoT сервіси можуть бути створені й розгорнуті поетапно [1, 7, 8]: 1) розвиток структурної платформи сервісів; 2) підсумовування функціональних і комунікаційних можливостей пристроїв; 3) надання єдиного комплексу сервісів. Сервіс керування ідентифікаційною інформацією містить у собі управлінський контекст і класифікацію об'єктів. «Інтернет речей» також дозволяє створити дзеркало для кожного реального об'єкта в IoT. Крім того, IoT має сервіс-орієнтовану й зв'язану архітектуру, у якій віртуальні й фізичні об'єкти можуть взаємодіяти між собою. Сервіс-орієнтований IoT дозволяє кожному з компонентів пропонувати свої функціональні характеристики як стандартні сервіси, що значно підвищує ефективність як всіх пристроїв, так і мереж, що беруть участь в «Інтернеті речей».

Ключові додатки IoT у промисловості

IoT-додатка поки перебувають на відносно ранній стадії розвитку [7, 8, 11]. Однак «Інтернет речей» використовується всі частіше. Досить багато додатків для IoT розробляється й/або вже використовується для моніторингу навколишнього середовища, у службах охорони здоров'я, керуванні товарними запасами й продукцією, а також у сферах, пов'язаних із продуктами живлення, транспортом, підтримкою робочих місць і будинків, забезпеченням безпеки й відеоспостереження. У роботах [7] і [8] дається огляд застосування «Інтернету речей» у різних областях. Ми ж у нашім обговоренні фокусуємся саме на промислових додатках IoT, для розробки яких необхідно вирішити кілька завдань. Залежно від передбачуваної області застосування дизайнерам потрібно знайти якийсь компроміс для досягнення балансу між витратами й вигодами [20]. Нижче наведені деякі додатки IoT у промисловості.

Використання IoT у гірському виробництві

Забезпечення безпеки на шахтах є великою проблемою для багатьох країн у зв'язку з умовами праці на підземних рудниках. З метою запобігання й зменшення кількості нещасних випадків необхідно використовувати технології IoT, які зможуть приймати аварійні сигнали із шахти [25]. За допомогою RFID, Wi-Fi і інших технологій і пристроїв бездротового зв'язку, що забезпечують ефективну взаємодію між наземним і підземним просторами, гірничодобувні компанії зможуть відслідковувати місце розташування шахтарів і аналізувати

критично важливі дані по безпеці, отримані від датчиків. Ще одним корисним додатком є хімічні й біологічні сенсори, застосовувані для діагностики й раннього визначення захворювань у шахтарів, що особливо важливо, оскільки вони працюють у небезпечних умовах. Ці сенсори можна використовувати для одержання біологічної інформації про стан людського тіла й органів, для виявлення небезпечного пилу, шкідливих газів і інших факторів навколишнього середовища, які можуть стати причиною нещасних випадків. Проблема використання всіх цих технологій полягає в тім, що бездротовим пристроям потрібна енергія, що потенційно може привести до вибуху газу в шахті. Таким чином, необхідні додаткові дослідження характеристик безпеки IoT-пристроїв, використовуваних у гірничорудній промисловості.

Використання IoT у сфері охорони здоров'я [21]

«Інтернет речей» дає нові можливості для поліпшення охорони здоров'я [12]. При повсюдній підтримці ідентифікації, зондування й комунікаційних можливостей «Інтернету речей» всі об'єкти системи охорони здоров'я (люди, техніка, препарати й т.д.) можна постійно відслідковувати й контролювати [22]. Глобальний зв'язок «Інтернету речей» дозволяє всі медичні відомості (забезпечення, діагностика, терапія, видужання, ліки, керування, фінанси й навіть добова активність) зібрати, обробити й ефективно використовувати. Наприклад, можна вимірювати частоту серцевих скорочень пацієнта за допомогою датчиків, а потім відправляти в кабінет лікаря. При використанні персональних обчислювальних пристроїв (ноутбук, мобільний телефон, планшет і т.д.) і мобільного доступу в Інтернет (Wi-Fi, мережі 3G, LTE і т.д.) медичні служби, що базуються на IoT, стають мобільними й персональними [23]. Широке поширення сервісів мобільного Інтернету прискорює розвиток заснованих на «Інтернеті речей» послуг охорони здоров'я «вдома» [21]. Але поки цьому перешкоджають проблеми, пов'язані з безпекою й конфіденційністю.

Використання IoT у ланцюжках поставок харчових продуктів [24]

Сьогодні ланцюжка поставок харчових продуктів (Food Supply Chains, FSC) широко поширені. Вони мають складні робочі процеси, мають значні географічні й тимчасові масштаби, а також можуть включати велика кількість учасників. Їхня складність викликала багато питань по керуванню якістю, оперативності й суспільній безпеці харчових продуктів. Великий потенціал для рішення проблем відслідковуємості, прозорості й контролю відкрили технології IoT. Вони можуть захистити мережі FSC у так званих ланцюжках «від ферми до тарілки»: від високоточного сільського господарства до виробництва продуктів живлення, їхній обробці, зберіганню, розподілу й споживанню. У майбутньому варто очікувати появи більше безпечних, ефективних і стійких FSC. Типове рішення «Інтернету речей» для FSC (т.зв. харчового IoT) складається із трьох частин:

а) польових пристроїв, таких як вузли бездротової сенсорної мережі (WSN), зчитувачі RFID-міток, термінали користувальницького інтерфейсу й т.д.;

б) магістральної системи, що включає бази даних, сервера й термінали багатьох видів, підключених до розподілених комп'ютерних мереж і т.д.;

в) інфраструктури зв'язку, такий як бездротова локальна мережа (WLAN), стільниковий, супутниковий зв'язок, лінії електропередач, Ethernet і т.д. Крім цього, IoT також надає ефективні функції зондування для відстеження й контролю процесів виробництва продуктів живлення.

Використання IoT в області транспорту й логістики

Роль «Інтернету речей» у транспортній і логістичній галузях промисловості стає усе більше значимої [7]. Оскільки усе більше й більше фізичних об'єктів оснащуються штрихкодами, RFID-позначками або датчиками, транспортні й логістичні компанії можуть відслідковувати в реальному часі рух фізичних об'єктів від вихідного пункту до місця призначення по всьому ланцюжку поставок, спостерігаючи за виробництвом, доставкою, дистриб'юцією і т.д. [26]. Крім того, очікується, що IoT надасть перспективні рішення для перетворення транспортних систем і автомобільних сервісів [27]. Тому що засобу пересування володіють усе могутнішими мережними й комунікативними можливостями, а

також засобами зондування й обробки даних, «Інтернет речей» можна використовувати як для їхнього поліпшення, так і для того, щоб ділитися маловикористовуємими ресурсами з іншими автомобілями на паркуванні або на дорозі.

Наприклад, інтелектуальна інформаційна система (iDrive), недавно розроблена компанією BMW, використовує різні датчики й мітки для моніторингу обстановки, зокрема відстеження місця розташування транспортного засобу й забезпечення схеми проїзду [28]. Група авторів [29] розробила інтелектуальну систему моніторингу для контролю температури й вологості усередині вантажівок-рефрижераторів за допомогою RFID-міток, датчиків і бездротових комунікаційних технологій. У найближчому майбутньому ми побачимо розвиток автомобільного автопілоту, що зможе виявляти пішоходи або інші транспортні засоби, а також маневрувати таким чином, щоб уникнути зіткнення [30]. Також для широкого застосування «Інтернету речей» у сфері транспорту й логістики важливі безпека й захист конфіденційності, тому що багато водіїв побоюються витоки інформації й вторгнення в приватне життя. Розумні зусилля за допомогою технологій, законів і регулювання будуть необхідні для запобігання несанкціонованого доступу або розкриття конфіденційних даних.

Використання IoT для пожежогасіння

«Інтернет речей» уже використовується в області пожежної безпеки для виявлення загорянь і раннього попередження можливих стихійних лих, пов'язаних з пожежами. У Китаї RFID-мітки й/або штрих-коди зв'язуються із засобами пожежогасіння для організації загальнонаціональної протипожежної інформаційної бази даних і систем керування. Завдяки використанню RFID-міток, мобільних RFID-зчитувачів, а також інтелектуальних відеокамер, сенсорних і бездротових мереж, управління пожежогасіння й прирівняні до них організації можуть виконувати автоматичну діагностику, щоб здійснювати в режимі реального часу моніторинг навколишнього середовища для раннього попередження пожеж і проведення необхідних аварійно-рятувальних мір. Дослідники в Китаї також використовують технології IoT, щоб вивести на новий рівень систему автоматичного протипожежного оповіщення з метою підвищення керування загораннями й іншими надзвичайними ситуаціями [31]. Недавно Цзи й Ци [32] продемонстрували інфраструктуру IoT-додатків, які використовуються для керування надзвичайними ситуаціями в Китаї. Інфраструктура цих IoT-додатків містить рівні зондування, передачі, підтримки, а також платформний і прикладний. IoT-інфраструктура розроблена таким чином, щоб інтегрувати локальні й специфічні галузеві системи. У цей час актуальної в цій області є проблема створення стандартів для протипожежного «Інтернету речей».

Дослідницькі проблеми й майбутні тенденції

Загальновизнано, що технології й додатки «Інтернету речей» поки що перебувають у зародковому стані [11]. Усе ще залишається безліч наукових проблем впровадження IoT у промисловість, що стосуються технологій, стандартизації, безпеці й конфіденційності [7, 8]. У майбутньому необхідно прагнути до їхнього рішення, вивчаючи особливості різних галузей індустрії, для того щоб забезпечити оптимальне впровадження IoT-пристроїв у промислових умовах. Галузеву специфіку й вимоги до таких факторів, як вартість, безпека, конфіденційність і ризики, необхідно усвідомити ще до того, як «Інтернет речей» почне широко використовуватися в промисловості.

Технічні проблеми

Хоча вже було проведено чимало досліджень за технологіями IoT, залишається ще досить технічних проблем.

– Дизайн сервіс-орієнтованої архітектури (SOA) для IoT доставляє певні труднощі, тому що сервіс-орієнтовані «речі» можуть постраждати від своєї продуктивності й цінових витрат. Також, у міру того як усе більше й більше фізичних об'єктів підключається до мережі, часто виникають проблеми з масштабованістю на різних рівнях, включаючи передачу даних і роботу з мережі, обробку даних і керування, а також забезпечення сервісів [8].

– «Інтернет речей» є дуже складною гетерогенною мережею, що включає в себе з'єднання між різними типами мереж за допомогою різних комунікаційних технологій. У цей час відсутня загальноприйнята єдина платформа, що приховує неоднорідність виділених мережних/комунікативних технологій і забезпечує прозорість іменованих сервісів для різних додатків [8]. Передача більших по обсязі даних по мережі в те саме час також може стати причиною частих затримок, конфліктів і комунікативних проблем. Це завдання може бути дозволена шляхом збору даних за допомогою великої кількості пристроїв. Керування зв'язаними «речами» з погляду полегшення взаємодії суб'єктів і адміністрування адресації, ідентифікації й оптимізації пристроїв на рівнях архітектури й протоколів є однієї з важливих дослідницьких завдань [6].

– Відсутність загальноприйнятої мови опису робить скрутним розвиток сервісу й ускладнює інтеграцію ресурсів фізичних об'єктів у сервіси, що приносять додатковий дохід (VAS-сервіси). Розвинені сервіси можуть бути несумісні з різним комунікаційним і впровадженим оточенням [7, 10]. Крім того, для поширення технології IoT повинні бути розроблені потужні методи виявлення сервісів і служби іменування об'єктів [7, 8].

– Тому що «Інтернет речей» часто розвивається на основі традиційний ІКТ-оточення й на нього впливає все, що підключено до мережі, буде потрібно багато роботи, щоб провести інтеграцію IoT з існуючими, у тому числі застарілими, ІТ-системами в єдину інформаційну інфраструктуру. Крім цього, велика кількість підключених до Інтернету зв'язаних «речей» буде автоматично відтворювати в режимі реального часу величезний потік даних [33], які не будуть мати особливого змісту, якщо люди не зможуть знайти ефективний спосіб їхнього аналізу й розуміння [34]. Аналіз або осмислення більших обсягів даних, генеруємих як додатками IoT, так і існуючими ІТ-системами, зажадає серйозних навичок, і це може виявитися складним для багатьох кінцевих користувачів. Крім того, для інтеграції IoT-пристроїв із зовнішніми ресурсами, такими як існуючі програмні системи й веб-сервіси, необхідні розробки різного проміжного ПЗ, тому що додатки сильно відрізняються по галузях. Вибудовування практичних додатків, у яких різнорідні й залежні від «Інтернету речей» дані комбінуються зі звичайними, може виявитися складним завданням для різних галузей промисловості.

Стандартизація

Швидкий розвиток «Інтернету речей» ускладнює стандартизацію. Однак саме вона відіграє важливу роль надалі становленні й поширенні «Інтернету речей». Стандартизація в IoT покликана знизити бар'єри для входу нових постачальників сервісів і користувачів, служить для поліпшення взаємодії різних додатків і сервісів, а також для забезпечення кращої якості продуктів або сервісів більше високого рівня. Достатня координація зусиль у процесі стандартизації забезпечить пристроям і додаткам з різних країн можливість обмінюватися інформацією [8]. Різні стандарти, використовувані в IoT (наприклад, стандарти безпеки, зв'язку й ідентифікації), можуть виявитися ключовими факторами для поширення й розробки технологій IoT. До специфічних питань в області стандартизації «Інтернету речей» відносяться проблеми сумісності, рівня радіодоступу, семантичної інтероперабельності, а також безпеці й конфіденційності [35-37]. Крім того, рекомендується розробити й галузеві стандарти або інструкції для спрощення інтеграції різних сервісів при впровадженні «Інтернету речей» у промисловість.

Інформаційна безпека й захист конфіденційності

Широке поширення нових технологій і сервісів «Інтернету речей» буде багато в чому ґрунтуватися на інформаційній безпеці й захисті конфіденційності даних, які стають проблематичними в IoT через особливості їхнього розгортання, мобільності й комплексності [38]. Багато хто з існуючих сьогодні технологій доступні для побутового використання, але не підходять для промислових додатків, у яких пред'являються підвищені вимоги по безпеці. Існуючі технології шифрування, запозичені з WSN (бездротової сенсорної мережі) або інших мереж, повинні бути ретельно перевірений перед їхнім використанням для захисту інформації при реалізації «Інтернету речей». Тому що IoT дозволяє багато повсякденних

речей відслідковувати, мониторити і зв'язувати, значна кількість особистої й персональної інформації може збиратися автоматично [7]. Захист приватності в середовищі «Інтернету речей» стане більше серйозної, чим у традиційному середовищі ІКТ, тому що кількість векторів атак на «речі» IoT, видимо, буде набагато більше [39-41]. Приміром, монітор здоров'я буде збирати дані пацієнта, такі як частота серцевих скорочень і рівень цукру в крові, а потім відправляти інформацію безпосередньо в кабінет лікаря по мережі. При цьому вона може бути украдена або зламана. Інший приклад – біодатчик, використовуваний у харчовій промисловості. Він може застосовуватися для моніторингу температури й бактеріального состава продуктів живлення, що зберігаються в холодильнику. Коли щось псується, дані про це відправляються в компанію через мережу. Однак така інформація повинна бути строго конфіденційної, щоб захистити репутацію харчової компанії [8]. Слід зазначити, що деякі питання, такі як визначення конфіденційності в IoT та її юридичне тлумачення, як і раніше чітко не визначені. Незважаючи на те, що вже існують мережні технології безпеки, для забезпечення основ конфіденційності й безпеки в IoT має бути проробити ще багато роботи. У першу чергу, необхідно вивчити наступні аспекти:

1) визначення безпеки й конфіденційності із соціальної, правової й культурної точок зору;

2) механізм довіри й репутації;

3) безпека зв'язку – зокрема, наскрізне шифрування (end-to-end);

4) конфіденційність переписки й даних користувача;

5) захист сервісів і додатків.

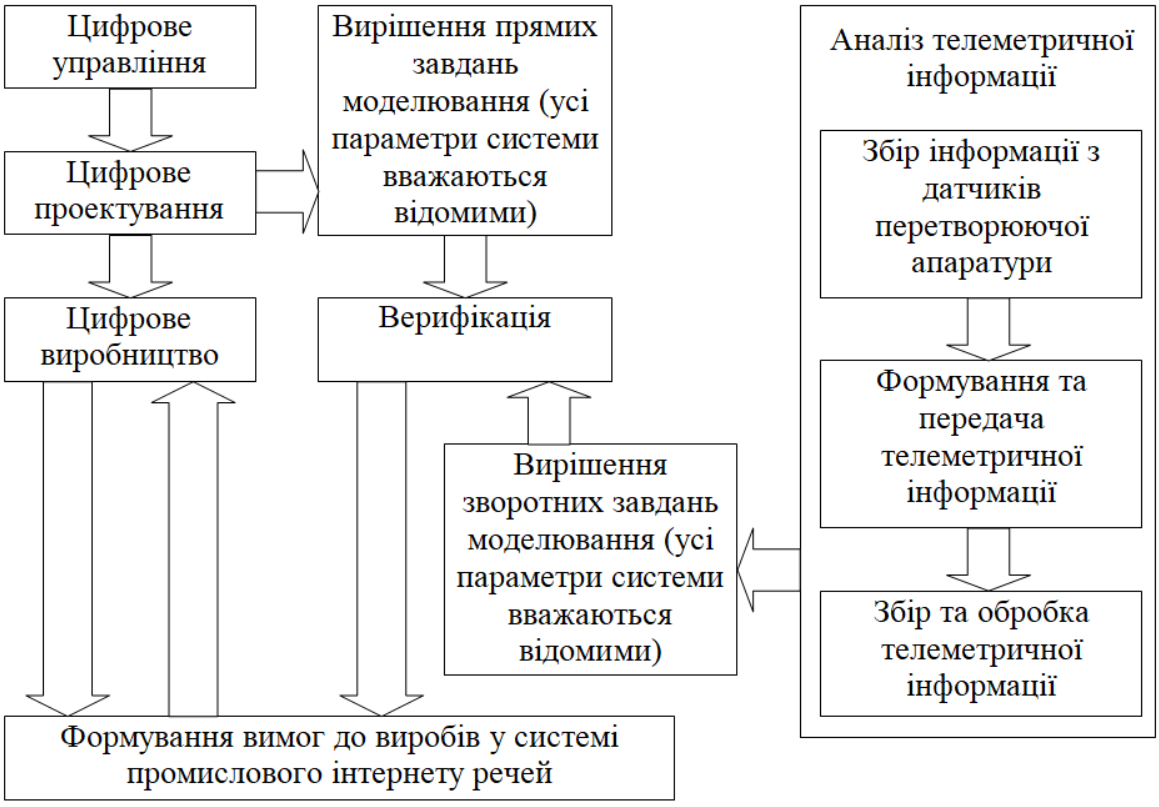


Рисунок 1 – Структурна схема системи

Напрямки досліджень

Підхід до розвитку інфраструктури «Інтернету речей» буде поетапним, що включає в себе розширення існуючих методів ідентифікації, таких як RFID. При цьому для рішення безлічі вищеописаних проблем необхідні міжнародне співробітництво й високий рівень системної перспективи [8,42-45]. У зв'язку із цим ми визначили, крім уже зазначених, деякі напрямки дослідження.

– Інтеграція соціальних мереж з IoT-рішеннями. Останнім часом виник великий інтерес до використання соціальних мереж для поліпшення комунікацій між різними « IoT-речами». Недавно групою вчених [14] була запропонована нова парадигма – соціальний «Інтернет речей» (SIoT). Також спостерігається тенденція переходу від «Інтернету речей» до нового напрямку, називаному «Веб речей» (Web of Things), що дозволить IoT-об'єктам стати акторами й рівноправними учасниками процесів у Всесвітній павутині [44-49].

– Розробка «зелених» IoT-технологій. Тому що «Інтернет речей» містить у собі мільярди підключених через бездротову мережу комунікативних датчиків, споживана ними потужність викликає більшу тривогу й обмежує використання «Інтернету речей». Поліпшення енергозбереження повинне стати найважливішою метою для розроблювачів IoT-пристроїв, насамперед бездротових датчиків [50, 51].

– Розробка контекстно залежних рішень сполучного програмного забезпечення IoT. Коли мільярди датчиків підключені до Інтернету, для людини стає неможливим обробити всі дані, зібрані цими датчиками. Контекстно залежні техніки обчислень, такі як сполучне програмне забезпечення IoT, призначені для кращого розуміння даних з датчиків і допомоги у відборі інформації для обробки [33]. У цей час більшість сполучних програмних забезпечень IoT не має можливостей для усвідомлення контексту. Європейський союз назвав контекстну залежність важливою областю досліджень IoT і вказав строки (2015-2020 р.) для проведення комп'ютерних досліджень і розробки контекстно-контекстно-залежного «Інтернету речей» [9].

– Застосування методів штучного інтелекту для створення розумних «речей». Деякі дослідники [52] пропонують створити «Інтернет розумних речей», привнесячи штучний інтелект в «речі» і комунікаційні мережі. На їхню думку, майбутні системи IoT повинні мати такі характеристики, як «самоконфігурування, самооптимізація, самозахист і самозцілення» [53, 54]. У майбутньому «розумні» речі стануть ще розумніше [55], контекстно залежні, будуть мати велику пам'ять і широкі можливості обробки, а також здатністю міркувати.

– Об'єднання «Інтернету речей» і хмарних обчислень. Хмари – гарний спосіб підключення «речей», вони можуть надати нам доступ до різного «речам» через Інтернет. Подальші дослідження будуть зосереджені на впровадженні нових моделей і платформ, які забезпечать «зондування як сервіс» у хмарах [56-58].

У якості складної кіберфізичної системи «Інтернет речей» поєднує різні пристрої, оснащені зондуванням, ідентифікацією, обробкою даних, комунікацією й які володіють мережними можливостями. Зокрема, датчики й виконавчі пристрої стають усе могутніше, дешевше й менше, що приводить до їхнього повсюдного використання. Індустрія сильно зацікавлена в розгортанні IoT-пристроїв для розробки промислових додатків, таких як автоматичний моніторинг, контроль, керування, експлуатація й технічне обслуговування. Передбачається, що через стрімкий розвиток технологій і промислової інфраструктури «Інтернет речей» буде широко застосовуватися в промисловості. Наприклад, у харчовій промисловості інтеграція бездротових сенсорних мереж (WSN) і радіочастотної ідентифікації (RFID) служить для побудови автоматизованих систем контролю, моніторингу й відстеження якості продуктів живлення по всьому ланцюжку поставок.

Висновок. У статті розглянуто та проаналізовано програмне забезпечення, яке призначено для системи промислового інтернету речей. В межах України в недостатній мірі представлені вітчизняні розробки в цій області. У роботі наведені теоретичне узагальнення й рішення наукового завдання дослідження методів промислового інтернету речей. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем промислового інтернету речей; Досліджена система промислового інтернету речей. На основі отриманих результатів досліджень створена програмна реалізація системи промислового інтернету речей. Розроблені під час виконання роботи алгоритми дозволяють успішно вирішувати завдання промислового інтернету речей. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована

алгоритм і вибраний середовище розробки. Розроблене програмне забезпечення має простий, дружній та зручний інтерфейс користувача, що забезпечує легкість у освоєнні роботи програмного продукту, зручність у використанні, і не потребує особливих спеціальних знань. При створені програмного забезпечення було використано об'єктно-орієнтований підхід, що відповідає сучасним тенденціям у галузі розробки комерційних програмних систем. Програма реалізована на мові високого рівня Builder C++. Дана мова програмування дозволяє найбільш ефективно обробляти дані. Це дозволило мінімізувати строк розробки програмного забезпечення, і, як слід, зменшити витрати на його розробку. Запропоноване програмне забезпечення ділиться на загальне програмне забезпечення, що поставляється із засобами обчислювальної техніки й спеціальне програмне забезпечення, що спеціально розроблене для даної конкретної системи й включає програми, що реалізують її функції. Даються необхідні рекомендації з установки розробленого програмного забезпечення. Для підвищення рівня безпеки запропоновано застосовувати алгоритм Khufu.

Список літератури

1. Van Kranenburg R., Anzelmo E., Bassi A., Caprio D., Dodson S., Ratto M. The internet of things // Proc. 1st Berlin Symp. Internet Soc. Germany, Berlin, 2011.
2. Jia X., Feng O., Fan T., Lei Q. RFID technology and its applications in internet of things (IoT) // Proc. 2nd IEEE Int. Conf. Consum. Electron., Commun. Netw. (CECNet). China, Yichang, 2012.
3. Sun C. Application of RFID technology for logistics on internet of things // AASRI Procedia. 2012. Vol. 1.
4. Ngai E. W. T., Moon K. K., Riggins F. J., Yi C. Y. RFID research: An academic literature review (1995–2005) and future research directions // Int. J. Prod. Econ. 2008. Vol. 112, No. 2.
5. Uckelmann D., Harrison M., Michahelles F. An architectural approach towards the future internet of things // Uckelmann D., Harrison M., Michahelles F. Architecting the Internet of Things. USA, NY: Springer, 2011.
6. Bandyopadhyay D., Sen J. Internet of things: Applications and challenges in technology and standardization // Wireless Pers. Commun. 2011. Vol. 58, No. 1.
7. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," Comput. Netw., vol. 54, no. 15, pp. 2787–2805, 2010.
8. Miorandi D., Sicari S., De Pellegrini F., Chlamtac I. Internet of things: Vision, applications and research challenges // Ad Hoc Netw. 2012. Vol. 10, No. 7.
9. Vermesan O., Friess P., Guillemin P. Internet of things strategic research roadmap. The Cluster of European Research Projects.
10. Sundmaeker H., Guillemin P., Friess P. Vision and Challenges for Realizing the Internet of Things. Belgium, Brussels: European Commission, 2010.
11. Xu L. Enterprise Systems: State-of-the-art and future trends // IEEE Trans. Ind. Informat. 2011. Vol. 7, No. 4.
12. Domingo M. C. An overview of the internet of things for people with disabilities // J. Netw. Comput. Appl. 2012. Vol. 35, No. 2.
13. Han C., Jornet J. M., Fadel E., Akyildiz I. F. A cross-layer communication module for the internet of things // Comput. Netw. 2013. Vol. 57, No. 3.
14. Atzori L., Iera A., Morabito G., Nitti M. The social internet of things (SIoT)-when social networks meet the internet of things: Concept, architecture and network characterization // Comput. Netw. 2012. Vol. 56, No. 16.
15. Lim M. K., Bahr W., Leung S. RFID in the warehouse: A literature analysis (1995–2010) of its applications, benefits, challenges and future trends // Int. J. Prod. Econ. 2013. Vol. 145, No. 1.
16. Zhu Q., Wang R., Chen Q., Liu Y., Qin W. IoT gateway: Bridging wireless sensor networks into internet of things // Proc. IEEE/IFIP 8th Int. Conf. Embedded Ubiquitous Comput. (EUC). China, Hong Kong, 2010.
17. Liu Y., Zhou G. Key technologies and applications of internet of things // Proc. 2012, 5th Int. Conf. Intell. Comput. Technol. Autom. (ICICTA). China, Zhangjiajie.
18. Cervantes H., Hall R. S. Automating service dependency management in a service-oriented component model // Proc. 6th Workshop Compon.- Based Softw. Eng. USA, Oregon, Portland, 2003.
19. Vazquez J. I., Almeida A., Doamo I., Laiseca X., Orduña P. Flexeo: An architecture for integrating wireless sensor networks into the internet of things // Proc. 2008, 3rd Symp. Ubiquitous Comput. Ambient Intell. Spain, Salamanca, 2009.
20. Flügel C., Gehrmann V. Scientific workshop 4: Intelligent objects for the internet of things: Internet of things-application of sensor networks in logistics // Commun. Comput. Inf. Sci. 2009. Vol. 32.
21. Pang Z., Chen Q., Tian J., Zheng L., Dubrova E. Ecosystem analysis in the design of open platform-based in-home healthcare terminals towards the internet-of-things // Proc. 2013, 15th Int. Conf. Adv. Commun. Technol. (ICACT). Korea, Pyeongchang.
22. Alemdar H., Ersoy C. Wireless sensor networks for healthcare: A survey // Comput. Netw. 2010. Vol. 54, No. 15.

23. Plaza I., Martin L., Martin S., Medrano C. Mobile applications in an aging society: Status and trends // J. Syst. Softw. 2011. Vol. 84, No. 11.
24. Pang Z., Chen Q., Han W., Zheng L. Value-centric design of the internet-of-things solution for food supply chain: Value creation, sensor portfolio and information fusion // Inf. Syst. Front. To be published.
25. Wei Q., Zhu S., Du C. Study on key technologies of internet of things perceiving mine // Procedia Eng. 2011. Vol. 26.
26. Karakostas B. A DNS architecture for the internet of things: A case study in transport logistics // Procedia Comput. Sci. 2013. Vol. 19.
27. Zhou H., Liu B., Wang D. Design and research of urban intelligent transportation system based on the internet of things // Commun. Comput. Inf. Sci. 2012. Vol. 312.
28. Qin E., Long Y., Zhang C., Huang L. Cloud computing and the internet of things: Technology innovation in automobile service // LNCS 8017. USA, NY, 2013.
29. Zhang Y., Chen B., Lu X. Intelligent monitoring system on refrigerator trucks based on the internet of things // Wireless Commun. Appl. 2012. Vol. 72.
30. Keller C. G., Dang T., Fritz H., Joos A., Rabe C., Gavrila D. M. Active pedestrian safety by automatic braking and evasive steering // IEEE Trans. Intell. Transp. Syst. 2011. Vol. 12, No. 4.
31. Zhang Y. C., Yu J. A study on the fire IOT development strategy // Procedia Eng. 2013. Vol. 52.
32. Ji Z., Qi A. The application of internet of things (IOT) in emergency management system in China // Proc. 2010 IEEE Int. Conf. Technol. Homeland Security (HST).
33. Wang S., Zhang Z., Ye Z., Wang X., Lin X., Chen A. Application of environmental internet of things on water quality management of urban scenic river // Int. J. Sustain. Develop. World Ecol. 2013. Vol. 20, No. 3.
34. Perera C., Zaslavsky A., Christen P., Georgakopoulos D. Context aware computing for the internet of things: A survey // IEEE Commun. Surveys Tuts. To be published.
35. Wang F., Ge B., Zhang L., Chen Y., Xin Y., Li X. A system framework of security management in enterprise systems // Syst. Res. Behav. Sci. 2013. Vol. 30, No. 3.
36. Li J., Yang J., Zhao Y., Liu B. A top-down approach for approximate data anonymization // Enterp. Inf. Syst. 2013. Vol. 7, No. 3.
37. Xing Y., Li L., Bi Z., Wilamowska-Korsak M., Zhang L. Operations research (OR) in service industries: A comprehensive review // Syst. Res. Behav. Sci. 2013. Vol. 30, No. 3.
38. Wan J., Jones J. Managing IT service management implementation complexity from the perspective of the Warfield version of systems science // Enterp. Inf. Syst. 2013. Vol. 7, No. 4.
39. Roman R., Najera P., Lopez J. Securing the internet of things // Computer. 2011. Vol. 44, No. 9.
40. Li L. Technology designed to combat fakes in the global supply chain // Bus. Horizons. 2013. Vol. 56, No. 2.
41. Ting S. L., Ip W. H. Combating the counterfeits with web portal technology. Inf. Syst. To be published.
42. Clarke J., Castro R., Sharma A., Lopez J., Suri N. Trust & security RTD in the internet of things: Opportunities for international cooperation // Proc. 1st Int. Conf. Security of Internet of Things. India, Kollam, 2012.
43. Xu L. Introduction: Systems science in industrial sectors // Syst. Res. Behav. Sci. 2013. Vol. 30, No. 3.
44. Li F., Jin C., Jing Y., Wilamowska-Korsak M., Bi Z. A rough programming model based on the greatest compatible classes and synthesis effect // Syst. Res. Behav. Sci. 2013. Vol. 30, No. 3.
45. Lin Y., Duan X., Zhao C., Xu L. Systems Science Methodological Approaches. USA, FL: CRC Press, 2013.
46. Atzori L., Carboni D., Iera A. Smart things in the social loop: Paradigms, technologies, and potentials. Ad Hoc Netw. To be published.
47. Xu L. Information architecture for supply chain quality management // Int. J. Prod. Res. 2011. Vol. 49, No. 1.
48. Sun J. Z. Towards the web of things: Open research issues and the BASAMI use case // Lect. Notes Electr. Eng. 2012. Vol. 144.
49. Guinard D., Trifa V., Mattern F., Wilde E. From the internet of things to the web of things: Resource-oriented architecture and best practices // Architecting the Internet of Things. USA, NY: Springer, 2011.
50. Xia F. Wireless sensor technologies and applications // Sensors. 2009. Vol. 9, No. 11.
51. Yaacoub E., Kadri A., Abu-Dayya A. Cooperative wireless sensor networks for green internet of things // Proc. 8th ACMSymp. QoSS Security Wireless Mobile Netw. Cyprus, Paphos, 2012.
52. Arsénio A., Serra H., Francisco R., Nabais F., Andrade J., Serrano E. Internet of Intelligent Things: Bringing artificial intelligence into things and communication networks // Stud. Comput. Intell. 2014. Vol. 495.
53. Kephart J. O., Chess D. M. The vision of autonomic computing // IEEE Computer. 2003. Vol. 36, No. 1.
54. Kortuem G., Kawsar F., Fitton D., Sundramoorthy V. Smart objects as building blocks for the internet of things // IEEE Internet Comput. 2010. Vol. 14, No. 1.
55. Ding Y., Jin Y., Ren L., Hao K. An intelligent self-organization scheme for the internet of things // IEEE Comput. Intell. Mag. 2013. Vol. 8, No. 3.
56. Rao B. P., Saluia P., Sharma N., Mittal A., Sharma S. V. Cloud computing for internet of things & sensing based applications // Proc. 2012 6th Int. Conf. Sens. Technol. (ICST). India, Kolkata, West Bangal.
57. Fang S., Xu L., Pei H., Liu Y. An integrated approach to snowmelt flood forecasting in water resource management // IEEE Trans. Informat. 2014. Vol. 10, No.1.

58. Gubbi J., Buyya R., Marusic S., Palaniswami M. Internet of things (IoT): A vision, architectural elements, and future directions // Future Gen. Comput. Syst. 2013. Vol. 29, No. 7.

УДК 004

В. Гермак, магістр гр. КН-18М3
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ IDS ЯКА БАЗУЄТЬСЯ НА ЧАСТОТНО-ЧАСОВОМУ АНАЛІЗІ

У статті розглянуто програмне забезпечення, яке призначено для системи IDS яка базується на частотно-часовому аналізі. Метою розробки є дослідження та програмна реалізація системи IDS яка базується на частотно-часовому аналізі. Об'єктом дослідження є процес виявлення вторгнення в мережу. Предметом дослідження є методи виявлення аномалій в роботі інформаційно-телекомунікаційних систем та мереж. Методи дослідження базуються на методах виявлення аномалій у даних про завантаження інтерфейсів телекомунікаційного устаткування на основі аналізу частотних характеристик, методах теорії ймовірностей і математичної статистики, методах теорії розпізнавання образів, методах теорії обчислювальних систем і мереж, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи IDS яка базується на частотно-часовому аналізі. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення. Розроблено зручний інтерфейс користувача. Наведені інструкції по роботі з програмними засобами.

комп'ютерні науки, система IDS, частотно-часовий аналіз

Постановка проблеми. З розвитком інформаційних технологій збільшується кількість уразливостей та загроз різноманітним системам обробки даних. Для забезпечення їх нормального функціонування та попередження вторгнень необхідні спеціалізовані засоби безпеки, а перспективним напрямком, який активно розвивається у сфері інформаційної безпеки є виявлення кібератак і запобігання вторгнень в інформаційних системах з боку неавторизованої сторони.

В реалізації політики безпеки інформаційно-комунікаційних мереж особливе місце займають системи IDS (системи виявлення вторгнень). Ці системи можуть бути використані як в ролі зворотного зв'язка, контролюючи ефективність компонентів системи безпеки, так і являти собою самостійний компонент системи безпеки. Для виявлення мережевих вторгнень використовуються сучасні методи, моделі, засоби і комплексні технічні рішення для систем виявлення та запобігання вторгнень, які можуть залишатись ефективними при появі нових або модифікованих видів кіберзагроз. Загалом при появі нових загроз та аномалій, породжених атакуючими діями з невстановленими або нечітко визначеними властивостями, зазначені засоби не завжди залишаються ефективними і вимагають тривалих часових ресурсів для їх відповідної адаптації. Тому системи IDS повинні постійно досліджуватись і удосконалюватись для забезпечення неперервності в їх ефективному функціонуванні. Серед таких систем є спеціалізовані програмні засоби, які направлені на виявлення підозрілої активності або втручання в інформаційну систему і прийняття адекватних заходів щодо запобігання кібератакам.

Для сучасних інформаційних систем та мереж гостро стоїть питання оперативного виявлення зловживань та аномалій. Для виявлення аномалій в системі IDS може використовуватися як сигнатурний метод, так і метод описової статистики.

Для дослідження сигналу можуть бути застосовані часові, спектральні і спектрально-часові алгоритми. Але слід зазначити, що за рахунок вираженої коливної поведінки

телекомунікаційного сигналу кращими у застосуванні будуть методи спектрального й спектрально-часового аналізу, аніж часові. Частотні алгоритми дозволяють розширити можливості існуючих систем IDS, які ґрунтуються на виявленні аномалій, але їх застосування вимагає великих розмірностей для подання результатів, також вони мають значну обчислювальну складність. Ці фактори стримують застосування частотних алгоритмів у прикладних завданнях. З цього випливає, що досить актуальною на сучасному етапі є розробка систем IDS, що грунтуються на методах виявлення аномалій в інтенсивностях потоків даних на основі алгоритмів аналізу частотних складових, оптимізованих по обчислювальному навантаженню.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини системи IDS яка базується на частотно-часовому аналізі.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи IDS яка базується на частотно-часовому аналізі.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем IDS.

– Дослідження системи IDS яка базується на частотно-часовому аналізі.

– Програмна реалізація системи IDS яка базується на частотно-часовому аналізі.

Об'єктом дослідження є процес виявлення вторгнення в мережу.

Предметом дослідження є методи виявлення аномалій у даних про завантаження інтерфейсів телекомунікаційного устаткування.

Методи дослідження базуються на методах теорії ймовірностей і математичної статистики, теорії розпізнавання образів, теорії обчислювальних систем і мереж, методах розробки програмного забезпечення.

Виклад основного матеріалу. В умовах сучасного розвитку інформаційних технологій на додаток до загальноприйнятих засобів захисту інформації, заснованих на розмежуванні і контролі прав доступу, авторизації і криптозахисті, все частіше використовують системи виявлення вторгнень.

Ефективні системи по спостереженню за безпекою враховують можливі ризики і вимагають глибокого розуміння цих ризиків, поточної архітектури мережі підприємства, ознак потенційних загроз і дій, які можуть наразити на небезпеку дані, розміщені на комп'ютерах цієї мережі. У інформаційно-телекомунікаційній системі IDS здійснює захист практично від тих же загроз, що і міжмережевий екран, проте між ними є принципові відмінності. Тоді як міжмережевий екран головним чином фільтрує небажаний вхідний та вихідний трафік, IDS аналізує певні параметри системи, у тому числі і трафік, і може сигналізувати про вторгнення в мережу. Тому міжмережевий екран і IDS зазвичай працюють спільно, і атаки, які міжмережевий екран пропускає, виявляє IDS.

Основним джерелом інформації для IDS є всілякі системні журнали і протоколи: вміст мережевого трафіку; показники функціонування системи, такі як число операцій введення-виведення, кількість працюючих процесів; інформація про продуктивність програмно-апаратного забезпечення, наприклад, об'єм використовуваної пам'яті і так далі; інформація про роботу користувачів з файлами і іншими ресурсами системи; адміністративна діяльність, наприклад, реєстрація нових користувачів.

Збір початкових даних здійснюється за допомогою спеціалізованих датчиків, що розміщуються в мережі, це один з найважливіших елементів IDS. IDS може включати два типи датчиків - мережеві і комп'ютерні. Мережеві датчики призначені для збору інформації про пакети даних, які передаються в тому сегменті мережі, де встановлений датчик. Комп’ютерні встановлюються на певні комп'ютери в мережі і призначаються для збору інформації про події, що виникають на цих комп'ютерах. При цьому на одному вузлі може бути присутніми одночасно декілька комп'ютерних датчиків, призначених для збору різної інформації. Зазвичай уся отримана датчиками інформація поступає на вузол обробки

інформації і ухвалення рішень. Мережеві датчики бувають двох видів.

Перший тип датчика має наступні функції і можливості:

− моніторинг трафіку в заданому сегменті мережі: фіксація SPAN, TAP, VACL і тому подібне;

− порівняння трафіку з сигнатурами атак, пошук евристичних шаблонів атаки, аномалій протоколів;

− визначення характеру атак на основі вбудованих логічних алгоритмів фрагментації і повторної зборки потоку;

− надання інструменту видачі сигналів тривоги і представлення можливості для певних активних дій: розрив TCP, блокування, реєстрація сеансу IP.

Такі датчики називають IDS датчиками.

Другий тип датчиків має наступні функції і можливості:

− виконує моніторинг усього трафіку, що «прозоро» проходить двома інтерфейсами;

− порівнює трафік з добре відомими сигнатурами атак, також здійснює пошук евристичних шаблонів атак і аномалій протоколів;

− включає логічний алгоритм фрагментації для чіткого визначення характеру атак, а також нормалізації потоку пакетів TCP/IP;

− слугує одночасно інструментом видачі сигналів тривоги і наочного представлення, виконує завдання профілактики шляхом фільтрації пакетів. Крім того, забезпечує можливість активних дій у відповідь : розрив TCP, блокування, реєстрація сеансу IP і відхилення пакету/потоку/користувача.

Такі датчики називають IPS датчиками.

Окрім описаних функцій, IDS може також вирішувати наступні завдання:

1. Дуже часто зловмисники пошкоджують міжмережеві екрани з метою подальшого безконтрольного проникнення в корпоративну мережу. Щоб понизити вірогідність такого проникнення можна використати системи виявлення атак, що функціонують на рівні мережі, для тимчасового резервування функцій міжмережевого екрану. IDS дозволяють здійснити фільтрацію мережевого трафіку по різних полях заголовка IP -пакета, що дозволяє організувати досить потужний пакетний фільтр, що мало чим поступається можливостям справжнього міжмережевого екрану. Крім того, IDS можуть використовуватися для тимчасового заміщення міжмережевого екрану під час регламентних робіт по оновленню програмного забезпечення міжмережевого екрану або тестування його налаштувань.

2. Контроль доступу до файлів. При цьому можуть бути використані як системи, що аналізують журнали реєстрації (наприклад, RealSecure Server Sensor), так і аналізуючі системні виклики (наприклад, Entercept).

3. Нерідкі випадки, коли співробітники компанії використовують службовий доступ в Internet у своїх особистих цілях - для пошуку роботи, розсилки резюме, спаму і інших несанкціонованих дій. Усе це призводить до втрати продуктивності праці, збільшенню витрат на оплату послуг Internet і так далі. Часто відбувається просочування конфіденційної службової інформації, яка може відбуватися не лише по електронній пошті, але і при зверненні до якого-небудь зовнішнього Web -серверу. З метою запобігання таким діям і виявленню неблагонадійних співробітників можуть застосовуватися IDS.

4. Антивірусний захист. IDS можуть бути застосовані і в даному випадку. І хоча вони в повному об'ємі не зможуть замінити класичну антивірусну систему, але частково можуть блокувати проникнення вірусів і троянських коней в корпоративну мережу.

5. Системи виявлення вторгнень, що функціонують як на рівні мережі, так і на рівні вузла, можуть бути використані для контролю несанкціонованих змін конфігурації вузлів, що захищаються, з боку користувачів, що мають адміністративні привілеї. В даному випадку ці системи виступають додатковим засобом контролю.

6. Нерідкі випадки, коли зловмисники підключають свої комп'ютери до критичних сегментів мережі з метою отримання доступу до конфіденційної інформації (наприклад, паролей або платіжних доручень). Встановлені на таких комп'ютерах аналізатори протоколів

(сніфери) дозволяють перехоплювати увесь мережевий трафік, циркулюючий між вузлами критичного сегменту. Небезпека таких несанкціоновано підключених пристроїв в тому, що вони без зусиль дістають доступ до паролів користувачів (в т.ч. і адміністратора), що передаються в незахищеному вигляді по більшості протоколів, побудованих на базі стека TCP/IP. Зокрема, беззахисними в даному випадку являються протоколи HTTP, FTP, Telnet, POP3, IMAP і так далі. В т.ч. відкритою залишається і інформація, що передається між SQL - сервером і клієнтським програмним забезпеченням. Нерідко співробітники компаній, в яких доступ в Internet регламентується і розмежовується за допомогою різних захисних засобів (наприклад, міжмережевих екранів або систем контролю змісту), підключають до своїх комп'ютерів модеми і використовують їх для виходу в Internet в обхід захисних механізмів. Також модеми дуже часто використовуються для отримання оновлень різних юридичних і бухгалтерських програм. І, нарешті, модеми можуть бути використані для доступу до робочого місця з дому. Це представляє велику загрозу для багатьох компаній, оскільки комп'ютери, до яких підключені модеми, ніяк не захищені і будь-який зловмисник, що виявив такий "чорний хід", може скористатися їм для несанкціонованого доступу до ресурсів, що вимагають обов'язкового захисту. IDS дозволяють виявляти в контрольованих сегментах мережі сторонні адреси від "чужих" комп'ютерів і вузлів, а також з незрозумілої причини збільшений трафік від якої-небудь робочої станції, раніше не поміченої в такій активності, що може свідчити про роботу з цього вузла зловмисника, що проник на нього через модем.

7. Міжмережевий екран - необхідний засіб для захисту інформаційних ресурсів корпоративної мережі. Але забезпечити необхідний рівень мережевої безпеки можна тільки при правильному налаштуванні міжмережевого екрану. Установка мережевих датчиків IDS до і після міжмережевого екрану дозволяє перевірити ефективність його налаштувань за рахунок порівняння числа атак, виявлених до і після міжмережевого екрану.

8. Нерідкі ситуації, коли співробітники відділів захисту інформації і відділів телекомунікацій не володіють достовірною інформацією про використовувані в сегментах мережі протоколи. За допомогою IDS можна контролювати усі використовувані в мережі протоколи і сервіси, а також частоту їх використання, що дозволяє побудувати схему інформаційних потоків в організації і карту мережі, що є запорукою успішного створення інфраструктури захисту інформації в організації.

9. Журнали реєстрації маршрутизаторів і інших мережевих пристроїв є додатковим джерелом інформації про атаки, спрямовані на інформаційні ресурси корпоративної мережі. Проте ці журнали реєстрації зазвичай не аналізуються на предмет виявлення в них слідів несанкціонованої діяльності, оскільки практично відсутні або дуже дорого коштують засоби (наприклад, netForensics), що вирішують цю задачу. Функція збору журналів реєстрації і аналізу подій в них може бути покладена на IDS, яка виступатиме в якості Syslog -сервера, і зможе не лише здійснити централізований збір, але і виявлення атак і зловживань в цих журналах. Крім того, це додаткова міра захисту журналів реєстрації від несанкціонованої зміни, оскільки події, що фіксуються маршрутизаторами, відразу ж передаються на сенсор IDS, що не дозволяє зловмисникові видалити або змінити компрометуючі його сліди.

10. IDS можуть і мають бути використані для збору доказів несанкціонованої діяльності за рахунок наступних можливостей: − запис подій, що відбуваються під час атаки, для подальшого аналізу і досліджень; − імітація неіснуючих застосунків з метою введення зловмисника в оману (т.з. режим обманної системи); − розширений аналіз журналів реєстрації прикладних і системних застосунків, серверів баз даних, Web -серверів і так далі; − можливість дослідження подій безпеки перед виконанням яких-небудь дій; − отримання DNS -, MAC -, NetBIOS - і IP -адрес комп'ютера зловмисника.

За способом аналізу даних IDS діляться на дві групи: сигнатурні та системи реєстрації аномалій (поведінкові).

Сигнатурні IDS представляють кожну атаку у вигляді спеціальної моделі або «сигнатури», що описує характеристики і сценарії можливих атак. Нині перспективними

вважаються три методи сигнатурного аналізу. Метод контекстного пошуку, що дозволяє найточніше задати параметри сигнатури, яку необхідно виявити в потоці початкових даних, метод аналізу станів і метод, що базується на експертних системах. Метод аналізу станів формує сигнатури атак у вигляді послідовності переходів мережі з одного стану в інший. Такі сигнатури атак зазвичай описуються за допомогою математичних апаратів кінцевих автоматів або мереж Петрі. Методи виявлення атак, що базуються на експертних системах, дозволяють описувати моделі атак на високо абстрактній природній мові. Така експертна система складається з бази фактів і бази правил. Факти є початковими даними про роботу мережі, а правила - методи логічного висновку про атаку на основі наявної бази фактів. Правила описують характерні ознаки атак, які повинна виявляти IDS.

Переваги сигнатурних систем: досить чітке визначення типу атаки, висока точність роботи практично без неправдивих спрацьовувань. Недоліки: нестійкість до новітніх типів атак, оскільки на момент атаки бази знань (сигнатур) ще не містять відповідних сценаріїв; залежність ефективності роботи від швидкості розробки нових сигнатур атак; відбувається втрата часу від розробки сигнатури розробниками IDS до оновлення бази цих сигнатур організацією споживача IDS; для складних розподілених атак перевірка на відповідність сигнатурі є нетривіальним завданням; більшість баз знань сигнатур і правил загальнодоступні, тому порушник може використати методи «маскування» атаки. Більшість цих недоліків можна звести до мінімуму, але головна проблема залишається завжди - якщо атака нова і для неї немає сигнатури, то виявлена вона ймовірно не буде.

IDS засновані на контролі частоти подій або виявленні статистичних аномалій більше орієнтовані на виявлення нових типів атак. Поведінкова IDS за певний час роботи (період навчання) обчислює «нормальну» мережеву активність і потім в експлуатаційному режимі аналізує параметри роботи мережі, і те, що не потрапляє під визначення «нормально», позначається як аномалія. Аномалію можна розглядати з трьох позицій: аномалія протоколу (включає пошук відхилень від стандартного протоколу), аномалія мережі (включає спостереження або запам'ятовування нормальних рівнів трафіку), поведінкова аномалія (включає запам'ятовування нормальної поведінки користувача). Найбільш ефективна проти хибних спрацювань IDS комбінація цих позицій спостереження аномалій. Особливістю будь-якої поведінкової IDS є її можливість вивчати мережеву активність і відрізняти нормальну мережеву активність від аномальної. Найчастіше такі IDS реалізуються на основі статистичних моделей. Ці моделі визначають статистичні показники, які характеризують параметри штатної поведінки системи. Якщо при роботі мережі ці параметри відхиляються від заданих значень, то метод дозволяє зробити висновок про факт реалізації атаки. В якості таких параметрів можуть виступати: рівень завантаженості процесора, завантаження каналів зв'язку мережі, штатний час роботи користувачів системи, кількість звернень користувачів до мережевих ресурсів мережі і так далі.

Найчастіше застосовуються такі статистичні моделі:

− порогова модель, яка для кожного статистичного параметра визначає порогові величини; якщо спостережуваний параметр перевищує заданий поріг, то ця подія є ознакою потенційної атаки;

− модель середнього значення і середньоквадратичного відхилення, яка для кожного статистичного параметра визначає так званий довірчий інтервал на основі математичного очікування і дисперсії; якщо поточне значення параметра не укладається в цьому інтервалі, то випадок розглядається як атака;

− багатоваріаційна модель, яка аналогічна моделі середнього значення і середньоквадратичного відхилення, але дозволяє одночасно враховувати кореляцію між великою кількістю статистичних показників.

Переваги поведінкових систем: - можуть виявляти абсолютно нові види атак; - здатні виявити атаки, що характеризуються великою тривалістю в часі; - такі системи в деякому розумінні простіше обслуговувати, оскільки немає потреби в оновленні сигнатур. Недоліки: - складно побудувати модель «нормальної» роботи мережі, тому вони схильні до хибного

спрацьовування сигналів про атаки; - такі системи необхідно «навчати» деякий період часу і вони не можуть працювати відразу ж після інсталяції в мережу; - введенням такої системи в експлуатацію повинні займатися висококваліфіковані в цьому напрямі фахівці; - на відміну від сигнатурних, поведінкові системи не генерують повідомлення, що точно описують атаку, а лише повідомляють про «аномальність», можливо з деякою додатковою інформацією і статистичними характеристиками; - необхідність установки ефективного порогового значення для сигналізації атаки; це вплине або на збільшення частоти хибних спрацювань, або система не видаватиме сигнали там, де необхідно.

У зв'язку з недоліками обох принципів побудови IDS останнім часом спостерігається тенденція до об'єднання різних методик виявлення несанкціонованої активності (сигнатур, аномалій протоколів, контролю поведінки трафіку і так далі); інтеграції з мережевим устаткуванням, переходом на програмно-апаратні рішення, поступовій відмові від сигнатурних методов на користь поведінкових.

Розглянемо специфіку формування вимог до базових механізмів підсистем IDS з точки зору розробки і реалізації конкретної архітектури IDS.

Модулі моніторингу, збору і аналізу інформації в режимі реального часу. Засоби (системи) аналізу захищеності повинні забезпечувати можливість виявлення вразливостей, пов'язаних з помилками в конфігурації програмного забезпечення інформаційної системи, які можуть бути використані зловмисником для реалізації атаки на систему.

Основні механізми, що повинні бути реалізовані: повна ідентифікація сервісів на випадкових портах; перевірка на вразливість серверів із складною нестандартною конфігурацією; евристичний метод визначення типів і імен серверів; визначення справжнього імені сервера і коректної роботи перевірок; визначення RPC сервісів і пошук вразливостей в них, а також визначення детальної конфігурації комп'ютера в цілому; перевірка стійкості парольного захисту; підбір паролів в сервісах, що вимагають аутентифікації, для виявлення нестійких паролів або таких що не відповідають розробленим політикам; глибокий аналіз контенту WEB сайтів; аналіз скриптів HTTP серверів і пошук в них наступних вразливостей; аналізатор структури HTTP серверів; пошук і аналіз директорій доступних для перегляду і запису; проведення перевірок на нестандартні DoS аномалії; здійснення перевірок на «відмову в обслуговуванні»; механізми, що зменшують вірогідність хибних спрацьовувань при скануванні; методи, що зменшують вірогідність помилкового визначення вразливостей.

Модулі централізованого управління повинні реалізовувати такі можливості: дистанційна установка додаткового програмного забезпечення; формування прав доступу користувачів; внесення змін до конфігурації; формування, перегляд і аналіз правил фільтрації; запит, отримання, перегляд, аналіз і обробка вказаної за видом і часом реєстраційної інформації про події безпеки; автоматичний моніторинг стану; централізований контроль стану і управління комплексом; перевірка доступності робочих станцій мережі або іншого устаткування.

Таким чином, система IDS повинна забезпечувати виконання наступних функціональних характеристик: повне охоплення джерел інформації про стан мережі; нарощування кількості джерел інформації; масштабування можливостей збору, ведення і аналізу неструктурованої інформації; розмежування доступу до інформації для різних категорій користувачів; міжмодульна взаємодія окремих підсистем і ролей персоналу в процесі функціонування, з можливим залученням експертів аналітиків.

Запропонований підхід до формування архітектури виключає ситуації, коли події, критичні для надійного і захищеного функціонування мережі, виявляться поза увагою аналітиків, і відносно них не будуть вжиті відповідні превентивні заходи.

Отже на сьогодні системи IDS стають необхідними додатками до інфраструктури захисту інформації кожної великої компанії. Питання про те, чи потрібна система IDS, для професіоналів захисту інформації вже не стоїть, проте перед ними виникає проблема вибору такої системи для конкретної організації. Крім того, висока вартість подібних продуктів

примушує ретельніше підходити до обгрунтування необхідності їх використання.

Розробка структурної схеми

На рисунку 1 зображена структурна схема розробленої системи.

На цій схемі можна побачити, що розроблена система IDS разом з середовищем її впровадження містить такі осковні структурні елементи:

– Мережа Інтернет.
– Мережевий екран.
– Мережевий комутатор.
– Корпоративна мережа, для захисту якої використовується система IDS.
– Зловмисники, які мають на меті завдати шкоди нормальному функціонуванню мережі.
– Бот-мережа яка може бути використана для здійснення атаки на мережу.
– Система IDS, яка складається з підсистеми аналізу, сенсорної підсистеми, консолі керування та сховища.
– Мережні ресурси.
– Система керування мережею.

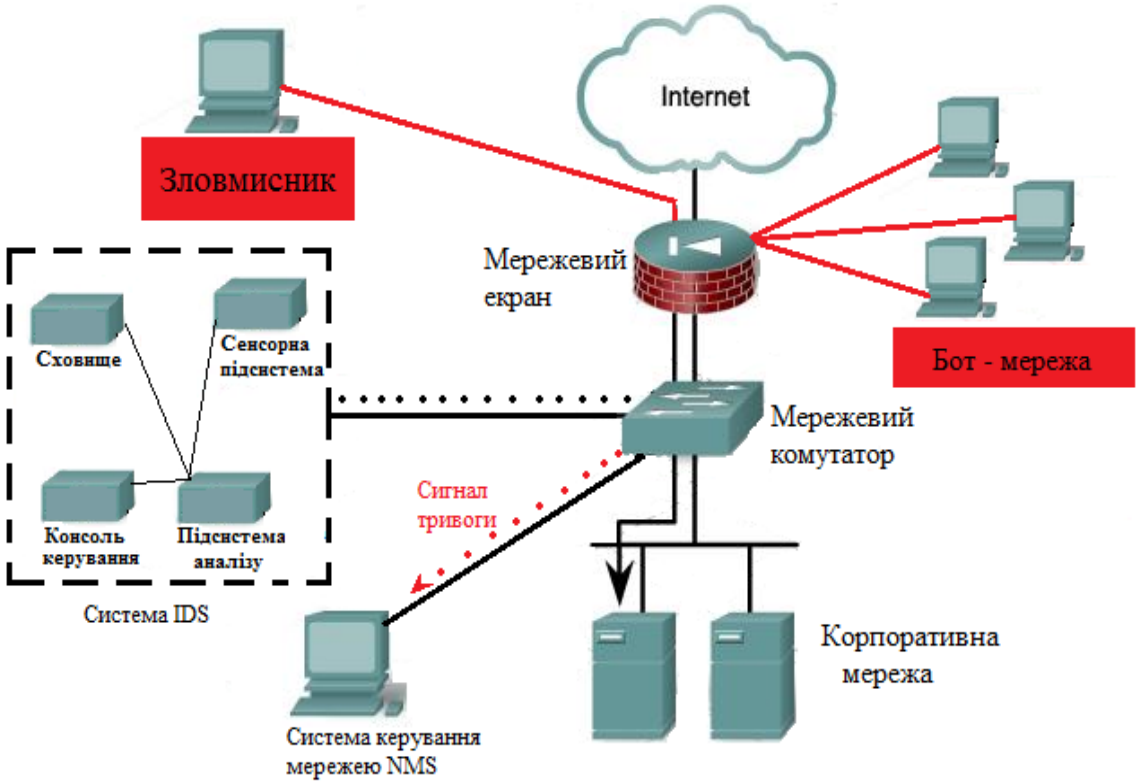


Рисунок 1 – Структурна схема системи

Розглянемо основні види загроз, які можуть бути реалізовані при здійсненні атаки на систему.

– Бот мережі.
– Віддалене проникнення (remote penetration).
– Локальне проникнення (local penetration).
– Атака на відмову в обслуговуванні (denial of service).
– Мережні сканери (network scanners).
– Сканери уразливостей (vulnerability scanners).
– Зламувачі паролів (password crackers).
– Аналізатори протоколів (sniffers).
– Спам e-mail (Mailbombing).

– Перехоплення каналу зв'язку (Man-in-the-Middle).
– Методи «грубої сили».

Бот мережі

Слово ботнет походить від англійських слів «robot» (робот) і «network» (мережа). Ботнет — це мережа пов'язаних між собою вірусом комп'ютерів, які управляються зловмисниками з командного центру. Ці шкідливі програми працюють непомітно, використовуючи при цьому системні ресурси комп'ютера користувача.

Основні можливості ботнетів:

– Перехоплення даних, які вводить користувач (логіни, паролі, дані кредитних карт) і передача їх в командний центр.
– Атаки на конкретні інтернет-ресурси. Залучені в ботнет комп'ютери відправляють по команді постійні запити на певний сайт, внаслідок чого той, не витримуючи такого навантаження, відключається.
– Розсилка спаму. Більше 80% світового спаму розсилається з ботнет-комп'ютерів.

Зловмисники включають комп'ютери в ботнети за допомогою двох основних стратегій:

– Вони спонукають користувача встановити їх шкідливе програмне забезпечення.
– Встановлення зловмисного програмного забезпечення через уразливості деяких програм або через злом облікових записів, які захищаються ненадійними паролями.

Задля убезпечення від видалення з інфікованого хоста, ПЗ ботнету має механізм самозахисту (механізм маскування). Механізм самозахисту аналогічний для більшості вірусів та руткітів. Крім того, ПЗ ботнету має певні механізми для забезпечення успішного запуску при увімкненні комп’ютера.

Кожен ботнет має механізми керування, завдяки якому всі інфіковані комп’ютери виконують дії, необхідні “власникові” ботнету. Раніше керування передбачало “очікування” певних команд від командного центру на певному порту, або участь в IRC-чаті. При відсутності команд програма “спить”, очікуючи на команду від командного центру, можливо намагається саморозмножуватись. При отриманні команди від командного центру ботнету, бот починає виконувати вказану команду. В ряді випадків за командою завантажується виконуваний файл (таким чином, є можливість “оновлювати” програму і завантажувати модулі, які додають функціональність). Наразі отримали поширення ботнети, які керуються через веб-сайт або по принципу p2p-мереж.

Відмова сервісу

Одним з різновидів втручання в роботу автоматизованих систем є атака на відмову в обслуговуванні (DoS), яка полягає в заблокуванні доступу користувачів до сервісу, що надається атакованою системою, або у примушуванні атакованої системи функціонувати потрібним зловмисникові чином. Якщо атака від- бувається одночасно з великої кількості IP-адрес, то її називають розподіленою (DDoS). Атаки на відмову зазвичай здійснюються з наміром зробити недоступними ресурси атакованої системи для легітимних користувачів. Крім того, метою атаки на відмову можуть бути й інші збої у функціонуванні атакованої системи. Наприклад, надмірне перевантаження ресурсів певної системи може призвести до відключення її міжмережевого екрану та зробити можливою іншу атаку на цю систему (наприклад, завантаження шкідливого програмного коду тощо), або атаку на другу систему, яка при нормальному функціонуванні першої атакованої системи була недосяжною для зловмисників.

За локалізацією реалізації атаки на відмову поділяються на локальні та віддалені. Локальні атаки (або атаки на стороні клієнта) реалізуються безпосередньо на атакованому хості. Віддалені атаки на відмову реалізуються ззовні відносно атакованого хоста або атакованої мережі.

В залежності від шляхів реалізації вони поділяються на два види:

– віддалена експлуатація уразливостей програмного забезпечення атакованої системи;

– перевантаження атакованої системи з метою вичерпання усіх наявних у атакованої системи ресурсів.

Віддалена експлуатація уразливостей програмного забезпечення представляє собою використання помилок, недоробок чи інших слабкостей у програмному забезпеченні атакованої системи з метою довести його до неробочого стану.

Перевантаження атакованої системи з метою вичерпання усіх наявних у атакованої системи ресурсів полягає у використанні величезної кількості безглуздих (рідше – осмислених) пакетів для завантаження ресурсів системи, необхідних для обробки запитів легітимних користувачів. Цей вид атаки також має назву флуд, що походить від англомовного терміну flood – повінь.

В залежності від напрямку реалізації флуд-атаки бувають:

– спрямовані на ресурси атакованої системи;

– спрямовані на канал зв'язку, що з'єднує атаковану систему з іншою частиною мережі.

В залежності від рівня мережевої моделі "OSI", на якому реалізується атака на відмову, виділяють сім рівнів: перший рівень – фізичний; другий – канальний; третій – мережевий; четвертий – транспортний; п'ятий – сеансовий; шостий – представлення; сьомий рівень – прикладний.

За схемою атаки, тобто за шляхами доставки атакуючим зловмисного трафіка жертві виділяють наступні атаки на відмову:

– пряма, під час якої пересилка трафіку здійснюється безпосередньо з одного або багатьох хостів;

– віддзеркалена, під час якої пересилка трафіка здійснюється через третіх осіб;

– прихована, під час якої зловмисний трафік ховається в "законому".

Існують наступні варіанти організації розподілених атак на відмову:

– Ботнет – зараження певного числа комп'ютерів програмами, які в певний момент починають здійснювати запити до атакованого сервера;

– Флешмоб – домовленість великого числа користувачів Інтернету почати здійснювати певні типи запитів до атакованого сервера;

– Смурфінг – атака з використанням широкомовних адрес та підробки IP-адреси відправника;

– Разове завантаження скрипта – здійснюється шляхом разового завантаження та виконання скрипта на комп'ютер, що бере участь у розподіленій атаці на відмову.

Наслідки DDoS-атак і їх ефективність можна істотно понизити за рахунок правильного налаштування маршрутизатора, брандмауера і постійного аналізу аномалій в мережевому трафіку.

Спам

Спам – масова розсилка комерційної, політичної і іншої реклами (інформації) або іншого виду повідомлень особам, що не висловлювали бажання їх отримувати. Легальність масової розсилки деяких видів повідомлень, для яких не потрібно згоду одержувачів може бути закріплена в законодавстві країни. Наприклад, це може торкатися повідомлень про стихійні лиха, що насуваються, масової мобілізації громадян і т. п.

Найбільш поширені види спаму:

– Реклама. Деякі компанії, що займаються легальним бізнесом, рекламують свої товари або послуги за допомогою спаму.

– Реклама незаконної продукції. За допомогою спаму рекламують продукцію, про яку не можна повідомити іншими способами. Сюди ж відноситься і реклама самих послуг розсилки спаму.

– Антиреклама. Заборонена законодавством про рекламу інформація (наприклад, очорніння конкурентів і їх продукції) також може поширюватися за допомогою спаму.

– "Нігерійські листи". Іноді спам використовується шахраями, щоб виманити гроші у одержувача листа. Найбільш поширений спосіб дістав назву "Нігерійські листи", тому що велика кількість таких листів приходила з Нігерії.

– Фішинг – ще один спосіб шахрайства. Він є спробою спамерів виманити у одержувача листа номери його кредитних карток або паролі доступу до систем онлайнових платежів. Такий лист зазвичай маскується під офіційне повідомлення від адміністрації банку.

Методи боротьби зі спамом:

– Ідеологія. Очевидно, що спам приносить економічну вигоду його замовникам. Це означає, що користувачі, незважаючи на неприязнь до спаму, все-таки користуються рекламованими за допомогою спаму послугами. Доти поки віддача від спаму перевищує витрати на подолання захисту, спам не зникне. Таким чином, найнадійнішим способом боротьби є відмова від послуг, що рекламуються за допомогою спаму.

– Превентивні заходи захисту від спаму. Самий найнадійніший спосіб боротьби із спамом - не дозволити спамерам упізнати електронну адресу.

– Фільтрація. Оскільки рекламні листи, як правило, сильно відрізняються від звичайної кореспонденції, поширеним методом боротьби з ними стало відсіювання їх з потоку пошти, що входить. На теперішній час цей метод - основний і найширше використовуваний.

– Автоматична фільтрація. Існує програмне забезпечення для автоматичного визначення спаму (спам-фільтри). Воно може бути призначене для кінцевих користувачів або для використання на серверах.

Висновок. У статті розглянуто та проаналізовано програмне забезпечення, створене в результаті виконання роботи, призначено для системи IDS яка базується на частотно-часовому аналізі. В межах України в недостатній мірі представлені вітчизняні розробки в цій області. У роботі наведені теоретичне узагальнення й рішення наукового завдання дослідження методів аналізу аномалій системи IDS яка базується на частотно-часовому аналізі. Рішення даного завдання полягало у вирішенні наступних задач: був проведений огляд існуючих систем IDS; досліджена система IDS яка базується на частотно-часовому аналізі; на основі отриманих результатів досліджень створена програмна реалізація системи IDS яка базується на частотно-часовому аналізі. Розроблені під час виконання роботи алгоритми дозволяють успішно вирішувати завдання виявлення вторгнень в телекомунікаційну мережу шляхом частотно-часового аналізу для реєстрації аномалій. Проведено аналіз предметної галузі, в ході якого були виявлені об’єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудовано алгоритм і обрано середовище розробки. Розроблене програмне забезпечення має простий, дружній та зручний інтерфейс користувача, що забезпечує легкість у освоєнні роботи програмного продукту, зручність у використанні, і не потребує спеціальних знань. При створенні програмного забезпечення було використано об’єктно-орієнтований підхід, що відповідає сучасним тенденціям у галузі розробки комерційних програмних систем. Програма реалізована на мові високого рівня Delphi. Дана мова програмування дозволяє ефективно обробляти дані. Це дозволило мінімізувати терміни розробки програмного забезпечення, і, як наслідок, зменшити витрати на його розробку. Запропоноване програмне забезпечення ділиться на загальне програмне забезпечення, що поставляється із засобами обчислювальної техніки й спеціальне програмне забезпечення, що спеціально розроблене для даної конкретної системи й включає програми, що реалізують її функції. В цілому створене програмне забезпечення підтверджує правильність використаних проектних рішень та повністю відповідає вимогам технічного завдання. Створене програмне забезпечення має потенційну можливість для подальшого вдосконалення і застосування у різних галузях.

Список літератури

1. Будько М.Б., Будько М.Ю. Отслеживание изменений в структуре сети и решение задач повышения безопасности на основе анализа потоков данных // Научно-технический вестник Санкт-Петербургского государственного университета информационных технологий, механики и оптики. Номер выпуска 59. – СПб.: СПбГУ ИТМО. – 2009. – С. 78-82.
2. Будько М.Б., Будько М.Ю. Определение источника широковещательного шторма на основе данных протокола SNMP // Сборник трудов конференции молодих ученых. Выпуск 6. Информационные технологии. – СПб.: СПбГУ ИТМО. – 2009. – С. 153-157.
3. Шалаева М.Б. Повышение эффективности алгоритмов кодирования речи // II межвузовская конференция молодих ученых – СПб: СПбГУ ИТМО, 2005. – С. 98-103.
4. Шалаева М.Б. Развитие алгоритмов сжатия речи // Научно-технический вестник Санкт-Петербургского государственного университета информационных технологий, механики и оптики. – 2005. – № 19. – С. 140-145.
5. Шалаева М.Б. Сравнение вычислительной сложности алгоритмов для кратковременного спектрально-временного преобразования // XII всероссийская научно-методическая конференция «Телематика'2005» – СПб: СПбГУ ИТМО. – 2005. – С. 95-97.
6. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей. Москва, ИД «ФОРУМ»: ИНФРА-М, 2008, 416 с.
7. Мельников В.В. Защита информации в компьютерных системах. Москва, Финансы и статистика, 1997, 368 с.
8. Лукацкий А.В. Обнаружение атак. 2-е изд. СПб.; БХВ-Петербург, 2003, 596 с.
9. Булдакова Т.И., Джалолов А.Ш. Анализ информационных процессов и выбор технологий обработки и защиты данных в ситуационных центрах. Научно-техническая информация. Серия 1, 2012, № 6, с. 16-22.
10. Нестерук Ф.Г., Осовецкий Л.Г., Нестерук Г.Ф., Воскресенский С.И. К моделированию адаптивной системы информационной безопасности. Перспективные информационные технологии и интеллектуальные системы, 2004, № 4, с. 25-31.

УДК 004

В. Горбов, магістр гр. КН-18М-1,9
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ ПОВЕДІНКОВОГО АНАЛІЗУ КОРИСТУВАЧІВ ЗА ДОПОМОГОЮ КОНЦЕПЦІЇ UEBA

У статті розглянуто програмне забезпечення, яке призначено для поведінкового аналізу користувачів за допомогою концепції UEBA. Метою розробки є дослідження та програмна реалізація поведінкового аналізу користувачів за допомогою концепції UEBA. Об’єктом дослідження є процес поведінкового аналізу користувачів за допомогою концепції UEBA. Предметом дослідження є методи поведінкового аналізу користувачів за допомогою концепції UEBA. Методи дослідження базуються на методах Big Data, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація поведінкового аналізу користувачів за допомогою концепції UEBA. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.
комп’ютерні науки, поведінковий аналіз користувачів, UEBA

Постановка проблеми. Функції, пов'язані з поведінковим аналізом, давно присутні в системах інформаційної безпеки, але окремий напрямок UEBA (User and Entity Behavior Analytics) з'явився всього кілька років назад. По визначенню Gartner, воно має на увазі перехід від аналізу правомірності використання даних до виявлення аномалій у поводженні користувачів і інших сутностей (entities): робочих станцій, додатків і мережного трафіку. Засновані на машинному навчанні й ретроспективному аналізі рішення UEBA дозволяють

побачити, що робив співробітник, скажемо, півроку назад і як змінилася його активність зараз. Поряд із застосуванням методів математичної статистики це називається профілюванням – з його допомогою можна виявити такі інциденти, які класичні системи пропускають.

Рішення класу UEBA можуть бути реалізовані у вигляді окремих інформаційних систем, а також у вигляді модулів до систем запобігання витоків (DLP – від англ. Data Leak Prevention), SIEM (Security Information and Event Management) або керування корпоративним контентом (ECM – від англ. Enterprise content management). У першому випадку вони мають величезну кількість конекторів до різного роду джерел структурованих і неструктурованих даних: системам керування обліковими записами, бізнес-додаткам, СУБД.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини системи поведінкового аналізу користувачів за допомогою концепції UEBA.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація поведінкового аналізу користувачів за допомогою концепції UEBA.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем поведінкового аналізу користувачів за допомогою концепції UEBA.
– Дослідження поведінкового аналізу користувачів за допомогою концепції UEBA.
– Програмна реалізація поведінкового аналізу користувачів за допомогою концепції UEBA.

Об’єктом дослідження є процес поведінкового аналізу користувачів за допомогою концепції UEBA.

Предметом дослідження є методи поведінкового аналізу користувачів за допомогою концепції UEBA.

Методи дослідження базуються на методах Big Data, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу.

Опис функціонування системи

Різноманітні рішення для забезпечення кібербезпеки виступають у ролі мудреців, кожний з яких знімає певну характеристику активності користувача й перевіряє її на приналежність до «чорного списку» критеріїв. Логічним розвитком цього підходу стало активне включення SIEM і Threat Intelligence у процес прийняття рішень – з їхнім об'єднанням з'явилася можливість збирати в одній крапці не тільки дані із сенсорів, але й «чорні списки» від різних виробників. За рахунок активного використання SIEM виходить збільшити відсоток детектуємих загроз (так званий detection rate) і наблизити його до якимось міфічних 100%. З у тім, що ці 100% мало пов'язані з реальною кількістю загроз, атак і ризиків, з якими зіштовхується будь-яка компанія.

Методи детектування загроз у своїй більшості засновані на зіставленні подій з відомими шаблонами шкідливої активності. Про це знають не тільки фахівці в області кібербезпеки, але й зловмисники. Для того щоб залишитися невидимим у потоці подій усередині інфраструктури, вони маскуються під реальних користувачів. Гірше всього, коли зловмисник – це і є реальний користувач або просто людина, що одержала у розпорядження обліковий запис користувача. І коли це відбувається, системи ІБ можуть серйозно спасувати. Щоб не дати злочинцеві успішно зробити атаку по новому сценарії, потрібно вивернути й сам метод виявлення навиворіт.

Насамперед, треба упокоритися з думкою, що потрібно шукати користувача. Не геш, не IP-адреса, не запис у реєстрі – а конкретного користувача, чий обліковий запис може зараз використовуватися по призначенню, а кілька разів у рік спонтанно робити шкідливі для бізнесу дії.

І шаблон його шкідливих дій нам буде швидше за все невідомий або замаскований під регулярну активність.

Місія підходу UEBA полягає в тому, щоб зібрати максимум даних із системи, сформувати з них логічні структури, об'єднані навколо користувачів, і зрозуміти по сукупності всієї наявної інформації, хто з користувачів поводиться «не так». У хід іде й побудова предиктивних математичних моделей, і ретроспективний аналіз даних, і активне використання високонавантажених розподілених систем зберігання даних. Проте, як слово захисту хочеться привести приклад із багатомільярдною індустрією онлайн-реклами на базі технології Real Time Bidding, що активно використовує всі вищезгадані технології. Їхнє використання в сфері кібербезпеки було лише питанням часу, і стартапи останніх декількох років, та й угода, зі згадування якої почалася ця замітка, говорять про те, що цей час прийшло.

Я б виділяв кілька відмітних критеріїв, чи ставиться рішення або його функціонал до сімейства UEBA:

– Система повинна вміти збирати й обробляти інформацію з великого числа (більше 80% експлуатованих у компанії) систем кібербезпеки.

– Щоб упоратися з навантаженням на системи зберігання й удержати час ухвалення рішення на «near real time» планці, система активно використовує розподілені високонавантажені платформи зберігання даних (HADOOP).

– Для одержання максимального контексту по подіях система повинна вміти працювати с даними – розпізнавати, агрегувати для подальшої обробки, індексувати – усередині користувальницької сесії.

– За зібраним даними за допомогою математичного моделювання й машинного навчання формуються ознаки «гарного поводження» користувача. Детектування виробляється на підставі відхилення від цих правил/ознак.

– Підсумкове завдання зводиться до пошуку конкретного облікового запису/особистості, що використовується в злобливих цілях інсайдером або зовнішнім зловмисником (у тому числі без ведена користувача).

Серед вендорів, що працюють у цьому напрямку, аналітики Gartner виділяють:

– Balabit.
– Bay Dinamics.
– CA Technologies.
– Datiphy.
– Dtex Systems.
– E8 Security.
– e-Safe Systems.
– Exabeam / тепер IBM.
– Forcepoint.
– Fortscale.
– Gurucul.
– Haystax Technology.
– IBM.
– Interset.
– Leidos.
– LightCyber / тепер Palo Alto.
– LogRhythm.
– Microsoft.
– Niara / тепер HPE.
– ObserveIT.
– Preempt.
– Rapid7.
– RedOwl.

– SecuPi.
– Securonix.
– Splunk.
– Varonis.
– Veriato.

На даний момент рішення UEBA можна розцінювати як спеціалізовані інструменти для роботи з рішення приватних кейсів трьох наступних загальних завдань:

– виявлення інцидентів, пов'язаних із захватом облікових записів користувачів зловмисником;
– виявлення інсайдерів серед співробітників компанії;
– формування єдиної бази знань про співробітників і побудова системи оцінки ризику не тільки на підставі даних з облікових систем, але й на базі їхнього поводження.

Розробка структурної схеми

UEBA або User-Entity Behavior Analytics – це модна тема, до якої стали звертатися організації, що не одержали задоволення від впровадження SIEM і інших інструментів аналізу даних у контексті інформаційної безпеки.

У яких випадках компанії звертаються до UEBA. Їх по суті три:

– недостача можливостей існуючих рішень і технологій по виявлення загроз, пов'язаних з діяльністю користувачів
– необхідність моніторити оточення, що не покривається іншими рішеннями й технологіями
– висока вартість сортування й пріоритезації подій ІБ в існуючих SIEM-рішень, які якось але оперують подіями, пов'язаними з користувачами.

Звідси відразу випливає вивід, що UEBA – це штучно створена сутність, що виникла на тлі проблем в існуючих на ринку рішень по ІБ, і коли ці завдання будуть вирішені, те й саме поняття "ринок UEBA" зникне (за прогнозами – до 2020-му року), злившись із іншими технологічними нішами, яких виділити можна дві:

– SIEM. Дуже часто виробники UEBA використовують системи керування подіями ІБ як крапку входу для своїх аналітичних можливостей. Воно й зрозуміло – навіщо самим збирати дані із джерел, коли можна взяти їх уже готові з SIEM. Але отут напрошується вивід, що SIEM-вендори могли б розширити функціонала своїх продуктів, додавши в них UEBA. Так і надходять, наприклад, Splunk, IBM, LogRhytm. Отут, щоправда, варто обмовитися, що UEBA відрізняється від класичного SIEM тим, що не опирається на тверді правила кореляції, граничні й "середні" значення, якими оперують системи керування подіями ІБ. Все-таки в абревіатурі UEBA остання буква означає "advanced analytics", тобто щось більше просунуте, що найчастіше базується на машинному навчанні й інших цікавих фішках, які дозволяють системі самонавчатися, а не жити за рахунок правил, створених аналітиком SIEM. Ще однією відмінністю від SIEM є робота з не "чистими" IT-даними. Нерідко UEBA беруть інформацію від HR-рішень, бізнесів-додатків, систем економічної безпеки й т.п., істотно розширюючи оперуємий ними контекст.
– DLP. З огляду на, що DLP останнім часом всі частіше трансформуються із засобів захисту від витоків інформації в засоби моніторингу поводження користувачів (навіть робочий час контролюють), те логічно припустити, що DLP будуть розширюватися функціями UEBA. На мій погляд це тупикова колія (от отут більш докладно написана, чому), тому що сама ідея DLP приречена на невдачу в сучасної IT-Середовищу, але, видимо, DLP-вендорів це мало зупиняє й вони хочуть додати новий поштовх своїм продуктам за допомогою хайповою UEBA.

Зрозуміло, що крім SIEM і DLP, технологія UEBA може розвиватися й самостійно. По такому шляху пішли лідери цього ринку – Securonix і Exabeam (у нас "чистих" вітчизняних UEBA-вендорів не спостерігається). З огляду на вищесказане, не виключаю, що зазначені компанії будуть куплені більшими гравцями й злиті з існуючими продуктами. Gartner уважає, що UEBA-функціональність буде з'являтися й в інших нішах ІБ – CASB, EDR, NTA,

що ще гостріше порушить питання про необхідність UEBA як самостійного рішення або вибору UEBA, як технології в якому-небудь із існуючих на ринку продуктів.

Gartner бачить два бізнес-кейса для покупки UEBA:

– Поліпшення виявлення загроз, що пропускаються іншими засобами захисту. Але є чи у вас такі засоби? Ви використовуєте щось крім IDS/IPS і антивірусів? Ви застосовуєте NTA, CASB? У вас уже є SIEM і ви, маючи багаторічний досвід роботи з ним, розумієте, що його можливостей вам реально не вистачає? Це важливий момент. UEBA потрібна тоді, коли ви реально перепробували всі й вас це не влаштовує. Отоді ви дійсно готові витратити кругленьку суму грошей на поведінкову аналітику. Якщо ж для вас це черговий хайп і ви із працею розумієте, що таке UEBA і навіщо вона потрібна, то варто почекати з вибором.

– Підвищення ефективності повсякденних операцій по ІБ, що дозволяють більш оперативно детектувати компрометацію користувальницьких облікових записів, витоку даних, порушення привілейованих користувачів і т.п. Але отут знову нас підстерігає засідка. Ви взагалі оцінюєте ефективність своїх операцій по ІБ? Ви реально оцінювали тимчасові й фінансові витрати на їхню реалізацію? Ви спробували знизити їх більше простими й, можливо, безкоштовними методами? Може почати із цього? От якщо ви готові із цифрами в руках показати, що поточне положення справ вас дійсно не влаштовує, вам варто подивитися убік UEBA. Але тільки в цьому випадку. У противному випадку ви витратите багато грошей і так і не зрозумієте, чи стало у вас краще й "ефективніше".

Серед деяких ключових проблем, з якими зіштовхуються замовники, що впроваджують або впровадили UEBA, Gartner називає наступні:

– Доступність і якість вихідних даних. Так-так, через 20 років з моменту появи SIEM на ринку, це дотепер основна проблема в моніторингу ІБ.

– Кваліфікація аналітиків. У вас є на прикметі ті, кого на Заході називають data scientist? Вони повинні добре розбиратися в ІБ і математику одночасно, щоб будувати й перевіряти коректність використовуваних моделей поводження, що закладаються в рішення UEBA. Найчастіше знайти таких фахівців майже нереально, а їхній річний фонд оплати праці може бути вище вартості UEBA-рішення. Без грамотних аналітиків набуте рішення перетвориться в гарбуз і стане черговою марною іграшкою в руках служби ІБ.

– Оцінка ефективності технології. Ну я б назвав це загальною проблемою в ІБ, а не тільки в UEBA.

– Приватність. Так, робота з Великими даними – взагалі представляє більшу проблему для приватності, так по аналізі розрізнених даних можна робити дуже цікаві, і часто безсторонні, виводи про поводження користувачів, що вступає в конфлікт із конституційними правами громадян на невтручання в приватне життя. Антон розповідав, що одного з американських UEBA-вендорів європейські замовники навіть попросили перейменувати продукт, щоб з його назви зникли слова "user behavior analysis", які є табу в Європі, що так бореться за права громадян.

Безпека – це завжди про розумного порушника і якою б супер-розумною не була технологія, вона завжди буде зіштовхуватися з ірраціональним поводженням людини, що складно пророкувати. В автоматизованих систем прийняття рішень в ІБ (читай, ІБ-роботів) є майбутнє, але не можна покладатися на них цілком – роль людини в прийнятті рішень залишається дуже важливої. Тому, впроваджуючи UEBA, SIEM, SOC, EDR, NTA і т.п. не забувайте приділяти належну увагу кваліфікації свого персоналу, що впроваджує, набудовує й експлуатує всі сучасні "розумні" ІБ-технології.

Рішення класу UBA (User Behavior Analytics, профілювання профілю поводження користувачів) представляють одне з найбільше що швидко розвиваються напрямків в області засобів безпеки. Витративши мільярди доларів на захист від шкідливих програм, DLP, керування журналюванням і SIEM-технології, комерційні й державні організації переконуються, що ці інвестиції не дозволяють виявляти сучасні складні атаки й мають обмежені можливості по підтримці центрів SOC. Як результат, ці організації розглядають

UBA-аналітику як засіб для аналізу даних у величезних сховищах журналів аудита, розділяючи такі завдання по двох категоріях:

Визначення пріоритетів: Аналітики щодня спостерігають стійкий потік повідомлень про події ІБ, з величезною кількістю помилкових і незначущих повідомлень. Багато компаній попросту ігнорують ці події, оскільки не мають необхідні ресурси для їхнього повноцінного аналізу. UBA-рішення частково звільняють перевантажений персонал центрів SOC від завдань по пріоритезації подій і інцидентів, що дозволяє їм зосередитися на деяких загрозах, що мають першорядне значення.

Реагування: У підсумку, після визначення факту атаки й залучення до неї уваги, фахівці з розслідування інцидентів повинні оцінити загрозу й вжити заходів, що роблять неможливим подальшу потайливу присутність хакера в мережі. У такий спосіб UBA-рішення допомагають фахівцям з розслідування інцидентів, надаючи інформацію про об'єкти, які підверглися атаці, про дії тих або інших осіб і про те, які облікові записи використовувалися для нападу.

При виборі рішення UBA-аналітики по виявленню, пріоритезації й реагуванню на загрози потрібно усвідомлювати весь потенціал наукомісткої аналітики даних. Організації повинні задавати продавцям питання про те, чи забезпечують їхні рішення підтримку наведених далі 12 структурних блоків застосування UBA, і, що більше важливо, зажадати продемонструвати цю підтримку **в рамках POC або пілотного рішення.**

Структурний блок завдання «виявлення»

Очевидною необхідністю є можливість виявлення сучасних кібератак; чим раніше організація виявить факт нападу, тим меншим буде негативний вплив. Перераховані далі завдання UBA-аналітики забезпечують підвищений рівень виявлення й у всіх випадках надають ефективне рішення.

Рисунок 1 – Структурна схема системи

- **Блок компрометації облікового запису користувача:** Необхідне, але не достатня умова для UBA-аналітики. Рішення повинне легко виявляти факт одержання хакером контролю над обліковим записом мережного користувача незалежно від напрямку вектора атаки або використання шкідливих програм. Це містить у собі виявлення атак типу *«pass the hash»* і *«golden socket».* Функція виявлення повинна працювати з будь-якими сполученнями облікових записів користувачів, пристроїв або IP-адрес. Важливо, що здатність до виявлення факту компрометації облікового запису будь-якого користувача або підрядника в межах організації є основною вимогою.
- **Блок компрометації облікового запису привілейованого користувача:** Компрометація облікового запису привілейованого користувача (наприклад, DBA або системного адміністратора) є більше важким завданням. Привілейовані користувачі можуть не працювати відповідно до стандартних шаблонів поводження, тому що їм регулярно доводиться реагувати на екстремальні ситуації. Тому профілювання дій таких користувачів виявляється більше важким завданням. Рішення UBA-аналітики повинні бути здатні ідентифікувати певні типи атак на привілейованих користувачів, які мають права доступу до критичних систем. Атакуючі одержують контроль над обліковим записом привілейованого користувача й потім одержують безпосередній доступ до ключових систем; засоби UBA-аналітики повинні негайно розпізнавати цю ситуацію.
- **Блок доступу до ресурсів керівництва:** Очевидними цілями хакерів є ресурси, що належать виконавчим або фінансовим директорам організацій, наприклад їхні ноутбуки. Ці системи містять важливу інформацію про власність, злиття й придбання або

інформацію, що має конкурентне значення. Наприклад, щорічно сотні мільйонів доларів викрадаються за допомогою електронних перекладів, здійснюваних з використанням веб-систем електронної пошти, шляхом обману керівників, що змушують, підтверджувати такі грошові перекази. Ефективні рішення UBA-аналітики повинні мати здатність до автоматичної побудови моделей ресурсів, що ідентифікують системи, що належать керівництву організацій, і повинні потім контролювати нестандартний і незвичайний доступ до таких систем.

- **Блок визначення внутрішніх загроз:** Хоча багато хто з більшості найбільш відомих уразливостей були викликані шкідливим впливом, спрямованим ззовні, шахраї-інсайдери продовжують залишатися джерелом втрати даних. Рішення UBA-аналітики повинні бути здатні виявляти ситуації, коли особа, що ставиться або не стосовне до категорії привілейованих користувачів, робить ризиковані операції, що виходять за рамки звичайного профілю поводження.

Кожна з наведених завдань пов'язана з виявленням тих або інших кіберзагроз. Ці загрози не є взаємовиключними, і ефективні рішення UBA-аналітики повинні мати здатність до одночасної роботи з усіма загрозами.

- **Структурний блок завдань «пріоритезації й реагування»**. Хоча багато які вендори рішень UBA-аналітики говорять про виявлення загроз, не всі ці рішення можуть використовуватися для збільшення ефективності роботи центрів SOC і IT-Персоналу. Перераховані далі завдання UBA-аналітики приділяють основну увагу більше точному визначенню пріоритетів і більше ефективному реагуванню на інциденти. У цих випадках рішення UBA-аналітики також повинні бути здатні до одночасної підтримки всіх перерахованих операцій.

- **Блок блокування облікових записів:** Блокування облікових записів вимагає зненацька більших витрат часу на адміністрування. Звичайно у великих організаціях використовують персонал, що працює в режимі повного робочого дня протягом усього року, тільки для аналізу блокувань користувальницьких облікових записів для з'ясування, чи було блокування викликане простою помилкою в наборі пароля або є ознакою спроби перехоплення, що мала місце, аккаунта. Для визначення ступеня ризику адміністратори нерідко по 4-5 годин аналізують дані по обліковому запису, пов'язані з тим або іншим конкретним блокуванням. Рішення UBA-аналітики повинні бути здатні автоматизувати цей процес і виносити вердикт про ризик для облікового запису. При ефективному використанні рішення UBA-аналітики можуть заощадити витрати на персонал, що працює в режимі повного робочого дня протягом усього року.

- **Блок створення облікових записів:** Хакери часто проникають у мережу через шкідливе ПЗ, установлене на одній системі, а потім використовують цей доступ для створення нових облікових записів, не пов'язаних з тим, що використовувався для входу аккаунтом. Навіть якщо IT фахівці перезапишуть образ скомпрометованої машини, хакери вже будуть перебувати в системі, використовуючи нові облікові записи. Рішення UBA-аналітики повинні аналізувати поводження при створенні облікових записів і швидко ідентифікувати незвичайні операції, наприклад неавторизоване створення нового облікового запису або порушення встановлених процедур.

- **Блок спільного використання облікових записів:** Багато організацій зіштовхуються із проблемами, викликаними використанням тих самих облікових записів декількома користувачами, що є порушенням політики й становить небезпеку для безпеки. Наприклад, група адміністраторів DBA може спільно використовувати аккаунт у БД для резервного копіювання й відновлення, настроювання продуктивності й ін. Рішення UBA-аналітики повинні ідентифікувати такі випадки із вказівкою користувачів, що використовують аккаунт у режимі спільного доступу, а також повинні допомагати в раціоналізації даного завдання.

- **Блок класифікації сервісних облікових записів:** Як правило, співробітники ІБ мають обмежені можливості для контролю за сервісними обліковими записами, які мають

високий рівень повноважень, що робить такі аккаунти мішенню для атакуючих. Наприклад, аккаунт «Firefighter» («пожежний») у системі SAP має значні повноваження, що забезпечують доступ до критично важливих додатків. Рішення UBA-аналітики повинні автоматично ідентифікувати сервісні аккаунти й позначати їхнім відповідним прапорцем при виявленні незвичайного поводження в межах цих аккаунтів.

- **Блок роботи з неактивними обліковими записами:** У багатьох організаціях діють політики у відношенні неактивних облікових записів. Якщо користувач не входив у свій аккаунт протягом 30 днів то можливо, що цей користувач покинув компанію й нормальний процес деактивації користувача не був доведений до кінця. Рішення UBA-аналітики повинні забезпечувати можливість безперервного спостереження за співробітниками й підрядниками, що не використовували свої облікові записи протягом установленого періоду.
- **Блок розслідування оповіщень системи безпеки:** Рішення для UBA-аналітики співіснують у рамках підприємства з багатьма рішеннями ІБ, наприклад із програмами захисту від шкідливого ПЗ, DLP, засобами керування мережним доступом і іншими. Ці програми видають оповіщення, які повинні бути розглянуті для усунення наявних проблем. Однак ці оповіщення можуть містити обмежену інформацію (наприклад, IP-адреса, але без прізвища власника й назви відділу), що ускладнює процес розслідування. Рішення UBA-аналітики повинні забезпечувати повний аналіз контексту для користувача й ресурсів, пов'язаних з оповіщеннями від сторонніх систем безпеки. Персонал центрів SOC повинен мати можливість доступу до ідентифікаторів оповіщень, формованих сторонніми програмами в UBA, для перегляду всього інформаційного контексту відповідного оповіщення.
- **Блок розслідування облікових записів:** Як правило, юридичні й кадрові департаменти компаній запитують щомісячні звіти з історією дій користувача. Добування й інтеграція інформації в межах всіх систем, пристроїв, мереж, IP-адрес і облікових записів представляє трудомістку ручну роботу. Рішення UBA-аналітики повинні надавати автоматичний перегляд тимчасової діаграми всієї мережної активності, включаючи доступ користувача через VPN і зміни облікового запису в межах однієї системи, і виділяти незвичайне поводження разом з оцінками ризику таких операцій. При правильному виконанні це може заощаджувати кілька днів роботи для кожного розслідування.
- **Блок огляду порушень безпеки:** Після виявлення інциденту, пов'язаного з витоком даних або зломом мережі, робота внутрішніх і зовнішніх команд розслідування інцидентів може зайняти тижня й місяці кропіткої праці для стикування тимчасових діаграм всіх порушень безпеки й визначення дій учасників, точного часу й переліку систем, порушених інцидентом. Рішення UBA-аналітики повинні забезпечувати можливість автоматичної обробки більших обсягів інформації для побудови тимчасових діаграм, що відбивають всіх користувачів і системи, порушені інцидентом.
- **Блок інтеграції з рішеннями Red Team:** У підсумку багато операційних центрів інформаційної безпеки SOC використовують засоби тестування Red Team для виявлення уразливостей і підготовки/навчання аналітиків до роботи з майбутніми атаками. Рішення UBA-аналітики повинні підтримувати роботу засобів тестування Red Team шляхом відображення всього ланцюжка атаки під час і після моделювання подій, пов'язаних з порушенням безпеки. При правильній реалізації UBA-аналітика забезпечує більше глибоке внутрішнє розуміння слабких місць і уразливостей.

Red Team

Термін Red Team прийшов з військового середовища й визначає «дружню» атакуючу команду. На противагу їй існує команда захисників – Blue Team.

Відмінність Red Team операцій від класичного пен-теста в першу чергу в регламенті дій і попередженні сторони, яка захиається. Також, при «класичному» пен-тесті найчастіше використовуються «білі списки», обмеження за часом проведених робіт, рівню взаємодії із системою. При проведенні Red Team операцій немає практично ніяких обмежень,

виробляється реальна атака на інфраструктуру: від атак зовнішнього периметра, до спроб фізичного доступу, «твердих» соціотехнічних технік (не фіксація переходу по посиланню, а, приміром, повноцінний реверс-шелл).

Завдання Blue Team – забезпечувати захист інфраструктури наосліп: команду захисників не попереджають про проведення атаки або її відмінностей від реальних зловмисників – це один із кращих факторів перевірити як захисні системи, так і здатність фахівців виявляти й блокувати атаки, а згодом проводити розслідування інцидентів. Після завершення операції необхідно зрівняти відпрацьовані вектори атак із зафіксованими інцидентами для поліпшення системи захисту інфраструктури.

Підхід Red Team ближче всього співвідноситься з таргетованой атакою – APT (Advanced Persistent Threat). Команда Red Team повинна складатися з досвідчених професіоналів, з багатим досвідом як побудови IT/ІБ інфраструктури, так і досвідом компрометації систем.

Що відрізняє Red Team операції:

– Тривалість. Атаки можуть проводиться протягом декількох місяців.

– Жорсткість. Атакуючі можуть досить жорстко впливати на інфраструктуру, що може привести до виходу частини компонентів інфраструктури з ладу.

– Відсутність звичних шаблонів тестування на проникнення. (Кейс із практики – під час обходу СКУД системи на одному з об'єктів аудита командою був здійснений винос оргтехніки, що містить критичні дані за межі компанії – природно при узгодженні з керівником робіт).

Red Team – це спроби одержати доступ до системи будь-якими способами, що включають у себе тестування на проникнення; фізичний доступ; тестування ліній зв'язку, бездротових і радіочастотних систем; тестування співробітників за допомогою сценаріїв соціальної інженерії.

Концепція Red Team операцій дозволяє провести роботи з тестування на проникнення максимально реалістично.

Командний підхід

Red Team схожий з військовою операцією: визначаються мети або об'єкти атаки, зони відповідальності й ролі членів команди. Нерідко в Red Team команді може виступати інсайдер, що передає дані зсередини компанії, або виконуючу допоміжну функції.

Чіткий розподіл ролей, системи оперативної взаємодії й аналізу даних спричиняються кілька ролей:

– лідер команди – керівництво;
– оперативники – активна фаза атаки;
– інсайдери – ця роль може бути відсутньою;
– аналітики – аналіз і нормалізація отриманих даних

Інструментарій

Використання конкретного інструментарію в окремому випадку може бути обумовлено специфікою того або іншого додатка або сервісу й слабко відрізняється від звичайного тестування на проникнення. При проведенні Red Team операцій встає питання командної взаємодії й систематизації отриманих результатів – це й звіти різних інструментальних засобів аналізу й уразливості виявлені в ручному режимі – все це представляє із себе величезний обсяг інформації, у якому без належного порядку й системного підходу можна упустити щось важливе або «розгрібати» можливі дублі. Також існує необхідність відомості звітів і їхня нормалізація й приведення до єдиного виду.

Звичайно Red Team операції покривають досить об'ємні інфраструктури, які вимагають застосування спеціалізованого інструментарію:

– Сканери й утиліти для проведення інвентаризації периметра, з можливістю поділу робочих зон і відомості результатів.

– Системи обробки даних при проведенні тестування на проникнення.

– Використання засобів аналізу й керування уразливостями.

– Системи проведення соціотехнічних кампаній.

Спеціалізоване програмне забезпечення:

Cobalt Strike

Cobalt Strike – це фреймворк для проведення тестів на проникнення. Це просунутий аналог Armitage, що у свою чергу є GUI надбудовою над Metasploit Framework. Просунута система убудованого скриптової мови дозволяє проводити найбільш ефективні атаки.

Dradis

Dradis Framework є платформою з відкритим вихідним кодом для спрощення спільної роботи й звітності в області інформаційної безпеки. Dradis є автономним веб-додатком, що забезпечує централізоване зберігання інформації. Існують дві версії – Community Edition (безкоштовна) і Professional Edition (від $59). У про версії більше функціонала, у тому числі в можливостях інтеграції, системі звітів, підтримці (у тому числі й пріоритетної), доступних методологіях і т.д. Можливе розширення функціонала у вигляді плагинів/аддонів.

Faraday IDE

Faraday – саме потужне середовище для спільної роботи, true multiplayer penetration testing. Підтримує роботу в ArchAssault, Archlinux, Debian, Kali, OSX, Debian. Працює в режимі реального часу, моментально обробляючи результати, прислані тим або іншим пен-тестером. У цьому фреймворку закладений концепт геймифікації, фахівцям дається можливість померяться скиллами по кількості і якості зарепорчених уразливостей.

Nessus

Один із самих популярних сканерів уразливостей, розроблений компанією Tenable Network Security. До 2005 року це було вільне програмне забезпечення з відкритим вихідним кодом, а в 2008 році вийшла платна версія продукту.

OpenVAS

OpenVAS (Open Vulnerability Assessment System, Відкрита Система Оцінки Уразливості, первісна назва GNessUs) фреймворк складається з декількох сервісів і утиліт, що дозволяє робити сканування вузлів мережі на наявність уразливостей і керування уразливостями.

SE Toolkit

Social Engineering Toolkit (набір для соціальної інженерії), класичний мультиінструмент, для проведення соціотехнічних атак.

GoPhish

OpenSource фреймворк для фішинга. Дозволяє проводити масовані фішингові атаки.

Logstash/Elasticsearch/Kibana

Рішення для широкого спектра завдань зі збору, аналізу й зберіганню даних.

Хоча ринок рішень UBA-аналітики усе ще є новим, такі рішення приносять досить реальні вигоди відносно виявлення сучасних загроз і ефективного реагування. Замовники нерідко й цілком обґрунтовано утрудняються у виборі тих або інших різноманітних продуктів, що важко піддаються порівняльній оцінці. Важливо вибрати рішення UBA, архітектура й конструкція якого забезпечують підтримку не тільки базового функціонала, такого як незвичайне поводження аккаунта, але також і більш складних завдань, наприклад блокувань аккаунтів і інших поки не ідентифікованих випадків.

Наведений вище список є гарним вихідним пунктом для оцінки рішень з аналізу поводження користувачів.

Висновок. У статті розглянуто та проаналізовано програмне забезпечення, створене в результаті виконання роботи, призначено для поведінкового аналізу користувачів за допомогою концепції UEBA. В межах України в недостатній мірі представлені вітчизняні розробки в цій області. У роботі наведені теоретичне узагальнення й рішення наукового завдання дослідження методів поведінкового аналізу користувачів за допомогою концепції UEBA. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем поведінкового аналізу користувачів за допомогою концепції UEBA; Досліджена система поведінкового аналізу користувачів за допомогою концепції UEBA; На

основі отриманих результатів досліджень створена програмна реалізація поведінкового аналізу користувачів за допомогою концепції UEBA. Розроблені під час виконання роботи алгоритми дозволяють успішно вирішувати завдання поведінкового аналізу користувачів за допомогою концепції UEBA. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки. Розроблене програмне забезпечення має простий, дружній та зручний інтерфейс користувача, що забезпечує легкість у освоєнні роботи програмного продукту, зручність у використанні, і не потребує особливих спеціальних знань. При створені програмного забезпечення було використано об'єктно-орієнтований підхід, що відповідає сучасним тенденціям у галузі розробки комерційних програмних систем. Програма реалізована на мові високого рівня PHP фреймворк Yii2. Дана мова програмування дозволяє найбільш ефективно обробляти дані. Це дозволило мінімізувати строк розробки програмного забезпечення, і, як слід, зменшити витрати на його розробку. Запропоноване програмне забезпечення ділиться на загальне програмне забезпечення, що поставляється із засобами обчислювальної техніки й спеціальне програмне забезпечення, що спеціально розроблене для даної конкретної системи й включає програми, що реалізують її функції. Програма призначена для виконання під управлінням багатозадачної операційної системи Windows XP/Vista/7/8/10. Для підвищення рівня безпеки запропоновано застосовувати алгоритм DSA. В цілому створене програмне забезпечення підтверджує правильність використаних проектних рішень та повністю відповідає вимогам технічного завдання. Створене програмне забезпечення має потенційну можливість для подальшого вдосконалення і застосування у різних галузях.

Список літератури

1. Смирнов А.А. Анализ и сравнительное исследование перспективных направлений развития цифровых телекоммуникационных систем и сетей / А.А.Смирнов, В.В.Босько, Е.В.Мелешко // Системи обробки інформації. – Х.: ХУ ПС, 2008. – Вип.7(74). – С.120-123.
2. Смирнов А.А. Усовершенствование метода управления очередями в многопротокольных узлах телекоммуникационной сети / А.А.Смирнов, Е.В.Мелешко // Збірник тез та доповідей другої всеукраїнської науково-практичної конференції «Системний аналіз. Інформатика. Управління». Запоріжжя. Тези доповідей. Запоріжжя: КПУ, 2011.
3. Смирнов С.А. метод безопасной маршрутизации метаданных в облачные антивирусные системы / А.К. Дидык, С.А. Смирнов // Информационные технологии в управлении, образовании, науке и промышленности: монография / Под редакцией профессора В.С. Пономаренко. – Х.: Видавець Рожко С.Г., 2016. – 566 с.
4. Смирнов С. А. Сравнительные исследования математических моделей технологии распространения компьютерных вирусов в информационно-телекоммуникационных сетях / Мохамад Абу Таам Гани, А. А. Смирнов, А. В. Коваленко, С. А. Смирнов // Системи обробки інформації: зб. наук. праць. – Х.: ХУПС, 2014. – Вип. 9(125). – 105-110.
5. Смирнов С. А. Математическая модель интеллектуального узла коммутации с обслуживанием информационных пакетов различного приоритета / Мохамад Абу Таам Гани, А. А. Смирнов, Н. С. Якименко, С. А. Смирнов // Збірник наукових праць Харківського університету Повітряних Сил. – Харків: ХУПС, 2014. – Вип. 4 (41). – С. 48-52.
6. Смирнов С. А. Исследование показателей качества функционирования интеллектуальных узлов коммутации в телекоммуникационных системах и сетях / Мохамад Абу Таам Гани, А. А. Смирнов, Н. С. Якименко, С. А. Смирнов // Наука і техніка Повітряних Сил Збройних Сил України: наук. журн. – Х.: ХУПС, 2014. – № 4(17). – С. 90-95.
7. Смирнов С. А. Усовершенствованный алгоритм управления доступом к «облачным» телекоммуникационным ресурсам / Мохамад Абу Таам Гани, А. А. Смирнов, Н. С. Якименко, С. А. Смирнов // Системи обробки інформації: зб. наук. праць. – Х.: ХУПС, 2015. –Вип. 1(126). – С. 150-153.
8. Smirnov S.A. Method of controlling access to intellectual switching nodes of telecommunication networks and systems / A.A. Smirnov, Mohamad Abou Taam, S.A. Smirnov // International Journal of Computational Engineering Research (IJCER). – **Volume 5, Issue 5. –** India. Delhi. – 2015. – P. 1-7.
9. Смирнов С. А. Анализ и исследование методов управления сетевыми ресурсами для обеспечения антивирусной защиты даннях / Мохамад Абу Таам Гани, А. А. Смирнов, С. А. Смирнов // Системи озброєння і військова техніка: наук. журн. – Х.: ХУПС, 2015. – № 3(43). – С. 100-107.

10. Смирнов С. А. Исследование эффективности метода управления доступом к облачным антивирусным телекоммуникационным ресурсам / Мохамад Абу Таам Гани, А. А. Смирнов, С. А. Смирнов // Наука і техніка Повітряних Сил Збройних Сил України: наук. журн. –Х.: ХУПС, 2015. –№ 3(20). – С. 134-141.

УДК 004

В. Григор'єв, магістр гр. КІ-18М-1,4
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ ПОДОВЖЕННЯ ЖИТТЄВОГО ЦИКЛУ ЦОД

У статті розроблено програмне забезпечення, яке призначено для системи подовження життєвого циклу ЦОД. Метою розробки є дослідження та програмна реалізація системи подовження життєвого циклу ЦОД. Об'єктом дослідження є процес подовження життєвого циклу ЦОД. Предметом дослідження є методи подовження життєвого циклу ЦОД. Методи дослідження базуються на методах теорії побудови центрів обробки даних, теорії Big Data, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи подовження життєвого циклу ЦОД.
комп'ютерна інженерія, Big Data, ЦОД, кодування

Постановка проблеми. Здавалося б, увівши в експлуатацію власний центр обробки даних, його власник може нарешті зітхнути спокійно й забути як про страшний сон про всі проблеми з узгодженнями, фінансуванням, недоробками, нестиковками, строками й т.п. – адже не зазря ж стільки зусиль було вкладено в проектування й будівництво. Однак у результаті прискореного розвитку ІТ скорочується й життєвий цикл ЦОДу, тому вже через рік-два-три, незважаючи на всю передбачливість, може знадобитися його модернізація. Що вже говорити, якщо ЦОД перебуває в експлуатації більше п'яти років – за цей час вимоги й технології міняються кардинально.

До основних технічних і економічних факторів, які впливають на життєвий цикл центрів обробки даних ставляться наступні. Техніка й економіка – дві сторони однієї медалі. У кожному разі інфраструктурне рішення повинне бути оптимальним: не занадто дорогим і разом з тим поставленим завданням, що відповідають, тобто адекватним по надійності, резервуванню й масштабуванню розраховуючи на весь цикл життя центра обробки даних.

Насамперед необхідно сказати кілька слів про самий цикл. Він починається з підготовчого етапу розробки концепції й проектування ЦОДу. Основні капітальні вкладення, як і впровадження ключових технічних рішень, доводяться на етап будівництва. З початком експлуатації головною витратною статтею стають операційні витрати. Як показує досвід, далеко не всі замовники й навіть системні інтегратори здатні коректно оцінити їх заздалегідь, особливо на довгострокову перспективу.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи подовження життєвого циклу ЦОД.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи подовження життєвого циклу ЦОД.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

- Огляд існуючих систем подовження життєвого циклу ЦОД.
- Дослідження системи подовження життєвого циклу ЦОД.
- Програмна реалізація системи подовження життєвого циклу ЦОД.

Об'єктом дослідження є процес подовження життєвого циклу ЦОД.

Предметом дослідження є методи подовження життєвого циклу ЦОД.

Методи дослідження базуються на методах теорії побудови центрів обробки даних, теорії Big Data, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Залежно від сегмента – фінансовий, телекомунікаційний і корпоративного, стан інфраструктури центрів обробки даних за результатами проведених аудитів оцінюється в такий спосіб.

У компаній з першої групи цілком сучасні ЦОДи, а IT-устаткування міняється раз у три роки саме з метою підвищення ефективності. Те ж саме ставиться до інженерних систем – по 15 років ЦОДи не працюють.

Центри обробки даних компаній із другої групи мало в чому їм уступають: за рівнем оснащення нові машинні зали цілком відповідають ЦОДам Google або Facebook двох-трирічної давнини. Старі, ще не модернізовані площадки, використовувані для нішевих завдань, дійсно мають інфраструктуру, що працює по 8-10 років, і там їсти що оптимізувати.

Третій великий блок – державний і корпоративний сегменти. У тих, хто більше пов'язаний з IT, зокрема в структур електронного уряду й сервісів для населення, сучасні площадки – за останні роки побудовано декілька дуже гарних центрів обробки даних для різних державних завдань. Однак нецентралізовані площадки – серверні окремих заводів і підприємств – залишають бажати кращого. Якщо підприємство надає значення показнику PUE – а він у таких випадках найчастіше більше 2, ми допоможемо скоротити його до 1,5.

Разом з тим запити по оптимізації фінансових витрат і підвищенню надійності частіше надходять від представників перших двох сегментів. При наявності цілком функціональних ЦОДів вони зацікавлені в їхньому подальшому поліпшенні. І дійсно, ми бачимо, що фінансові установи проводять модернізацію.

Розглянемо типовий приклад. У замовника є серверна або ЦОД середнього розміру, скажемо на 20-30 стійок, і потужністю 100 кВт. Найчастіше без переривання роботи сервісів і завдань цю площадку модернізувати не можна. Тому найпростіша тактика складається в побудові нової резервної площадки. Таку топологію із двома працюючими площадками зараз можна вважати класичної. Деякі наші клієнти не обмежуються облаштованістю двох основних площадок і для виконання конкретних завдань розміщають частина стійок з устаткуванням у комерційному ЦОДі, причому так надходять навіть замовники з фінансового сегмента.

Після запровадження в дію резервна площадка стає основною, а стару можна або закрити на реорганізацію, або повністю модернізувати й дати їй друге життя, або переобладнати для інших цілей – наприклад, перетворити у фронт-офіс. Таким чином, якщо при експлуатації ЦОДу не вистачає потужностей, один з варіантів організації найбільш правильного рішення – побудувати нову площадку.

Яким образом це краще зробити? Оптимальним є використання сучасних технологій. У такому випадку вдається не тільки зменшити капітальні витрати, але й підвищити гнучкість інфраструктури, щоб наступні п'ять років навіть при зміні парку IT-устаткування можна було обійтися без заміни інженерних компонентів. До нас часто надходять запити на підбір устаткування для відносно невеликих ЦОДів. І ми радимо звернути увагу на наші нові рядні кондиціонери, парк яких обновився цього року. Це фреонові машини по 30 кВт (а в деяких режимах роботи – і до 42 кВт холодильної потужності на один блок), у них зменшилося енергоспоживання, але збільшилася холодильна потужність.

Крім того, ми пропонуємо використовувати ІБЖ Galaxy VM з літій-іонними батареями. При трохи більшій вартості вони займають на 40% менше місця, а це пряма економія капітальних витрат на дорогих площах. Ці батареї швидко перезаряджаються, тоді як типовим свинцево-кислотним після 10–15 хв роботи потрібно у вісім разів більше часу на перезарядження. При значних потужностях (0,5–1 МВт) ця різниця стає ще більш істотною –

через обмеження потужності зарядного пристрою. До того ж літій-іонні акумулятори не потрібно міняти кожні п'ять років, вони пророблять у два рази довше.

Літій-іонні батареї застосовуємо досить давно, але як типові конфігурації вивели на ринок відносно недавно. Протягом попередніх двох років був реалізований цілий ряд проектів, де вони застосовувалися й зарекомендували себе із кращої сторони. Ні в спеціальних краш-тестах, ні протягом експлуатації не було зафіксовано жодного випадку запалення або якихось інших інцидентів.

У цьому зв'язку хотілося б звернути увагу на істотну різницю між літій-іонними батареями, використовуваними в популярних пристроях для масового ринку й застосовуваними в промислових рішеннях. Усього є кілька типів літій-іонних батарей, які поєднує, мабуть, тільки використання оксиду літію для катода. У всіх же інших відносинах вони різні – починаючи від форм-фактора корпуса й щільності потужності, терміну служби й вартості й закінчуючи безпекою й сукупними експлуатаційними характеристиками.

У портативних пристроях найчастіше використовуються батареї архітектури LCO (літієво-кобальтові) с ємністю кілька ампер-годин у корпусі з фольги. У наших ІБЖ застосовуються батареї із внутрішньою структурою LMO (літієво-марганцеві) з ємністю однієї батареї 67 А/ч у твердому алюмінієвому корпусі. LMO-батареї успішно проходять спеціальний тест на перегрів (відсутність загоряння), викликаний ушкодженням стороннім предметом. Батареї цього типу давно й успішно використовуються в електромобілях, наприклад у компанії BMW.

Будь-які інвестиції повинні окупатися. Дійсно, в Україні дуже ретельно стали вважати гроші й не хочуть їх витрачати на ефемерні речі. Будь-які інвестиції повинні окупатися за три роки. Останнім часом впроваджується комплексна пропозиція по підвищенню енергоефективності ЦОДів: дивимося, наскільки добре працює ЦОД, і на підставі проведених вимірів видаємо й виконуємо ряд конкретних рекомендацій. Такі контракти вже підписані з декількома компаніями.

Після проведення модернізації зниження енергоспоживання можна відслідковувати по показниках лічильників на сайті. Мінімальне значення становить 10–15% від загального споживання інженерних і обчислювальних систем. Використовуючи 15% як орієнтир, легко підрахувати, скільки вдасться заощадити. Якщо це система ЦОДів телекомунікаційного оператора, де розміщені тисячі стійка, загальні витрати на електрику дуже великі, а виходить, впровадження даного рішення виявиться вигідним, навіть якщо економія складе всього 4–5% – сума в абсолютному вираженні виходить досить значної.

У власників невеликих ЦОДів із сумарним споживанням в 100–150 кВт оптимізація викликає інтерес, якщо вдається заощадити 20% і більше – інакше кажучи, коли модернізація окупається знову ж за три роки. Економія в 7% при строку окупності п'ять-шість років інтересу не викликає. Разом з тим мені зустрічалися всього одна-дві дійсно ефективно працюючі площадки, де вдавалося показати пряму економію всього в 5–7% – типова цифра становить 15%.

Крім прямої економії, варто враховувати й непряму. Наприклад, у компанії є площадка на 20 стійок, але через недостачу електрики або неефективного охолодження вдається використовувати сумарну кількість юнітів лише 15 з них. Ми реалізували ряд проектів, коли замовник не будував новий ЦОД, а, дотримуючись наших рекомендацій по підвищенню ефективності, вивільняв до 20% інфраструктури. У результаті кондиціонери починали краще й більше прохолоджувати, при тім що загальне споживання ЦОДу знижувалося й можна було додавати корисне навантаження.

Як бачимо, розмова вже йде в інших термінах – не про порівняння витрат з економією: крім прямої ефективності, досягається непряме поліпшення параметрів.

Життєвий цикл ЦОДів можна розбити на п'ять фаз: перша – розробка концепції, друга – проектування, третя – будівництво, четверта – експлуатація, п'ята – оптимізація. Ми активно взаємодіємо із замовником на етапі підготовки концепції, пояснюючи, що необхідно

розглядати ЦОД у цілому, а не окремі його складові, і показуючи, як взаємозалежні всі системи.

Ледве менше ми залучені в проектування, при цьому в наших самих відповідальних проектах ми готовили концепцію. За допомогою в розробці проектної документації звертаються такі відомі оператори, як DataLine і Datapro, що побудували чимало ЦОДів і мають у своєму штаті досвідчених фахівців з їхньої експлуатації. І ми робили їм підтримку при сертифікації проектів в Uptime Institute – ця послуга на нашім ринку теж затребувана.

Етап будівництва, напевно, єдиний, де послуги Schneider Electric мало затребувані на російському ринку. У нас є досвідчені партнери в цій області: якщо їм сказати, як зробити, особливо якщо видати опис із тривимірної BIM-моделлю, питань звичайно не виникає.

Фази експлуатації й оцінки єдині для замовників. Усе більше запитів надходить щодо оптимізації, коли службі експлуатації потрібно підвищити надійність роботи, оптимізувати розміщення встаткування, поліпшити ефективність систем кондиціювання й т.д. У кожному разі, щоб оцінити поточну ситуацію, потрібно провести аудита. Протягом трьох-п'яти днів наші фахівці із систем електропостачання, охолодження проводять детальні виміри, після чого формується звіт з рекомендаціями.

Іноді замовник сам займається їхнім втіленням, але частіше доручає це завдання нам. Разом з партнерами ми реалізуємо комплекс заходів щодо поліпшення інфраструктури, і ця послуга, мабуть, найбільш затребувана.

Всі ЦОДи можна розділити по потужності на дві більші групи – до 300 кВт і більше. Головна їхня відмінність: у ЦОДах на 300-400 кВт і вище застосовуються принципово інші системи охолодження, чим у ЦОДах меншій потужності.

У невеликих ЦОДах найчастіше виникає необхідність у доробці систем охолодження. Як правило, при модернізації потрібно встановити ще один кондиціонер або реорганізувати встаткування для забезпечення ефективного охолодження.

У другу чергу виникають завдання в рамках системи електропостачання. При модернізації електрики найчастіше залишають наявне ІБЖ – реорганізується інша система електропостачання: установлюється додаткове щитове встаткування, переробляються схеми живлення ІТ-устаткування для організації живлення по двох променях і т.п.

Третім завданням, всі частіше виникаючої в рамках модернізації об'єктів, є впровадження системи моніторингу, причому часто вона реалізується незалежно від систем електропостачання й охолодження. При цьому передбачається установка датчиків температури й вологості, PDU із засобами контролю або урізань в існуючі щити, що дозволяє одержати повну картину енергоспоживання.

Це три типові завдання модернізації для ЦОДів потужністю менше 300 кВт.

У могутніших ЦОДах в основному застосовується чіллерне охолодження. Як правило, схема кондиціювання вже передбачає можливість масштабування, тому встановити ще одну систему набагато простіше. При реорганізації енергопостачання з'являється потреба в нарощуванні потужності ІБЖ і підвищенні щільності потужності на стійку. Можуть виникати й нетривіальні завдання – наприклад, коли кластер в 20 стійок по 4,5 кВт треба трансформувати в 10 стійок по 20 кВт плюс ще 10 стійок по 7 кВт, – оскільки, крім живлення, необхідно забезпечити охолодження.

Як правило, у великих ЦОДах уже є та або інша система моніторингу. Іноді вона реалізується за допомогою SCADA-систем з відповідними термодатчиками й датчиками живлення, в інших випадках – на базі ІТ-систем з використанням вимірювальних PDU і т.п. Проте при модернізації ми намагаємося збільшити кількість датчиків: три-чотири роки тому замовники встановлювали чотири датчики температури на холодний коридор і два датчики на гарячий. Як показують обстеження ЦОДів, цього недостатньо, оскільки виявити локальні точки перегріву не вдається. Відповідно, замість двох-чотирьох датчиків на ряд установлюється по двох-трьох на стійку.

Як правило, у компанії є департаменти служби експлуатації – адміністративно-господарський («енергетики», «холодильщики», «агошники»), відповідальний за зміст

приміщення, підведення електрики й холоду, і підрозділи, що забезпечує роботу IT-устаткування («айтишники»).

І часто виникає питання про те, де проходить границя відповідальності. Зона відповідальності АГВ може доходити до клем живлення стійки (умовно – до PDU), а все, що після цього, – справа IT-відділу. Але бувають і інші розмежування. Для проведення робіт з модернізації потрібно залучати представників обох департаментів. Тому проблема частіше виникає не в нас, а в наших партнерів: донести й пояснити важливість розв'язуваних завдань керівникам обох підрозділів.

Якщо хто-небудь із них не зацікавлений у модернізації, гарного результату не буде. Без допомоги «айтишників» не можна правильно організувати повітряні потоки усередині стійки, тому що вони повинні затвердити розташування елементів, що блокують або, навпаки, що організують подачу холодного повітря для кожної одиниці IT-устаткування. А без допомоги «агошників» не вдасться переналаштувати кліматичне встаткування, реорганізувати живлення або хоча б одержати доступ до щита електропостачання для виконання вимірів.

Як бачите, мова не про конфлікти, а про взаємний інтерес. Співробітники повинні розуміти, з якою кінцевою метою виконується процес. Якщо є, наприклад, рекомендації посібника з надання взаємодопомоги, усе робиться дуже добре.

Те, про що я розповідав, – це класична служба експлуатації. У нас є трохи клієнтів, у яких у службі експлуатації виділяється ще один підрозділ, відповідальне за «корисний простір» (white space): за приміщення ЦОДу, де встановлюються стійки, відповідає окрема команда (data center managers). У різних компаніях у штаті цього підрозділу значиться від 7 до 15 чоловік. Вони відповідають за все, що перебуває усередині ЦОДу: розміщення встаткування, охолодження, резервування подачі живлення від щитів до стійок, – але не за зовнішній периметр (скажемо, за ІБЖ, установлені в більших щитові), тому що є споживачами цих послуг. Наявність такого підрозділу – ідеальний варіант, оскільки його керівництво й кожний співробітник безпосередньо зацікавлені в проведенні всіх робіт, про які ми говорили. Це самі вдячні замовники, адже ми допомагаємо їм вирішувати їх самі насущні проблеми.

Розробка структурної схеми

На рисунку 1 зображена структурна схема системи. З неї бачимо, що розроблена система подовження життєвого циклу ЦОД з наступних основних функціональних блоків:

– сам носій інформації у ЦОД;

– кодер циклічного коду, який використовується, коли відбувається запис інформації у ЦОД на носій інформації у ЦОД, при цьому необхідно враховувати, що об’єм інформації у ЦОД, яка записується на носій інформації у ЦОД, повинна бути меншою, ніж об’єм носія інформації у ЦОД, в зв’язку, з тим, що коди циклічного коду відносяться до кодів з надмірністю, за рахунок якої й відбувається кодування;

– декодер циклічного коду, який використовується при читанні даних с відповідного носія інформації у ЦОД;

– файли для перешкодостійкого збереження;

– відновлені файли.

Розглянемо більш детально перераховані функціональні блоки кодування та декодування за допомогою циклічного кодування.

Блок кодування складається з наступних підблоків:

– Модуль формування томів для відновлення.

– Модуль формування закодованих даних шляхом множення інформаційної та породжуючої матриці.

– Перевірочна матриця.

– Породжуюча матриця.

– Інформаційна матриця.

Рисунок 1 – Структурна схема системи

Блок декодування складається з наступних підблоків:
– Інформаційна матриця.
– Перевірочна матриця.
– Матриця локаторів помилок.
– Модуль перевірки цілісності та пошуку помилок.
– Модуль виправлення помилок.
– Модуль перетворення томів для відновлення в початкові дані.

Коди циклічного коду базуються на спеціальному розділі математики – полях Галуа (GF) або кінцевих полях. Арифметичні дії (+, -, х, / і т.д.) над елементами кінцевого поля дають результат, що також є елементом цього поля. Кодер та декодер циклічного коду повинні вміти виконувати ці арифметичні операції. Ці операції для своєї реалізації вимагають спеціального устаткування або спеціалізованого програмного забезпечення.

Кодове слово циклічного коду формується із залученням спеціального полінома. Всі коректні кодові слова повинні ділитися без залишку на ці утворюючі поліноми. Загальна форма утворюючого полінома має вигляд:

$$g(x) = (x\text{-}a^{i})(x\text{-}ai^{+1})\ldots(x\text{-}a^{i+2t}),$$

а кодове слово формується за допомогою операції:

$$c(x) = g(x)i(x),$$

де – $g(x)$ є утворюючим поліномом;
– $i(x)$ являє собою інформаційний блок;
– $c(x)$ – кодове слово, що називається простим елементом поля.

$2t$ символів парності в кодовому слові циклічного коду визначаються з наступного співвідношення:

$$p(x) = i(x)\cdot x^{n-k} \bmod g(x).$$

Перейдемо до розгляду іншого функціонального блоку – декодеру циклічного коду.

Декодер працює наступним чином.

Введемо позначення:

– $r(x)$ – Отримане кодове слово.

– S_i – Синдроми.
– $L(x)$ – Поліном локації помилок.
– X_i – Положення помилок.
– Y_i – Значення помилок.
– $c(x)$ – Відновлене кодове слово.
– v – Число помилок.

Отримане кодове слово r(x) являє собою вихідне (передане) кодове слово c(x) плюс помилки: $r(x) = c(x) + e(x)$.

Декодер циклічного коду намагається визначити позицію й значення помилки для числа t помилок (або $2t$ втрат) і виправити помилки й втрати.

Обчислення синдрому

Обчислення синдрому схоже на обчислення парності. Кодове слово циклічного коду має $2t$ **синдромів**, це залежить тільки від помилок (а не переданих кодових слів). Синдроми можуть бути обчислені шляхом підстановки $2t$ коріння утворюючого полінома $g(x)$ в $r(x)$.

Знаходження позицій символьних помилок

Це робиться шляхом рішення системи рівнянь із t невідомими. Існує кілька швидких алгоритмів для рішення цього завдання. Ці алгоритми використовують особливості структури матриці кодів циклічного коду й сильно скорочують необхідну обчислювальну потужність. Робиться це у два етапи:

1. Визначення полінома локації помилок

Це може бути зроблене за допомогою алгоритму Berlekamp-Massey або алгоритму Евкліда. Алгоритм Евкліда використовується частіше на практиці, тому що його легше реалізувати, однак, алгоритм Berlekamp-Massey дозволяє одержати більш ефективну реалізацію встаткування й програм.

2. Знаходження кореня цього полінома. Це робиться із залученням алгоритму пошуку Chien.

Знаходження значень символьних помилок

Тут також потрібно вирішити систему рівнянь із t невідомими. Для рішення використовується швидкий алгоритм Forney.

Розглянувши усі блоки функціональної схеми перейдемо до розгляду діаграми взаємодії процесів, які відбуваються у системі.

Опис циклічного коду, який використовується для подовження життєвого циклу ЦОД

Опишемо процес кодування та декодування інформації у ЦОД за допомогою циклічного кодування.

Циклічним кодом називається лінійний блоковий (n,k)-код, що характеризується властивістю циклічності, тобто зрушення вліво на один крок будь-якого дозволеного кодового слова дає також дозволене кодове слово, що належить цьому ж коду й у якого, множина кодових слів представляється сукупністю багаточленів ступеня (n-1) і менш, що діляться на деякий багаточлен $g(x)$ ступеня $r = n$-k, що є співмножником двочлена x^n+1.

Багаточлен $g(x)$ називається породжуючим.

Як треба з визначення, у циклічному коді кодові слова представляються у вигляді багаточленів:

$$a(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \ldots + a_1x^1 + a_0x^0, \quad (1)$$

Де n – довжина коду; a_i – коефіцієнти з поля $GF(q)$.

Якщо код побудований над полем $GF(2)$, то коефіцієнти приймають значення 0 або 1 і код називається двійковим.

Наприклад, якщо код побудований над полем $GF(q)=GF(2^3)$, що є розширенням $GF(2)$ по модулі багаточлена, що не *приводиться,* $f(z)=z^3+z+1$, а елементи цього поля мають вигляд, представлений у таблиці 1.

То коефіцієнти $\alpha_i(x)$ приймають значення елементів цього поля й тому вони самі відображаються у вигляді багаточленів наступного виду:

$$\alpha_i(z) = a_{m-1} \cdot z^{m-1} + a_{m-2} \cdot z^{m-2} + \ldots + a_1 \cdot z^1 + a_0 \cdot z^0, \quad (2)$$

де m – ступінь багаточлена, по якому отримане розширення поля *GF*(2);

α_i – коефіцієнти, що приймають значення елементів *GF*(2), тобто 0 і 1. Такий код називається *q*-ним.

Таблиця 1 – Елементи поля *GF*(2)

0	000	0	α^3	011	Z+1
α^0	001	1	α^4	110	Z^2+Z
α^1	010	Z	α^5	111	Z^2+Z+1
α^2	100	Z^2	α^6	101	Z^2+1

Довжина циклічного коду називається примітивної й сам код називається примітивним, якщо його довжина $n= q^{m-1}$ на *GF*(*q*).

Якщо довжина коду менше довжини примітивного коду, то код називається вкороченим або непримітивним.

Як треба з визначення загальна властивість кодових слів циклічного коду – це їхня подільність без остачі на деякий багаточлен *g*(*x*), називаний породжуючим.

Результатом ділення двочлена x^n+1 на багаточлен *g*(*x*) є перевірочний багаточлен *h*(*x*).

Матричне завдання кодів

Циклічний код може бути заданий породжуючий й перевірочною матрицями. Для їхньої побудови досить знати породжуючий *g*(*x*) і перевірочний *h*(*x*) багаточлени.

Для несистематичного циклічного коду матриці будуються циклічним зрушенням породжуючого й перевірочного багаточленів, тобто шляхом їхнього множення на *x*:

$$G_{(n,k)} = \begin{vmatrix} g(x) \\ x \cdot g(x) \\ x^2 \cdot g(x) \\ \bullet\bullet\bullet \\ x^{k-1} \cdot g(x) \end{vmatrix},$$

та:

$$H_{(n,k)} = \begin{vmatrix} h(x) \\ x \cdot h(x) \\ x^2 \cdot h(x) \\ \bullet\bullet\bullet \\ x^{r-1} \cdot h(x) \end{vmatrix}.$$

При побудові матриці $H_{(n,k)}$ старший коефіцієнт багаточлена *h*(*x*) розташовується праворуч.

Для систематичного циклічного коду матриця $G_{(n,k)}$ визначається з вираження:

$$G_{(n,k)} = \left| I_k, R_{k,r} \right|, \quad (3)$$

де I_k – одинична матриця;

$R_{k,r}$ – прямокутна матриця.

Рядки матриці $R_{k,r}$ визначаються з виражень:

$$r_i(x) = R_{g(x)} \left| a_i(x) \cdot x^r \right|, \quad (4)$$

або:

$$r_i(x) = R_{g(x)}\left[x^{n-i}\right], \tag{5}$$

де $a_i(x)$ – значення і-т*ого* рядка матриці I_k;

i – номер рядка матриці $R_{k,r}$.

Використовуючи вираження:

$$r_i(x) = R_{g(x)}\left[x^{n-i}\right], \tag{6}$$

одержимо той же результат.

Рядки матриці $G_{(n,k)}$ можна визначити безпосередньо з вираження:

$$g_i(x) = a_i(x)\cdot x^r + r_i(x), \tag{7}$$

де:

$$r_i(x) = R_{g(x)}\left[a_i(x)\cdot x^r\right]. \tag{8}$$

Перевірочна матриця в систематичному виді будується на основі матриці $G_{(n,k)}$, а саме:

$$H_{(n,k)} = \left|R^T_{k,r}, I_r\right|, \tag{9}$$

де I_r – одинична матриця;

$R^T_{k,r}$ – матриця з $G_{(n,k)}$ у транспонованому виді.

Одна з основних задач, що коштують перед розроблювачами пристроїв захисту від помилок при передачі дискретних повідомлень по каналах зв'язку є вибір багаточлена, породжуючий, $g(x)$ для побудови циклічного коду, що забезпечує необхідну мінімальну кодову відстань для гарантійного виявлення й виправлення t-кратних помилок.

Існують спеціальні таблиці на вибір $g(x)$ залежно від пропонованих вимог до коригувальних можливостей коду. Однак у кожного циклічного коду є свої особливості формування $g(x)$. Тому при вивченні конкретних циклічних кодів будуть розглядатися відповідні способи побудови $g(x)$.

Задача кодування полягає у формуванні по інформаційних словах $a(x)$ кодових слів (x) циклічного (n,k)-коду, що по своїй структурі може бути несистематичним і систематичним.

Формування кодових слів несистематичного коду полягає в множенні багаточлена $a(x)$, що відображає інформаційну послідовність довжини k, на породжуючий багаточлен, тобто $(x)=a(x)\times g(x)$. Формування кодових слів систематичного коду полягає в перетворенні інформаційної послідовності $a(x)$ відповідно до вираження $(x)=a(x)\oplus x^r+r(x)$.

Перевірочна послідовність $r(x)$ визначається двома способами:

– при використанні "класичного" способу кодування:

$$r(x) = R_{g(x)}\left[a(x)\cdot x^r\right], \tag{10}$$

– при використанні способу кодування, рекомендованого МККТТ:

$$r(x) = \overline{R}_{g(x)}\left[a(x)\cdot x^r + x(1)^{r-1}\cdot x^k\right], \tag{11}$$

де $x(1)^{r-1}$ – одиничний багаточлен ступеня $(r-1)$.

Зазначені вище математичні операції виконують кодерии несистематичного й систематичного кодів.

Способи декодування з виявленням помилок

Процедура декодування циклічного коду з виявленням помилок, за аналогією із процесом кодування, використовує два способи:

– При кодуванні "класичним" способом декодування засноване на використанні властивості подільності без остачі кодового багаточлена (x) циклічного (n,k)-коду на породжуючий багаточлен $g(x)$. Тому алгоритм декодування містить у собі ділення прийнятого кодового слова, описуваного багаточленом $g'(x)$ на $g(x)$, обчислення й аналіз остачі $r(x)$. Якщо $r(x)=0$, то прийняте кодове слово вважається неспотвореним. Якщо $r(x)<>0$,

то прийняте кодове слово стирається й формується сигнал "помилка".

– При кодуванні способом МККТТ декодування засноване на властивості одержання певної контрольної остачі $R_0(x)$ при діленні прийнятого кодового багаточлена (x) на породжуючий багаточлен. Тому, якщо отриманий при діленні остача $\overline{r(x)} = R_0(x)$, то прийняте кодове слово вважається неспотвореним. Якщо остача $\overline{r(x)} \neq R_0(x)$, то прийняте кодове слово стирається й формується сигнал "помилка". Значення контрольної остачі визначається з вираження:

$$R_0(x) = R_{g(x)}\left[x(1)^{r-1} \cdot x^k\right]. \quad (12)$$

Способи декодування з виправленням помилок і схемна реалізація декодувальних пристроїв

Декодування циклічного коду в режимі виправлення помилок можна здійснювати різними способами. Нижче викладаються два способи, що є найбільш простими.

В основу першого способу покладене використання таблиці синдромів (декодування), у якій кожному багаточлену або зразку помилок $e_i(x)$, відповідає певний синдром $S_i(x)$, що представляє остачу від ділення прийнятого кодового слова $\upsilon_i'(x)$ й відповідного йому $e_i(x)$ на $g(x)$. Процедура декодування наступна. Прийняте кодове слово $\upsilon_i'(x)$ ділиться на $g(x)$, визначається $S_i(x)$ і відповідний йому багаточлен $e_i(x)$, а потім $\upsilon_i'(x)$ підсумується з $e_i(x)$. У результаті одержуємо виправлене кодове слово, тобто:

$$\upsilon_i(x) = \upsilon_i'(x) + e_i(x). \quad (13)$$

До складу декодера входять: обчислювач синдрому (ВР), два регістри зрушення *RG*1 і *RG*2, постійний запам'ятовувальний пристрій (ПЗП), що містить $\sum_{i=1}^{t_u} C_n^i$ слова довжини n, що відповідають багаточленам помилок $e_i(x)$.

Прийняте кодове слово $\upsilon_i'(x)$ надходить на вхід обчислювача синдрому, де здійснюється ділення його на $g(x)$ і формування $S_i(x)$, і одночасно – на вхід *RG*2, де $\upsilon_i'(x)$ накопичується. Синдром $S_i(x)$ використовується як адреса, по якому із ПЗП в регістр *RG*1 записується $e_i(x)$, що відповідає синдрому $S_i(x)$. Перераховані операції завершуються за n тактів. Протягом наступних n тактів відбувається заелементне підсумовування вмісту *RG*2 і *RG*1, тобто операція:

$$\upsilon_i(x) = \upsilon_i'(x) + e_i(x), \quad (14)$$

і виправлення помилок.

В основі другого способу виправлення помилок, що дозволяє значно скоротити об'єм використовуваних табличних синдромів і істотно спростити схему декодера, лежать наступні положення:

1. Синдром $S_i(x)$, що відповідає прийнятому кодовому слову дорівнює остачі від ділення $\upsilon_i'(x)$ на $g(x)$, а також остачі від ділення відповідного багаточлена помилок $ei(x)$ на $g(x)$, тобто:

$$S_i(x) = R_{g(x)}\left[\upsilon_i'(x)\right] = R_{g(x)}\left[e_i(x)\right]. \quad (15)$$

2. Якщо $S_i(x)$ відповідає $\upsilon_i'(x)$ й $e_i(x)$, то $x \in S_i(x)$ є синдромом, що відповідає:

$$R_{g(x)}\left[x \cdot S_i(x)\right] = R_{g(x)}\left[x \cdot \upsilon_i'(x) \bmod(x^n - 1)\right] = R_{g(x)}\left[x \cdot e_i(x) \bmod(x^n - 1)\right], \quad (16)$$

і:

$$x \cdot \upsilon_i'(x) \bmod(x^n - 1), \quad (17)$$

або:

$$x \cdot e_i(x) \bmod(x^n - 1). \quad (18)$$

3. При виправленні помилок використовуються синдроми зразків помилок тільки з ненульовим коефіцієнтом у старшому розряді.

Тому при реалізації цього способу множина всіх зразків помилок розбивається на класи еквівалентності. Кожний клас представляє циклічне зрушення одного зразка помилок, а синдром цього класу відповідає зразку помилок з ненульовим старшим розрядом. Якщо обчислений синдром належить одному із класів еквівалентності зразків помилок, що виправляються, то старший символ кодового слова виправляється. Потім прийняте слово й синдром циклічно зрушується, а процес знаходження в попередній по старшинству позиції повторюється.

Для виправлення помилок, що належать даному класу еквівалентності, потрібно зробити *n* циклічних зрушень.

Найпростішим є декодер Меггіта. До складу декодера входять: обчислювач синдрому, що здійснює ділення кодового слова $\upsilon'(x)$ на $g(x)$ і формування відповідного синдрому; блок декодерів (ДК), що налаштований на синдроми всіх зразків помилок, що виправляються, з ненульовими старшими розрядами; регістр зрушення *RG*.

При надходженні на вхід схеми кодового слова $\upsilon'(x)$ його символи заповнюють регістр *RG*, а в обчислювачі формується відповідний синдром $S_i(x)$. Обчислений синдром рівняється з усіма табличними синдромами, закладеними в схему блоку ДК, і у випадку збігу з одним з них на його виході формується сигнал, що виправляє помилковий символ, що перебуває в старшому розряді регістра. Після цього вміст обчислювача й *RG* циклічно зрушується на один крок. Це зрушення реалізує операції $R_{g(x)}[x \cdot S_i(x)]$ й $x \cdot \upsilon'(x) \bmod(x^n - 1)$. Якщо новий синдром збігається з одним з табличних синдромів, то це означає, що відбулася помилка в другому по старшинству символі кодового слова, що, перейшовши в старший розряд *RG*, виправляється. Потім виробляється нове циклічне зрушення на одну позицію й нову перевірку на збіг синдромів. Після повторення цього процесу *n* раз в *RG* буде сформоване виправлене кодове слово. Введення зворотного зв'язка для *RG* не обов'язково, тому що в процесі виправлення помилок символи кодового слова надходять на вихід декодера.

При декодуванні циклічних кодів використовуються багаточлен помилок $e(x)$ і синдромний багаточлен $S(x)$.

Багаточлен помилок ступеня не більше (n-1) визначається з вираження:

$$e(x) = \upsilon'(x) + \upsilon(x), \quad (19)$$

де $\upsilon'(x)$ и $\upsilon(x)$ – багаточлени, що відображають відповідно прийняте (з помилкою) і передане кодові слова.

Ненульові коефіцієнти в $e(x)$ займають позиції, які відповідають помилкам.

Синдромний багаточлен, використовуваний при декодуванні циклічного коду, визначається як остача від ділення прийнятого кодового слова на породжуючий багаточлен, тобто:

$$S_i(x) = R_{g(x)}[\upsilon'(x)], \quad (20)$$

або:

$$S_i(x) = R_{g(x)}[\upsilon'(x) + e_i(x)] = R_{g(x)}[e_i(x)]. \quad (21)$$

Отже, синдромний багаточлен залежить безпосередньо від багаточлена помилок $e(x)$.Це положення використовується при побудові таблиці синдромів, застосовуваної в процесі декодування. Ця таблиця містить список багаточленів помилок і список відповідних синдромів, обумовлених з вираження:

$$S_i(x) = R_{g(x)}\left[e_i(x)\right] \tag{22}$$

Таблиця 2 – Список багаточленів помилок і список відповідних синдромів

(x)	$S(x)$
1	$R_{g(x)}[1]$
X	$R_{g(x)}[x]$
X^2	$R_{g(x)}[x^2]$
X+1	$R_{g(x)}[x+1]$
X^2+1	$R_{g(x)}[x^2+1]$

У процесі декодування по прийнятому кодовому слову обчислюється синдром, потім у таблиці перебуває відповідний багаточлен $e(x)$, підсумовування якого із прийнятим кодовим словом дає виправлене кодове слово, тобто:

$$v_i(x) = v_i'(x) + e_i(x). \tag{23}$$

Перераховані багаточлени $v(x), v'(x), g(x), h(x), e(x)$ и $S(x)$ можна складати, множити й ділити, використовуючи відомі правила алгебри, але із приведенням результату по mod 2, а потім по mod x^n+1, якщо ступінь результату перевищує ступінь (n-1).

При побудові й декодуванні циклічних кодів у результаті ділення багаточленів звичайно необхідно мати не частка, а остача від ділення.

Висновок. У статті розглянуто та проаналізовано програмне забезпечення, яке призначено для системи системи подовження життєвого циклу ЦОД. В межах України в недостатній мірі представлені вітчизняні розробки в цій області. У роботі наведені теоретичне узагальнення й рішення наукового завдання дослідження методів подовження життєвого циклу ЦОД. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем подовження життєвого циклу ЦОД; Досліджена система подовження життєвого циклу ЦОД; На основі отриманих результатів досліджень створена програмна реалізація системи подовження життєвого циклу ЦОД. Розроблені під час виконання роботи алгоритми дозволяють успішно вирішувати завдання подовження життєвого циклу ЦОД. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки. Розроблене програмне забезпечення має простий, дружній та зручний інтерфейс користувача, що забезпечує легкість у освоєнні роботи програмного продукту, зручність у використанні, і не потребує особливих спеціальних знань. При створені програмного забезпечення було використано об'єктно-орієнтований підхід, що відповідає сучасним тенденціям у галузі розробки комерційних програмних систем. Програма реалізована на мові високого рівня Visual C#. Дана мова програмування дозволяє найбільш ефективно обробляти дані. Це дозволило мінімізувати строк розробки програмного забезпечення, і, як слід, зменшити витрати на його розробку. Запропоноване програмне забезпечення ділиться на загальне програмне забезпечення, що поставляється із засобами обчислювальної техніки й спеціальне програмне забезпечення, що спеціально розроблене для даної конкретної системи й включає програми, що реалізують її функції. Даються необхідні рекомендації з установки розробленого програмного забезпечення. Для підвищення рівня безпеки запропоновано застосовувати алгоритм ДСТ Р 34.10-2012.

Список літератури

1. Jui-Fa Chen, Wei-Chuan Lin. A Message Interchange Protocol based on Routing Information Protocol in a Virtual World / Proceedings of the 19th International Conference on Advanced Information Networking and Applications (AINA'05) – 2005, P. 201-208.

2. Босько В.В. Анализ и сравнительное исследование перспективных направлений развития цифровых телекоммуникационных систем и сетей / Смирнов А.А., Босько В.В., Мелешко Е.В. // Системи обробки інформації. – Х.: ХУ ПС, 2008. – Вип.7(74). – С.120-123.
3. Босько В.В. Разработка методики оценки середнего времени обслуживания информационных пакетов в телекоммуникационной сети / Смирнов А.А., Босько В.В., Мелешко Е.В. // Системи управління, навігації та зв'язку. – Київ: ДП «Центральний науково-дослідний інститут навігації і управління», 2009. – Вип. 2(10). – С.162-165.
4. Босько В.В. Разработка математической модели процесса динамического управления маршрутизацией данных в телекоммуникационной сети / Смирнов А.А., Босько В.В. // Системи управління, навігації та зв'язку. – К.: ДП «ЦНДІ навігації і управління», 2009. – Вип. 3(11). – С.208-210.
5. Босько В.В. Разработка метода определения оптимального множества путей передачи информации в телекоммуникационной сети / Смирнов А.А., Босько В.В. // Збірник наукових праць. – Х.: ХУПС, 2009. – Вип. 3(21). – С.102-108.
6. В.В. Босько. Разработка метода прогнозирования поведения информационного потока в телекоммуникационной сети // Збірник наукових праць. Харківського університету Повітряних Сил: – Х.:ХУ ПС, – 2010.-Вип. 3 (25) .- С.126-130.
7. Босько В.В. Исследование особенностей построения современных телекоммуникационных систем и сетей / Смирнов А.А., Босько В.В. // Проблемы информатики и моделирования. Материалы восьмой международной научно-технической конференции 26-28 ноября. – Х.: НТУ "ХПИ", 2008. – С.54.
8. Босько В.В. Исследование влияния времени мониторинга телекоммуникационной сети на точность прогнозирования поведения трафика / Смирнов А.А., Босько В.В. // Перша міжнародна науково-практична конференція "Проблеми й перспективи розвитку IT-індустрії" м. Харків , 18-19 листопада 2009р. – С.198-200.
9. Босько В.В. Анализ математических моделей телекоммуникационной сети / Смирнов А.А., Босько В.В. // Проблемы информатики и моделирования. Материалы девятой международной научно-технической конференции 26-28 ноября. – Х.: НТУ "ХПИ", 2009. – С.52-53.
10. Босько В.В. Метод повышения оперативности передачи данных в телекоммуникационной сети / Смирнов А.А., Босько В.В. // Збірник тез доповідей науково-практичної конференції "Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку" 24-25 березня. – Х.: АВВ МВС України, 2010. – С.54.
11. Босько В.В. Динамическое управление процессом маршрутизации данных в телекоммуникационной сети / Смирнов А.А., Босько В.В. // Тези доповідей Міжнародної науково-практичної конференції м. Вінниця, Україна 19-21 травня 2010 року. – Вінниця: ВНТУ, 2010. – С.231-232.

УДК 004

В. Грудік, магістр гр. КІ-18М-1,4
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ ВІРТУАЛІЗАЦІЇ МЕРЕЖІ НА БАЗІ ЗАСТОСУВАННЯ ТЕХНОЛОГІЇ VXLAN OFFLOAD

У статті розроблено програмне забезпечення, яке призначено для віртуалізації мережі на базі застосування технології VXLAN offload. Метою розробки є дослідження та програмна реалізація віртуалізації мережі на базі застосування технології VXLAN offload. Об'єктом дослідження є процес віртуалізації мережі на базі застосування технології VXLAN offload. Предметом дослідження є методи віртуалізації мережі на базі застосування технології VXLAN offload. Методи дослідження базуються на методах віртуалізації мережі, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація віртуалізації мережі на базі застосування технології VXLAN offload. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.
комп'ютерна інженерія, віртуалізація мережі, VXLAN offload

Постановка проблеми. За винятком хіба що самих великих хмарних провайдерів всі інші впроваджують SDN в урізаному виді, при цьому широке застосування одержують

накладені мережі на основі технологій VXLAN, NVGRE і GENEVE. Через центри обробки даних пересилається все більші обсяги трафіку. Однак проблема не тільки й не стільки в збільшенні обсягів, скільки в зміні його природи: основну частку становить хмарний трафік. Саме тому мережа повинна відповідати вимогам до хмарної інфраструктури, тобто бути надзвичайно гнучкою й адаптуємою. Програмно обумовлені мережі саме й дозволяють створити динамічну й програмувальну мережну інфраструктуру. Якщо споконвічно рішення SDN знаходили застосування в мережах ЦОДів великих хмарних провайдерів, то тепер вони використовуються в усі більшому числі корпоративних центрів обробки даних, і залишається тільки зрозуміти, яке рішення краще вибрати. Технології програмувальних мереж порівняно молоді, а віртуалізація мережі може бути реалізована декількома способами. Багато великих компаній мають значну інстальовану базу мережного встаткування, що не підтримує OpenFlow. Щоб такі замовники могли скористатися перевагами мережної віртуалізації / SDN, цілий ряд вендорів пропонують рішення для розгортання накладених мереж. Такий підхід припускає організацію логічної мережі поверх наявної фізичної інфраструктури. Переносячи інтелект на границю мережі, накладені мережі дозволяють одержати функціональність програмно обумовлених мереж без заміни фізичного мережного встаткування (хоча, через зростаючі вимоги до пропускної здатності й зміни картини трафіку, така заміна бажана або навіть необхідна).

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні віртуалізації мережі на базі застосування технології VXLAN offload.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація віртуалізації мережі на базі застосування технології VXLAN offload.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем віртуалізації мережі на базі застосування технології VXLAN offload.

– Дослідження віртуалізації мережі на базі застосування технології VXLAN offload.

– Програмна реалізація віртуалізації мережі на базі застосування технології VXLAN offload.

Об'єктом дослідження є процес віртуалізації мережі на базі застосування технології VXLAN offload.

Предметом дослідження є методи віртуалізації мережі на базі застосування технології VXLAN offload.

Методи дослідження базуються на методах віртуалізації мережі, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Ряд експертів характеризують поточну ситуацію в мережній галузі як «критичну й революційну». Домінуючі на ринку закриті (пропрієтарні) рішення представляють для додатків «чорні ящики», а сумісність рішень різних вендорів забезпечується в найкращому разі на рівні інтерфейсів. Мережі є надто складними, що утрудняє їхнє масштабування й керування ними, знижує їхня надійність. Очевидно, що це гальмує подальший розвиток мереж і функціонуючих у них додатків [1].

Основними передумовами до появи концепцій «програмно обумовлених» (або «програмно конфігуруємі») мереж (Software-Defined Networking, SDN) і віртуалізації мережних функцій (Network Function Virtualization, NFV) є, насамперед, швидкий ріст трафіку даних і кількості підключених до мережі пристроїв.

При цьому сам трафік стає різнорідним – якщо наприкінці 1990-х рр. його основу становило пересилання даних і файлів, що не вимагають особливих вимог до каналу, за винятком швидкості передачі даних, те вже до середини 2000-х на перше місце вийшли питання забезпечення якості сервісу (QoS), мінімальної затримки в каналі (latency) та ін. Це, у першу чергу, пов'язане зі зміною структури користувальницького трафіку, у якому стали переважати комунікації в реальному часі (Real Time Communications, RTC) – VoIP,

відеосервіси та ін. В операторів виникла реальна потреба в динамічної приоритезації трафіку. Наприклад, у деяких випадках пріоритет повинен бути зроблений для ftp-протоколу, в інші – для SIP і навпаки.

В області мобільного зв'язку установка додаткових макростільник (базових станцій) після досягнення певного порога щільності їхнього розміщення вже не дає істотного приросту пропускної здатності і ємності мереж радіодоступу (RAN), тому наступним етапом стає використання малих стільник (фемто- і пікосот). У результаті конфігурування великомасштабних мереж перетворюється в складне завдання й вимагає серйозних змін принципів побудови, експлуатації й керування мереж і керуванню ними.

Концепції SDN і NFV

SDN і віртуалізація мережних функцій (NFV) на думку аналітиків підривають ринок традиційних мережних продуктів і загрожують дохідному бізнесу таких компаній як Cisco,Juniper Networks і Hewlett-Packard на встаткуванні. SDN і NFV переносять функції керування й визначення завдань мережі з дорогого встаткування в ПЗ, що може працювати на більше дешевих системах, що випускаються масово. Ціль полягає в створенні більше рухливих, програмувальних і автоматизованих мереж.

Ключові принципи програмно-конфігуруємих мереж – поділ процесів передачі й керування даними, централізація керування мережею за допомогою уніфікованих програмних засобів, віртуалізація фізичних мережних ресурсів. Протокол OpenFlow, що реалізує незалежний від виробника інтерфейс між логічним контролером мережі й мережним транспортом, є однієї з реалізацій концепції програмно-конфігуруємої мережі й уважається рушійною силою її поширення й популяризації.

Основна суть SDN складається у фізичному поділі рівня керування мережею (network control plane) від рівня передачі даних (forwarding functions) за рахунок переносу функцій керування (маршрутизаторами, комутаторами й т.п.) у застосунки, що працюють на окремому сервері (контролері).

У результаті повинна вийти гнучка, керована, адаптивна й економічна архітектура, що здатна ефективно адаптуватися під передачу великих потоків різнорідного трафіку.

Основні ідеї SDN включають:

- поділ проходження трафіку (data plane) і сигналізацію/керування (control plane);
- істотне спрощення мережних елементів рівня data plane;
- єдиний, уніфікований, незалежний від постачальника інтерфейс між рівнем керування й рівнем передачі даних;
- логічно централізоване керування мережею, здійснюване за допомогою контролера із установленою мережною операційною системою й реалізованими поверх мережними додатками;
- віртуалізація фізичних ресурсів мережі.

Базові ідеї SDN були сформульовані фахівцями університетів Стенфорда й Берклі ще в 2006 р., і ініційовані ними дослідження знайшли підтримку у великих операторів і інтернет компаній (Google, Deutsche Telekom, Facebook, Microsoft, Verizon і Yahoo). У результаті в березні 2011 р. був утворений консорціум Open Networking Foundation (ONF), склад якого швидко розширюється, в 2013 р. у нього ввійшли більше 100 компаній, включаючи Brocade, Citrix, Oracle, Dell, Ericsson, HP, IBM, Marvell, NEC, VMware і ін.

ONF розвиває, насамперед, протокол OpenFlow, що реалізує взаємодія контролера з мережними пристроями, однак ряд членів цієї організації зацікавлений у більше універсальних специфікаціях. У квітні 2013 р. компанії Cisco, Citrix і IBM сформували структуру OpenDaylight.org, ціль якої – випуск відкритого загальнодоступного стандарту SDN, заснованого на вільному ПЗ.

Таким чином, SDN намагається розділити дві площини – керування мережею й транспорт, і в підсумку забезпечити централізацію керування розподіленої мережі з метою більше ефективного використання ресурсів і автоматизації керування мережними сервісами. NFV же зосереджена на оптимізації мережних сервісів усередині мережі за рахунок поділу

мережних функцій (наприклад, DNS, кешовані та ін.), від властиво реалізації апаратного забезпечення. Уважається, що NFV дозволяє універсалізувати програмне забезпечення, прискорити впровадження нових функцій мережі й служб і при цьому не вимагає відмови від уже розгорнутої мережної інфраструктури.

Стосовно до мереж мобільного зв'язку віртуалізація виражається, зокрема, у концепції C RAN – хмарної (Cloud) або централізованої (Centralized) мережі радіодоступу. У цьому випадку радіоподсистема (remote radio heads, RRHs) і антени відділяються від основних блоків (модулів керування) базової станції (baseband units, BBUs), які розташовуються в так званому base station hotel і з'єднуються через оптоволоконий кабель із блоками RRHs. Таким чином, оператори можуть будувати хмарні мережі радіодоступу за принципом NFV, розміщаючи в хмарі основний функціонал базової станції, відповідальний за цифрову обробку сигналу, синхронізацію, керування, збір статистики та ін. Не виключено, що такий тип хмарних і віртуальних мереж радіодоступу може істотно змінити розміщення сил на користь IT-вендорів.

SDN формує віртуальний рівень для мережі, аналогічно тому, як гіпервізор або віртуальна машина робить це для серверів або настільних ПК. Протокол OpenFlow дозволяє програмному забезпеченню SDN взаємодіяти з відповідними елементами мережі – маршрутизаторами й комутаторами через відкриті Application Programming Interface (API). Шлях пакетів у програмно-конфігуруємій мережі визначається не встаткуванням виробників і «зашитими» у них алгоритмами обробки потоків даних, а спеціальним керуючим контуром у софте.

Віртуалізована функція мережі може працювати на одній або декількох віртуальних машинах. Тим самим сервіси виявляються нечутливі до самому «залізу». Це можуть бути стандартні сервери, системи зберігання, перемикачі. NFV дозволяє програмувати сервіси, які раніше були доступні тільки у вигляді апаратних рішень [2].

Схема SDN-архітектури

SDN і NFV дозволяють спростити конфігурацію мереж, масштабувати мережі й сервіси за запитом, автоматизувати керування мережею, збільшити потужність фізичної інфраструктури за рахунок накладення віртуальної, знизити CAPEX і OPEX, а в перспективі – швидко реконфігурувати бізнес під поточні завдання.

Перша велика мережа SDN була реалізована в 2012 р. компанією Google на базі комутаторів власної розробки. У такий спосіб їй удалося зняти ті обмеження, які властиві рішенням, використовуваним традиційними операторами. Трафік перенаправляється між ЦОДами так, як це зручно й вигідно в сучасний момент. Крім Google, технологію SDN використовують фірми NTT, Pertino, AT&T, Telecom Italia і ряд інших компаній [3].

Складається два стратегічних напрямки впровадження SDN, NFV і хмар. Перше пов'язане з підвищенням ефективності мережі й гнучкості послуг. Головна мета – зниження вартості експлуатації мережі й скорочення часу виходу на ринок. Друге націлено на одержання переваг від сполучення нових бізнес-можливостей. Ціль у цьому випадку інша – формування нових диференційованих хмарних сервісів і динамічне, залежне від поточного профілю попиту їхнє надання. По першому шляху йдуть такі компанії, як німецька Deutsche Telekom і іспанська Telefonica, по другому – японська NTT і американська AT&T.

Вигоди хмарної реалізації SDN:

- Практичний ефект від впровадження NFV/SDN для B2B клієнта.
- Керування послугами з Особистого Кабінету.
- Одержання Мережних функцій як Послуг с чітким SLA..
- Зниження витрат на обслуговування власних мережних функцій і IT систем за рахунок їхнього переносу на «сторону» оператора.
- Одержання доступу до Послуг у режимі 24/7 навіть при зміні фізичного місця перебування офісу.

– Одержання доступу до Послуг за мінімальний час при підключенні додаткового офісу.

– Можливість Тестової експлуатації послуги без необхідності її реалізації.

– Практичний ефект від впровадження NFV/SDN для провайдеру.

– Зниження вартості підключення – послуги віртуалізюванні й не вимагають виділеного встаткування.

– Використання COTS устаткування (стандартне встаткування x86 архітектури).

– Скорочення або повне скасування виїздів до клієнта для підключення додаткових послуг.

– Доступ до Послуг у режимі 24/7 навіть при переїзді клієнта.

– Зниження часу як на підключення нового клієнта, так і на додавання нових послуг.

– Зниження вартості експлуатації.

– Швидке й еластичне масштабування послуг залежно від потреб.

– Уніфіковані включення на мережі – зниження кількості різнотипного прикінцевого встаткування.

– Інтегратор як Сервіс Провайдер.

– Відсутність витрат на вивід послуги на ринок – платформа може бути розміщена в сторонньому Дата Центрі або на власних серверах інтегратора розміщених в Оператора..

– Використання моделі Revenue Sharing: є клієнт – є дохід, немає клієнта – немає витрат.

– Накопичений досвід і експертиза дозволяють реалізовувати й виводити на ринок нові послуги за найкоротші строки.

– Гнучке використання як «вендорських» так і Open Source рішень для реалізації мережних функцій.

– Підтримка й розвиток рішення є на боці інтегратора.

Software Defined Everything (SDX)

Ключовими споживачами концепції SDX є дата-центи, оператори й великі корпорації, технологічна й IT інфраструктура яких вимагає гнучких підходів до проектування, впровадженню й керуванню мережною архітектурою, а також її експлуатацією.

SDN для DaaS і BYOD

Останнім часом на ринку стає популярна віртуалізація, у тому числі у форматі DaaS (as-a-service). Дана модель припускає надання готового віртуального робочого місця, що кожний користувач може набудовувати під свої завдання. Тут незамінні технології віртуалізації додатків або робочого місця, які дозволяють централізовано управляти корпоративними додатками, забезпечуючи їхню безпеку й моніторинг. Тим самим організується контрольований доступ співробітників з будь-якого пристрою й значно знижує ймовірність витоку конфіденційних даних через особисті пристрої співробітника. Такий підхід допомагає впровадити модель BYOD («принеси свій власний пристрій»), при цьому значно спрощуючи керування інфраструктурою й забезпечуючи безпеку корпоративних даних. Згодом це приводить до значного скорочення операційних витрат і збільшує лояльність співробітників.

У даному сценарії SDN може виявити всі свої переваги повною мірою. Додавання нової віртуальної робочої станції не зажадає проведення налаштування різного мережного встаткування, а також додавання нових правил на сервісних пристроях (Firewalls, ADC і інші).

Всі дії можуть бути автоматизовані й вироблятися з одного місця – оркестратора. Система, що буде займатися конфігурацією гіпервізора, системи зберігання даних і мережі.

Стратегія переходу на технології SDN

Для найбільш швидкого й ефективного розгортання SDN необхідно насамперед визначити проблеми, з якими фахівці можуть зштовхнутися при впровадженні нових технологій [4].

По-перше, потрібно визначити мети, які переслідує впровадження SDN. Керівники проектів повинні ясно розуміти, для чого це необхідно й забезпечувати координацію спільної роботи підрозділів, які в минулому, можливо, ніколи не взаємодіяли між собою.

По-друге, забезпечити новий підхід до моніторингу мережі. Тому що мережа представляється єдиним, логічним цілим, особливі вимоги пред'являються до синхронізації прикінцевих пристроїв і контролера. Завдання моніторингу каналів зв'язку між компонентами SDN повинні бути вирішені за допомогою самого SDN-рішення або сторонніх систем. До того ж моніторинг необхідний при пошуку місця появи тої або іншої проблеми, що може виникнути на стику різних технологій.

Таким чином, перед початком розгортання SDN IT-фахівці повинні зрозуміти, яка інфраструктура вже є в наявності й що необхідно зробити, щоб лежачі в її основі системи могли швидко реагувати на зміни, пов'язані із впровадженням SDN-технологій.

Основні драйвери й стримуючі фактори впровадження

Вибір на користь SDN пояснюється багатьма причинами:

– По-перше, класичні підходи до рішення проблем мереж на основі їх віртуалізації відстають від рівня розвитку віртуалізації серверів і СЗД. У результаті мережі виявляються статичними й не відповідають швидкій динаміці розвитку IT-бізнесу [5].

– По-друге, при масштабуванні мереж з'являється велика кількість розподілених мережних пристроїв. В умовах, що змінилися, засобу традиційного керування стають великоваговими й неефективними.

– По-третє, традиційна прив'язка до того або іншому мережному вендору, що заздалегідь проробляє необхідні міри у випадку тих або інших трансформацій мережі, також виявляється неспроможною. Головна проблема – бізнесу не гарантується підтримка для майбутніх додатків і сервісів, що позбавляє його гнучкості при виборі майбутнього шляху розвитку.

Щомісячний світовий IP-трафік в 2018 г. складе 110 ЕБ, CAGR = 32%, по оцінках аналітиків. На відео прийде 55% трафіку, на web – 23%, на обмін файлами – 21%, на голос – тільки 1%. ARPU неухильно знижується. При цьому ростуть CAPEX і OPEX. Мир стає «хмарно центричним» (cloud-centric). Наростає розрив між поточної, багато в чому статичній і надлишково зарезервованою архітектурою телекомунікаційних мереж і IT інфраструктурою, з одного боку, і хмарною адаптивною концепцією споживання послуг і додатків, з іншої.

Драйвери розвитку віртуалізації мережних функцій

Ріст трафіку від різних пристроїв зіштовхується з "вузьким горлечком" мереж. Незабаром не залишиться жодного клаптика землі без фіксованого або мобільного зв'язку. Висока щільність покриття фіксованими широкополосними мережами стимулюється поширенням сервісів на базі кабельних і оптоволоконних мереж. Іде підривний ріст числа мобільних пристроїв, які завжди онлайн. І у фіксованих і в мобільних мережах міняється природа навантаження – від комунікацій до хмара-центричного міжмережного взаємодії. Ріст числа M2M-пристроїв збільшує навантаження на мережі.

Перехід до хмарних сервісів вимагає як вертикального (збільшення ресурсів), так і горизонтального (нові точки присутності) швидкого масштабування мережних функцій і їхньої взаємодії – за кілька секунд/мінут на противагу дням/тижням.

Постійно ростуть вимоги до якості контенту, міняється характер його споживання й генерації, тому потрібні нові підходи до передачі й керування потоками різнорідного трафіку.

Структура й обсяг трафіку на мережах визначаються профілем споживання з боку користувачів, причому динаміка трафіку стає усе більше нерівномірною.

Поширюються застосунки, що поєднують велику кількість пристроїв і генерують великий обсяг трафіку (міжмашину взаємодію, інтернет речей). Ефективне масштабування таких додатків вимагає нових мережних архітектур, які можуть бесшовно з'єднати площину передачі даних і передачі сигналу.

Ефективне керування такими навантаженнями й трафіком у мережах неможливо за рахунок нескінченного резервування, що дуже дорого.

Порівняння традиційних мереж і SDN

Контур керування трафіком в SDN мережі переміщається з рівня пристроїв і елементів мережі (фізичних або віртуальних) на централізований рівень спеціального ПЗ.

З погляду операторів, інтерес в SDN пов'язаний з підвищенням ефективності мережного встаткування, зниженням витрат, підвищенням мережної безпеки й наданням можливості програмно створювати нові сервіси й оперативно завантажувати їх у мережне встаткування.

SDN формує віртуальний рівень для мережі, аналогічно тому, як гіпервізор або віртуальна машина робить це для серверів або настільних ПК.

Протокол OpenFlow дозволяє програмному забезпеченню SDN взаємодіяти з відповідними елементами мережі – маршрутизаторами й комутаторами через відкриті Application Programming Interface (API).

Шлях пакетів в SDN мережі визначається НЕ встаткуванням виробників і «зашитими» у них алгоритмами обробки потоків даних, а спеціальним керуючим контуром у ПЗ.

До основних драйверів розвитку ринку SDN/NFV ставляться:

1. Зниження капітальних і операційних витрат, сукупної вартості володіння мережею. У випадку мобільного зв'язку розмір економії на CAPEX особливо существенен у тому випадку, якщо оператор має досить розвинену оптоволокону мережу. У цьому випадку компанія може скоротити капітальні витрати при використанні C-RAN аж до 60%. У противному випадку економія на CAPEX складе близько 30%. Скорочення CAPEX, зокрема, відбувається за рахунок зменшення базових блоків (BBUs). По тій же причині відбувається й зниження OPEX – за рахунок більше низького енергоспоживання[1] і зменшення витрат на обслуговування. По оцінці China Mobile, «зелена» альтернатива у вигляді хмарних мереж радіодоступу зменшує рахунку на електроенергію на 71% у порівнянні із традиційними мережами.

По даним NEC, впровадження віртуалізованого пакетного ядра (vEPC) у рамках концепції NFV дозволить операторові мобільного зв'язку істотно знизити сукупну вартість володіння (TCO).

2. Швидкість впровадження й адаптації послуг. Віртуальна (софтверна) екосистема споконвічно є програмувальною в істотно більшому ступені, чим «класична» мережа. Очікується, що ця можливість дозволить швидше впровадити й адаптувати сервіс і піти від існуючої в теперішньому часі концепції middleboxes – величезної кількості програмно-апаратних засобів у мережі оператора, які реалізують відповідну послугу.

Разом з тим, одним з основних стримуючих факторів для розвитку SDN – це відсутність єдиного стандарту й прагнення ряду вендорів нав'язати ринку «своє» рішення, хоча такий підхід абсолютно суперечить основним принципам SDN. У результаті в SDN ще багато невизначеності, і потенційні споживачі програмно-конфігуруємих рішень зайняли вичікувальну позицію, стежачи за появою успішних великих проектів у цій області.

Загальні цілі, що стимулюють розвиток напрямку SDN, включають [6]:

- гнучкість при створенні VPN, розподілі смуги пропущення й виділенні сегментів мережі;
- інтерфейси, що дозволяють користувачам вибирати стандартні мережні шаблони;
- створення інтерфейсів систем;
- швидке виявлення й заміна з'єднань, що відмовили;
- потужний брандмауер між користувачами й зовнішнім миром;

– значне скорочення витрат людино-годин на керування мережею;

– автоматичне масштабування відповідно до розв'язуваних завдань і обсягом трафіку.

Обґрунтування економічного ефекту SDN усе ще є видом мистецтва. Кількісний вимір нематеріальних речей, таких як більше високий рівень безпеки або більше швидка реакція на вимогу внесення змін, – це справа складне. У результаті увагу воліють концентрувати на речах відчутних, таких як зниження витрат на обслуговування мережі, скорочення витрат на придбання продуктів і т.д. Нематеріальні вигоди, однак, мають набагато більшу цінність, чим матеріальні, особливо, якщо в результаті підприємство в цілому стає більше гнучким.

Стратегічні напрямки впровадження SDN, NFV і хмар

Якими будуть ЦОД майбутнього? Стандартними. Гетерогенність – реальність хмар, нею треба вміти управляти, що тому випливає після хмар прорив в індустрії убік підвищення ефективності буде неможливий без стандартизації. Для інтеграції й масштабування хмар не вистачає стандартів, єдиної, відкритої для всіх вендорів платформи, загального стека технологій. Звідси випливає складність і висока ціна гібридних конфігурацій, зібраних з безлічі хмар. У випадку програмного підходу можна створити відкриту платформу, побудовану по модульному принципі. Питання вже не в неможливості зробити це, а в необхідній кваліфікації проектувальників ЦОД. Майбутнє – за програмно-визначаємими ЦОД, які замінять портали Service Desk, автоматизувавши процеси керування. Кусочне керування мережею, пам'яттю, безпекою, обчисленнями й додатками буде замінено інтегрованим керуванням процесами доставки додатків за запитом без втручання IT-служби [7].

Головна відмінність – традиційний ЦОД являє собою набір апаратних пристроїв (сервери, мережні пристрої, системи зберігання даних, обчислювальні й програмні керуючі ресурси), тоді як SDDC вибудовується як надбудова над існуючою апаратною інфраструктурою, де всі підсистеми ЦОДа віртуалізовані й зібрані в захищену програмну систему. Налаштування, керування й обслуговування віртуальних компонентів ЦОДа виробляються програмним шляхом, потім необхідні команди автоматично переносяться на апаратні ресурси [8].

Завданням технології програмно-конфігуруємих центрів обробки даних (SDDC), що стала популярної останнім часом, є поліпшення продуктивності центра за рахунок оптимізації на рівні додатків і гіпервізора. Однак аналітики Forrester думають (осінь 2013 року), що при керуванні центрами варто прагнути до оптимізації на рівні конкретних бізнес-процесів – обробки фінансових даних, рішення завдань постачання й так далі – а не на рівні окремих додатків, будь те ERP-системи, CRM, HCM та інші.

Навіщо переходити із традиційного ЦОДа на SDDC?

Головним системообразуючим елементом у традиційному ЦОДі часто називають комутатор. Цей мережний пристрій відповідає за виконання трьох основних функцій: керування підключеними пристроями, керування трафіком і фізична передача даних.

При переході на програмно-визначаєму модель ЦОДа функції керування пристроями й трафіком централізуються й переводяться в програмну форму. Їхньої команди забезпечують злагоджену роботу всієї інфраструктури SDDC. На частку комутатора залишається тільки функція передачі даних.

У результаті внесених змін комутатор стає більше простим. Зате ЦОД одержує додаткові можливості: спрощуються завдання масштабування інфраструктури, функції налаштування й керування стають більше гнучкими, з'являються додаткові ресурси для роботи із прикладним навантаженням, оптимізації, виправлення помилок.

Перехід на SDDC дозволяє також одержати більше високу обчислювальну потужність, нарощувати ресурси зберігання даних і мережної комутації, причому це досягається без виділення додаткового території під ЦОД або установки нових стійок.

Реальність і конкуренція на ринку ведуть до того, що власникам ЦОДів доводиться постійно обновляти власний парк устаткування, нарощувати обчислювальні потужності й домагатися підвищення ефективності в його керуванні. Для цього їм необхідно мати повну інформацію про поточну інфраструктуру. Якщо набір зібраних даних виявляється неповним, то приймати обґрунтовані рішення вкрай важко. Без ясного розуміння, що відбувається в ЦОДі, устаткування періодично попадає в стан простою. З розвитком віртуалізації в ЦОДах вимоги до його встаткування також ростуть. Для забезпечення доступності інфраструктури й контролю витрати обчислювальних ресурсів не обмежуються тільки збором інформації. Потрібно одержувати неї в повному обсязі й бути впевненим в актуальності зібраних даних. Якщо ці умови дотримані, можна проводити оптимізацію фізичної інфраструктури й переходити на програмне керування ЦОДом.

Зібрану інформацію про встаткування в традиційних ЦОДах часто зберігають у вигляді електронних таблиць. Коли приходить час для інвентаризації й модернізації, саме з них починається пошук вільного місця. По цим «документах» звіряються резерви електричних потужностей, перевіряється достатність ресурсів для охолодження, наявність вільних портів для підключення.

Однак тепер такі способи збору даних стають усе менш неефективними, особливо в умовах росту популярності хмар і віртуалізації. При відновленні ЦОДа з його оптимізацією необхідно використовувати спеціалізовані інструменти для збору й аналізу даних.

Світовий ринок SDDC

По даним Research & Markets, обсяг цього сегмента світового ринку склав в 2017 р. 25,61 млрд. дол. Протягом найближчих п'яти років очікується стійкий ріст при середньому річному темпі росту 26,57%. Згідно із прогнозом, до кінця 2021 р. цей ринок досягне рівня 89,21 млрд. дол.

Світовий ринок SDDC, 2017-2021 гг.

На відміну від звичних всім ЦОДів, основою яких є «залізо» – сервери, системи зберігання даних, мережні пристрої та ін. SDDC являє собою надбудову над існуючою інфраструктурою, керування якої виробляється програмним шляхом. А значить і захищати такі центри обробки даних треба інакше – традиційні рішення в сфері ІБ занадто ресурсоємні й гальмують роботу бізнес-додатків. Особливо помітно це в моменти сканування й відновлення антивірусних баз, що запускаються віртуальною машиною. У теж час, відключення віртуальної машини на тривалий період спричиняє поява слабкого місця в системі безпеки, оскільки встановлені на ній ІБ-компоненти перестають працювати.

Динаміка, проекти, активності

Розвитком SDN і NFV займаються галузеві альянси. За результатами нового дослідження IHS за 2017 р., основна частка впровадження SDN у дата-центрах зараз доводиться на установку іспитових стендів [9].

В 2017 р. бажання побудувати тестові стенди для дослідження SDN висловлювали 89% опитаних сервісів-провайдерів. Реальні результати, відповідно до звіту за 2017 р. виявилися нижче – 67%. Значно скоротилася також кількість передексплуатаційних перевірок і реальних впроваджень SDN у порівнянні з тим, що очікувалося в 2015 р.

У даному звіті також відзначається із впроваджень комутаторів без ОС (bare-metal switch, BMS) – мережних пристроїв, що поставляються без убудованого ПЗ, але із програмним завантажувальним середовищем, що забезпечує установку сумісних мережних ОС. Ці пристрої призначені в першу чергу для заміни пропрієтарних мережних комутаторів.

Orange Business Services і AT&T розроблять стандарти SDN

Orange Business Services і AT&T підписали влітку 2017 року угода про співробітництво в області розробки ініціатив по використанню відкритого коду й стандартизації, які прискорять прийняття стандартів для технологій програмно-визначаємих мереж (software-defined networking – SDN) і віртуалізації мережних функцій (network function virtualization – NFV). Компанії розділяють стратегічне бачення, відповідно до якого не тільки встаткування, але й мережі повинні ставати більше інтелектуальними, завдяки чому будуть

знижуватися витрати й складність експлуатації. Спільні зусилля партнерів наблизять поява більше маневрених, гнучких і оперативно реагуючих на потребі користувачів мереж майбутнього для індустрії й бізнес-замовників.

Розгортання нових віртуальних мережних сервісів і функцій сьогодні надмірно ускладнено. Постачальникам мережних послуг і інших мережних компаній доводиться мати справа із приватними стандартами, закритими архітектурами й устаткуванням від безлічі різних постачальників, що орієнтуються на різні платформи й специфікації. AT&T і Orange організують обговорення проблем галузевої стандартизації, щоб разом рухатися до їхнього рішення. Прийняття загальних стандартів і інтерфейсів допоможе індустрії спростити технологічну інтеграцію, підвищити операційну ефективність і знизити витрати, що прискорить процеси інновацій і розробки.

Коли технології SDN і NFV будуть засновані на загальних, відкритих і функціонально-сумісних технологічних стандартах, це допоможе перебороти труднощі надання мережних послуг з високим ступенем безпеки й власним інтелектом, що враховує особливості використовуваних додатків. Поява екосистеми функціонально-сумісних сервісів і постачальників устаткування позитивно відіб'ється як на технологіях програмно-визначаємих мереж, так і на бізнес-замовниках, які зможуть швидше й простіше розгортати сервіси, набудовувати їхню інфраструктуру в реальному масштабі часу й створювати інновації.

Взявши за основу мережецентричний підхід, AT&T і Orange мають намір зробити переваги свого бачення технологій SDN і NFV більше доступними як для бізнес-замовників, так і для індустрії. Компанії зосередяться на наступних завданнях:

Домогтися того, щоб як телекомунікаційне встаткування, розташоване на території замовників, так і мережні сервіси стали дійсно універсальними завдяки створенню загальних специфікацій мережної інфраструктури й могли працювати в будь-яких середовищах програмно-визначаємих мереж з різним мережним програмним забезпеченням.

Спростити й зробити більше ефективним процес впровадження технології NFV завдяки загальним рекомендаціям і шаблонам, які зроблять екосистему постачальників цієї технології більше зрілої, а саму технологію – більше простої у використанні.

Розробити стандартизовані інтерфейси прикладного програмування, які дозволять архітектурам програмно-визначаємих мереж різних постачальників взаємодіяти один з одним, роблячи розгортання віртуалізованних мережних функцій і сервісів більше швидким і легенею.

Розробка структурної схеми

Відповідно до опитування SDXcentral, закриті пропрієтарні рішення поки переважають над відкритими. Це пов'язане з тим, що якісне працююче рішення, яке можна впровадити на виробництві, складно зібрати з компонентів з відкритим вихідним кодом, до того ж хтось повинен його підтримувати. Проте відкриті компоненти одержують усе більше широке поширення, а рішення на базі відкритого вихідного коду й відкритих стандартів розвиваються досить інтенсивно. Відповідно, багато виробників, будь те постачальник мережного встаткування або розроблювач програмного забезпечення, розвивають паралельно два напрямки – власні закриті розробки й підтримку відкритого коду.

Така невизначеність у кардинальних напрямках подальшого розвитку SDN багаторазово ускладнює завдання вибору для замовника. Тим часом необхідність у використанні гнучких мереж, їхньому швидкому розгортанні й адаптації до мінливих вимог стає реальною. Звичайно, ніякий опис не замінить безпосереднього тестування або пілотного проекту, адже тільки так можна оцінити, наскільки те або інше рішення відповідає умовам конкретного мережного середовища. Однак всі доступні рішення протестувати однаково неможливо, тому бажано мати хоча б загальне подання про те, чим є той або інший продукт, технологія або підхід і в якому напрямку розвиваються.

Що таке мережна віртуалізація

Додаткову плутанину вносять безліч термінів і акронімів. Дотепер зберігається плутанина в поняттях: що таке мережна віртуалізація, SDN і NFV – те саме чи це? SDN означає OpenFlow або його підтримка необов'язкова? SDN являє собою повністю програмну реалізацію? Якщо так, то як вона пов'язана з комутаторами (фізичним устаткуванням)?

Програмно обумовлені мережі – це підхід до архітектури, що полягає в поділі площин даних, контролю й керування (data, control&management planes). Мережна ж віртуалізація являє собою продукт, що на цій архітектурі базується.

Причому функції площини даних відтворюються повністю на програмному рівні, а не на рівні комутаторів. Останні спрощуються й стають просто фізичним транспортом, тоді як вся функціональність і логіка реалізуються програмно.

Історично для мережної віртуалізації основним драйвером розвитку було створення хмарної інфраструктури за запитом. У ЦОДі очолюють прикладні системи, а не інфраструктура. Відповідно, вимоги до інфраструктури залежать від додатків, а не навпаки. Застосунки повинні бути захищеними, забезпечуючи цілісність і схоронність даних, швидко розгортатися й замінятися, якщо це потрібно. І бути доступними: якщо відбувся збій, то відновлення повинне відбуватися швидко, бажано автоматично. Ці вимоги – безпека, швидке розгортання й висока доступність – залишаються колишніми.

Виходячи з досвіду використання замовниками платформи NSX від VMware виділяється три основних сценарії застосування для мережний віртуалізації: безпека, автоматизація й підвищення доступності.

Відкритість і програмуємість – добре, але це чисто академічний, технічний підхід.

Будь-яке впровадження будь-якої технології в комерційній організації повинне бути підкріплене бізнес-вимогами, як правило комерційно адекватними. Так, наприклад, забезпечення безперервності для віртуалізованих середовищ є реальним практичним завданням. Мережна віртуалізація дозволяє переміщати між ЦОДами й резервувати разом з додатком не тільки дані, але й всі мережні налаштування.

Однак якщо завдання залишаються незмінними, то умови для їхнього рішення вже помінялися. Для все більшого числа додатків зовнішній доступ доводиться забезпечувати звідусюди, що веде до зміни шаблонів взаємодії з додатками. Архітектура останніх теж перетерплює зміни в результаті поширення таких технологій, як контейнерна віртуалізація. Нарешті, трансформується й інфраструктура, оскільки класична архітектура мережі не відповідає архітектурі додатків. Як результат, всі виробники мережного встаткування пропонують ті або інші варіанти для реалізації L3-фабрик. А класичне розтягування мереж L2 поступається місцем накладеним мережам.

Все це відбивається в рішеннях для віртуалізації мережі. Раніше, коли мережна віртуалізація тільки з'явилася, високий рівень доступності – на рівні п'яти дев'яток – був необхідний лише для площини даних. Для площини керування вимоги були нижче. Зараз ситуація змінилася, оскільки все більшу роль у компаніях, наприклад в Ощадбанку, грають розроблювачі.

Навіть площина керування повинна бути резервуємою, розподіленою, що дуже швидко реагує на зміни.

Центр досліджень VMware розробив технологію поліпшення розподіленості для площини керування Corfu DB (проект із відкритим вихідним кодом). Це розподілений журнал транзакцій, що дозволяє реалізувати площина керування по розподіленій зарезервованій архітектурі, тобто в режимі « активний-активний».

Наступний напрямок розвитку VMware NSX – підтримка DPDK. Навантаження стають усе більше, оператори зв'язку хочуть перенести мережні функції на стандартні сервери, тому вимоги до продуктивності віртуальних комутаторів, як і до затримок, сталі рости. Intel розробила набір бібліотек і драйверів для швидкої обробки пакетів, що одержав назву «Комплект розроблювача для площини даних» (Data Plane Developer Kit, DPDK). VMware планує застосовувати цю технологію для підключення до фізичної мережі: Тільки там це й потрібно, тому що у віртуальному середовищі в нас все розподілене – ми досягаємо

продуктивності методом розподілу всього навантаження. Відповідно, у нас з'являться граничний кластер в NSX у режимі « активний-активний» і засобу швидкого оповіщення фізичної мережі про збої.

Три варіанти реалізації SDN

Пропонований VMware спосіб реалізації SDN за допомогою накладених мереж є, природно, не єдино можливим.

По-перше, це реалізація SDN у вигляді програмувальної фабрики, що припускає низькорівневе програмування комутаторів фабрики з використанням відкритого протоколу OpenFlow. Логіка мережі централізовано виноситься в контролер, що і програмує мережа відповідно до заданої політики. Цей «класичний» підхід відрізняється найбільшою гнучкістю й універсальністю, але одночасно є найбільш витратним, тому що припускає заміну успадкованого встаткування у всій мережі – фактично мережа прийде побудувати заново, оскільки на всьому мережному встаткуванні повинні підтримуватися певні API. Один із прикладів відкритої SDN – це, звичайно, OpenFlow. При використанні OpenFlow всі комутатори повинні його підтримувати. Цілий ряд вендорів, зокрема BigSwitch, реалізують подібний підхід, але в деяких він особливий – наприклад, в Cisco в Application Centric Infrastructure.

Другий варіант – SDN у вигляді накладених мереж (overlay). Ідея полягає в тому, щоб винести всю програмну логіку SDN з кінцевих комутаторів на сервери, де можна реалізувати всі що завгодно. Цей варіант набагато простіше в реалізації, тому він зараз активно розвивається: SDN можна розгорнути, не міняючи вже наявне мережне встаткування, а просто встановивши необхідне програмне забезпечення. Завдяки збереженню успадкованого встаткування витрати відносно невеликі – в основному на покупку ПЗ. Однак керування мережею й діагностування ускладнюються, тому що доводиться управляти нижчележачою фізичною мережею й накладеня логічної, корелювати інформацію від фізичних і віртуальних пристроїв.

Основною областю застосування даного підходу є центри обробки даних. SD-WAN – ще один приклад реалізації подібного підходу в мережах WAN, хоча одне іншого не виключає. Дана модель (overlay) знайшла втілення в рішеннях VMware NSX, Nuage Networks (тепер частина Nokia), VSP, PLUMGrid ONS, OpenContrail і Midokura MidoNet. Накладені мережі реалізуються повністю програмно на сервері (на базі віртуальних комутаторів) або виносяться в мережну фабрику (на комутатори в стійці, ToR).

І нарешті, SDN через API. Не самий очевидний варіант. Раніше його ніхто не називав SDN але зараз у якімсь ступені можна віднести до DevOps, що використовується як засіб автоматизації й уніфікації керування». Ідея складається у використанні єдиної моделі даних для опису конфігурації, а також стандартних інтерфейсів керування, наявних у мережних пристроїв, – це класичний SNMP, Netconf, XML, REST і ін. Різні програмувальні API дозволяють замість керування через Web-Інтерфейс і через CLI використовувати автоматизовані сценарії. Модель припускає найменші витрати. Однак функціональність обмежується можливостями CLI на конкретному пристрої. Проте вона часто використовується як доповнення до першої й другої моделей, тим більше що на ринку є цілий ряд засобів автоматизації, наприклад Chef, Puppet і Ansible.

OPEN Ethernet як доповнення до SDN

Якщо раніше мережні пристрої являли собою якийсь «чорний ящик» зі своєю апаратною архітектурою й програмним забезпеченням, то зараз цей підхід поступово йде в минуле.

Ініціатива Open Ethernet припускає використовувати мережний пристрій як відкрита платформа для запуску ОС і додатків.

Купуючи сервер від HPE, ви ж не будете встановлювати на нього тільки певну ОС? Ви можете поставити Windows, Linux – все що завгодно. Те ж можливо й у випадку Open Ethernet: купивши комутатор, ви можете встановити будь-яку ОС із необхідним набором додатків для підтримки обраного варіанта реалізації програмувальної мережі.

Використання тільки Open Ethernet не приносить настільки відчутних переваг, як у зв'язуванні з SDN. Доповнюючи SDN, він дає істотне збільшення свободи дій: користувач більше не прив'язаний до конкретного виробника встаткування й програмного забезпечення. Це досягається цілим набором засобів. Насамперед це використання відкритої апаратної платформи. Мікросхема ASIC – серце комутатора, вона повинна підтримувати відкриті інтерфейси, що забезпечують керування комутатором. Інакше кажучи, інтерфейси повинні бути відкриті, загальнодоступні, описані й документовані.

Прикладом такого інтерфейсу може служити інтерфейс абстракції комутатора (Switch Abstraction Interface, SAI). Це набір бібліотек, які дозволяють створити мультивендорну абстракцію для керування різними чипами: за допомогою того самого коду можна управляти чипом Mellanox, чипом Marvell і ін. Тим часом під егідою Linux Foundation, усередині самого співтовариства Linux, ведеться розробка Switchdev. Цей прошарок являє собою повністю відкритий драйвер усередині ядра Linux для комутаторів. Завдяки підтримці Switchdev, на комутатори Mellanox, як і на звичайний сервер, можна встановити операційну систему Linux. Головне, щоб версія ядра відповідала.

По своїй архітектурі комутатор є спрощеним сервером, що складається із процесора, пам'яті, диска, у якого на PCI-Шині є ще й ASIC. Якщо для ASIC є драйвер, яким ми можемо управляти, то для установки будь-який ОС досить скористатися відкритим завантажником. Він був створений у рамках проекту Open Compute і називається ONIE. По суті, це аналог BIOS/UEFI у сервері на комутаторі. З його допомогою можна встановити будь-яку ОС, після чого використовувати будь-які застосунки. Таким чином, спостерігається зустрічна тенденція: сервери перетворюються в (віртуальні) комутатори, а комутатори – у сервери.

Прискорення накладеної мережі

Як виходить з назви, логічна мережа організується за допомогою тунелів між кінцевими вузлами, а тунелі «накладаються» на наявну фізичну мережу. Найбільш відомими протоколами туннелювання є Virtual eXtensible LAN (VXLAN), Network Virtualization using GRE (NVGRE) і Generic Network Virtualization Encapsulation (GENEVE). У випадку VXLAN кінцеві точки тунелів називаються VXLAN Tunnel End Points (VTEP). Контролер накладеної мережі SDN взаємодіє з VTEP, які часто (але не завжди) являють собою віртуальні комутатори й маршрутизатори на серверах.

На практиці накладена мережа може бути реалізована двома способами. Перший – винятково програмний, коли самі тунелі й логічна мережа організуються віртуальними комутаторами, що функціонують на серверному гіпервізорі. Цей підхід використовує VMware c NSX, Nuage, OpenStack. Як ми вже відзначали, заміни мережного встаткування не потрібно. Потенційний недолік такого підходу очевидне – використання процесорного часу для інкапсуляції трафіку і його розбору, якщо не застосовувати спеціальних мір для розвантаження.

Другий варіант – апаратний VTEP на комутаторах у стійці (ToR), коли тунелі організуються не гіпервізорами, а комутаторами. Для цього комутатор ToR повинен одержувати інформацію про віртуальні машини, здійснювати перетворення MAC-адрес для ВМ, підтримувати більші таблиці для переадресації. Проблема такого рішення в тім, що висока продуктивність досягається за рахунок втрат у гнучкості: чип комутатора не може підтримувати всю ту функціональність, яку можна реалізувати програмно.

VXLAN (offload)

Однак зниження продуктивності в першому варіанті можна компенсувати, наприклад, шляхом установки в сервері мережних адаптерів з підтримкою розвантаження VXLAN (offload) і інших протоколів інкапсуляції. У результаті продуктивність програмної реалізації накладеної мережі наближається до апаратного, а гнучкість і функціональність підвищуються. Як показало тестування, при включенні інкапсуляції VXLAN реальна пропускна здатність каналу між двома серверами з інтерфейсом 40 Гбіт/с падає з 35–37 до 5 Гбіт/с – майже на порядок. Це пов'язане з тим, що більшу частину часу процесор витрачає на перерахунок контрольних сум і частково на інкапсуляцію.

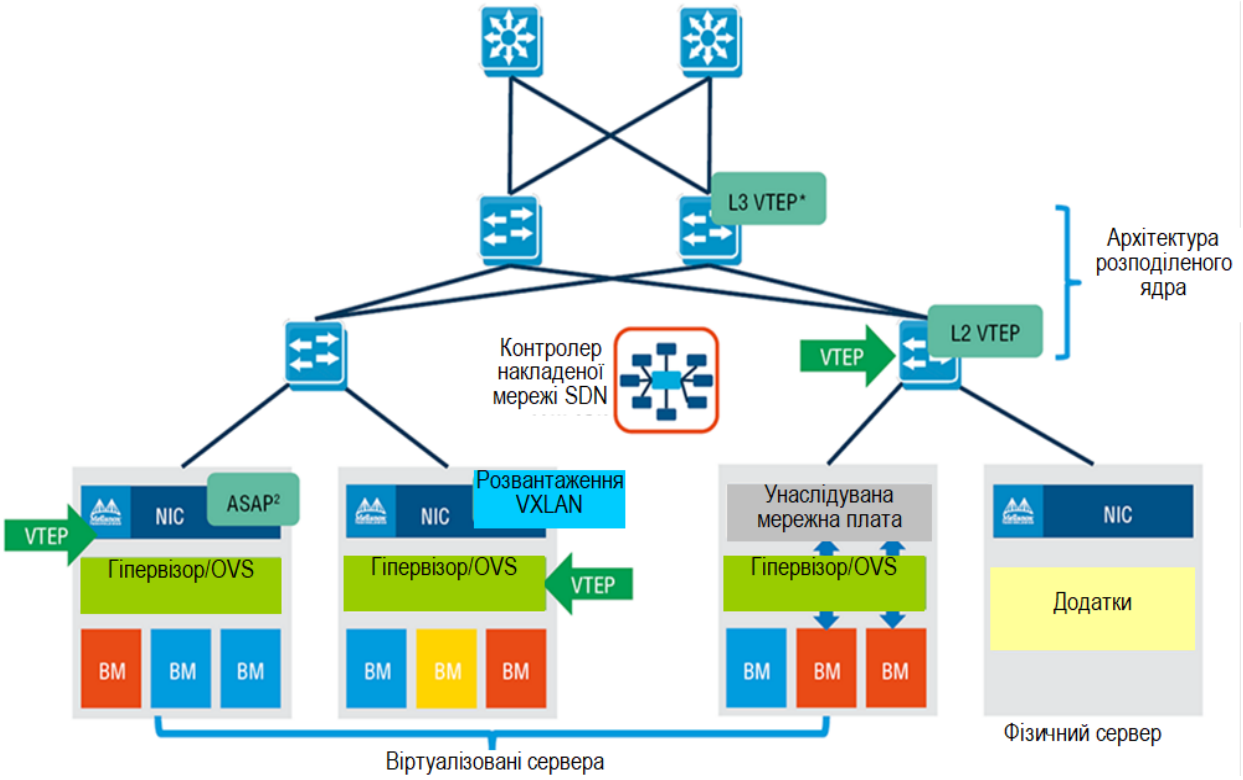


Рисунок 1 – Структурна схема системи

Застосування VXLAN offload – технології, завдяки якій обчислення контрольних сум для інкапсульованих пакетів здійснює не процесор, а мережна карта, – дозволяє збільшити продуктивність до 36 Гбіт/с.

Причому, чим більше ВМ запущено, тим менше різниця між пропускною здатністю без інкапсуляції VXLAN і з використанням VXLAN offload. Інакше кажучи, один лише перерахунок контрольних сум на мережній карті дозволяє досягти продуктивності накладеної мережі, близької до номінальної швидкості інтерфейсу (wire-speed), при цьому ще звільняються ресурси процесора – їх можна віддати наявним ВМ або навіть запустити більше ВМ на тім же хості.

Чип сучасної мережної карти являє собою міні-комутатор: він уміє збирати інформацію про MAC-адреси (MAC learning), інкапсулювати різні пакети, здійснювати обробку потоків. Крім найпростішого розрахунку контрольних сум, мережні карти Mellanox Connect-4 забезпечують вивантаження всієї площини даних віртуального комутатора в чип карти. Наприклад, у випадку Open Virtual Switch (OVS) всі правила можуть бути завантажені на мережну карту, у результаті на обробку складних мережних правил процесорний час взагалі не витрачається. Цю технологію можна використовувати для прискорення критично значимих ВМ, дуже активно взаємодіючих з мережею. Стандартний приклад – віртуальні мережні функції NFV, які дійсно пропускають через себе великий обсяг трафіку. Вони можуть бути значно прискорені за допомогою цієї платформи.

Термінування тунелів VXLAN на комутаторах ToR найчастіше застосовується в рамках гібридної схеми, коли більшість віртуальних хостов будують між собою тунелі прямо, програмно, за допомогою механізмів акселерації. Однак у мережі є невіртуалізовані хости, наприклад бази даних і різні платформи на UNIX. Щоб їх включити в накладену мережу, можна використовувати апаратний шлюз на базі комутатора й організувати на ньому або L2 VTEP, або L3 VTEP.

Мережна фабрика для SDN

Перш ніж запускати всі необхідні сервіси, варто правильно вибудувати інфраструктуру. Якщо мережа побудована неефективно (втрачає пакети, на портах відбуваються помилки й т.д.), SDN працювати не буде. Ключова ідея – об'єднання класичних

універсальних пристроїв у дворівневу топологію Leaf-Spine, коли кожний комутатор першого рівня (leaf) пов'язаний з кожним комутатором другого рівня (spine). Ця топологія була запропонована Чарльзом Клозом в 50-х роках минулого століття для побудови масштабованих телефонних мереж.

Комутатори доступу (leaf, або «аркуш») забезпечують підключення кінцевих вузлів: серверів, систем зберігання, різних мережних пристроїв, таких як комутатори, балансувальники навантаження, міжмережні пристрою й т.д. Комутатори ядра (spine, або «стовбур») здійснюють міжз'єднання листів: кожний лист з'єднаний з усіма іншими стовбурами. Між листами, як і між стовбурами, з'єднань немає. Це дозволяє організувати безліч надлишкових шляхів між листами. Відмова одного з комутаторів приводить лише до незначного зниження продуктивності мережної фабрики.

Багато хто вендори пропонують пропрієтарні рішення для реалізації топології Клоза. Однак, актуальні стандартні варіанти реалізації ECMP-фабрики. Через доступність декількох маршрутів, необхідно розподіляти трафік між ними, для чого використовується протокол равновіддалених маршрутів (Equal Cost MuptiPathing, ECMP). Для підтримки накладеної мережі досить з'єднати всі комутатори по топології Клоза й настроїти на них маршрутизацію у відповідності зі стандартними протоколами OSPF/BGP. (У принципі, поверх тої ж фізичної топології можна реалізувати й програмувальну мережу на базі протоколу OpenFlow.)

Як приклад приведемо схему реальної мережі на базі комутаторів Spectrum – практично така ж схема неодноразово використовувалася в проектах Mellanox. Вона дозволяє побудувати мережу, що містить понад 5 тис. порти по 25 Гбіт/с (або 10 Гбіт/с) з мінімальної передподпискою 2,5 до 1 для підключення 64 стійок на 2,5 тис. серверів. При високоплотному розміщенні серверів – приблизно 40 серверів на одну стійку – в одну стійку встановлюється по двох комутатора SN2100 половинчастого виконання. Сервери підключаються до кожного з них через два порти по 25 Гбіт/с. При цьому кожний SN2100 має 4 порти для каскадування по 100 Гбіт/с, що, таким чином, дає перепідписку 2,5 до 1. Для з'єднання стійок будується розподілене ядро на 16 spine-комутаторів і 32 leaf-комутатора, у якості яких використовуються пристрої серії 2700, з'єднані в неблокуєму фабрику топології Клоза. Одна половина портів на кожному leaf-комутаторі служить для підключення комутаторів у стійці, інша – для підключення до spine-комутаторів.

Такий віртуальний модульний комутатор (Virtual Modular Switch, VMS) дозволяє забезпечити підключення 512 портів по 100 Гбіт/с.

Якщо знадобиться подальше масштабування, можна збільшити або рівень перепідписки, або кількість таких фабрик. В останньому випадку буде потрібно ввести новий рівень – це буде вже багаторівнева топологія Клоза.

SDN викликають все більший практичний інтерес внаслідок потреб хмарних центрів обробки даних у забезпеченні віртуалізації, стандартизації й автоматизації. Завдяки абстрагуванню площини даних і контрольної площини, програмно обумовлені мережі надають IT-адміністраторам зовсім новий інструмент для ефективного керування критичними мережними ресурсами. Рішення для реалізації SDN і віртуалізації мережі випускають багато хто вендори, причому часом їхні пропозиції відрізняються не тільки деталями, але й принципами, на яких базуються рішення. Однак всі зусилля націлені на те, щоб в остаточному підсумку спростити мережа й керування нею.

Висновок. У статті розглянуто та проаналізовано програмне забезпечення, яке призначено для віртуалізації мережі на базі застосування технології VXLAN offload. В межах України в недостатній мірі представлені вітчизняні розробки в цій області. У роботі наведені теоретичне узагальнення й рішення наукового завдання дослідження методів віртуалізації мережі на базі застосування технології VXLAN offload. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем віртуалізації мережі на базі застосування технології VXLAN offload; Досліджена система віртуалізації мережі на базі застосування технології VXLAN offload; На основі отриманих результатів досліджень створена програмна реалізація віртуалізації мережі на базі

застосування технології VXLAN offload. Розроблені під час виконання роботи алгоритми дозволяють успішно вирішувати завдання віртуалізації мережі на базі застосування технології VXLAN offload. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки. Розроблене програмне забезпечення має простий, дружній та зручний інтерфейс користувача, що забезпечує легкість у освоєнні роботи програмного продукту, зручність у використанні, і не потребує особливих спеціальних знань. При створені програмного забезпечення було використано об'єктно-орієнтований підхід, що відповідає сучасним тенденціям у галузі розробки комерційних програмних систем. Програма реалізована на мові високого рівня Delphi 10.2 Tokyo. Дана мова програмування дозволяє найбільш ефективно обробляти дані. Це дозволило мінімізувати строк розробки програмного забезпечення, і, як слід, зменшити витрати на його розробку. Запропоноване програмне забезпечення ділиться на загальне програмне забезпечення, що поставляється із засобами обчислювальної техніки й спеціальне програмне забезпечення, що спеціально розроблене для даної конкретної системи й включає програми, що реалізують її функції. Даються необхідні рекомендації з установки розробленого програмного забезпечення. Для підвищення рівня безпеки запропоновано застосовувати алгоритм RC5.

Список літератури

1. Microsoft Corporation. Межсетевое взаимодействие. Ресурсы Microsoft Windows 2000 Server. /Пер, с англ. – М.: Издательско-торговый дом "Русская Редакция*, 2002. – 736 с.: ил,
2. Microsoft Corporation. Разработка инфраструктуры сетевых служб Microsoft Windows 2000. Учебный курс MCSE. /Пер. с англ. – М: Издательско-торговый дом "Русская Редакция", 2001. – 992 стр.: ил.
3. Microsoft Corporation. Распределенные системы. Книга 1. Ресурсы Microsoft Windows 2000 Server. /Пер, с англ. – М.: Издательско-торговый дом "Русская Редакция", 2001. – 864 с.: ил.
4. Microsoft Corporation. Управление сетевой средой Microsoft Windows 2000. Учебный курс MCSA/MCSE. /Пер. с англ. – М.: Издательско-торговый дом "Русская Редакция". 2003. – 896 стр.: ил.
5. В.Г. Олифер, Н.А. Олифер. Компьютерные сети: Принципы, технологии, протоколы.
6. Селезнев Д.А. Построение локальной компьютерной сети масштаба малого предприятия на основе сетевой OS Linux. /МГИФИ, М., – 1999.
7. Терентьев А.М., Винокуров А.Е. Методы аудита локальных сетей в MS-DOS /Вопросы информационной безопасности узла Интернет в научных организациях. Сборник статей под ред. М.Д. Ильменского – М: ЦЭМИ РАН, 2001, с. 79 – 83.
8. Терентьев А.М. Методы и средства наблюдения загрузки локальных вычислительных сетей на примере ЦЭМИ РАН / Препринт #WP/2001/110 – М.: ЦЭМИ РАН, 2001. – 74 с.
9. Терентьев А.М. Задачи полноценного аудита корпоративных сетей. – «Концепции», N1(11), 2003, с.94-95.
10. Смирнов А.А. Разработка методики оценки среднего времени обслуживания информационных пакетов в телекоммуникационной сети / А.А.Смирнов, В.В.Босько, Е.В.Мелешко // Системи управління, навігації та зв'язку. – Київ: ДП «Центральний науково-дослідний інститут навігації і управління», 2009. – Вип. 2(10). – С.162-165.

УДК 004

М. Гурбанов, магістр гр. КІ-18М-1,9
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ КЛАВІАТУРНОГО ШПИГУНА В KVM-SWITCH ПОБУДОВАНОГО НА БАЗІ МІКРОКОНТРОЛЕРА PIC16C57C

У статті розглянуто програмне забезпечення, яке призначено для клавіатурного шпигуна в KVM-switch побудованого на базі мікроконтролера PIC16C57C. Метою розробки є дослідження та програмна реалізація клавіатурного шпигуна в KVM-switch побудованого на базі мікроконтролера PIC16C57C. Об'єктом дослідження є процес реалізації клавіатурного шпигуна в KVM-switch побудованого на базі мікроконтролера PIC16C57C. Предметом дослідження є методи реалізації клавіатурного шпигуна в KVM-switch побудованого на базі мікроконтролера PIC16C57C. Методи дослідження базуються на методах захисту інформації, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація клавіатурного шпигуна в KVM-switch побудованого на базі мікроконтролера PIC16C57C. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення. Розроблено зручний інтерфейс користувача. Наведені інструкції по роботі з програмними засобами. Програма може використовуватися на KVM-світчі на базі платформи Arduino.

комп'ютерна інженерія, клавіатурний шпигун, KVM-switch, PIC16C57C

Постановка проблеми. Занадто часто фахівці з безпеки при оцінці ризиків, пов'язаних із пристроями, підключеними до мереж і систем, розглядають тільки уразливості в програмному забезпеченні. Коли мова заходить про оцінку потенційних ризиків, пов'язаних із приєднаними пристроями, у тому числі пов'язаними з інтернетом речей, професіонал повинен розглядати не тільки проломи в програмах і прошиваннях цих систем, але й фізичні уразливості в апаратній частині.

Один з методів пов'язаний з фізичною модифікацією систем, наприклад, з метою додавання шкідливої функціональності для добування потрібної інформації без експлуатації проломів у програмному забезпеченні.

У цій роботі буде продемонстрована можливість модифікації стандартного KVM-світча (Keyboard, Video monitor, Mouse; пристрій для керування декількома системами з одного місця) з метою додавання функції перехоплення натиснутих клавіш на базі платформи Arduino. Ми покажемо, що подібне можна зробити за допомогою стандартних інструментів і компонентів з мінімальними знаннями в області електроніки й програмування.

KVM-світчи являють собою пристрою, часто використовувані в таких випадках, коли необхідно управляти множиною комп'ютерів за допомогою однієї клавіатури, миші й монітора.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини реалізації клавіатурного шпигуна в KVM-switch побудованого на базі мікроконтролера PIC16C57C.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація клавіатурного шпигуна в KVM-switch побудованого на базі мікроконтролера PIC16C57C.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем реалізації клавіатурного шпигуна в KVM-switch побудованого на базі мікроконтролера PIC16C57C.

– Дослідження клавіатурного шпигуна в KVM-switch побудованого на базі мікроконтролера PIC16C57C.

– Програмна реалізація клавіатурного шпигуна в KVM-switch побудованого на базі мікроконтролера PIC16C57C.

Об'єктом дослідження є процес реалізації клавіатурного шпигуна в KVM-switch побудованого на базі мікроконтролера PIC16C57C.

Предметом дослідження є методи реалізації клавіатурного шпигуна в KVM-switch побудованого на базі мікроконтролера PIC16C57C.

Методи дослідження базуються на методах захисту інформації, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу.

Опис функціонування системи

Для того, щоб зменшити число використовуваних моніторів і пристроїв уведення, необхідних для керування декількома серверами, більшість IT-служб використовує KVM-перемикачі. Абревіатуру «KVM» можна розшифрувати як: «клавіатура» («Keyboard»), «відеомонітор» («Video monitor»), «миша» («Mouse»).

Будь-який KVM-перемикач складається із двох основних пристроїв: відео-перемикача (міняє напрямок аналогових відео- і синхро- імпульсів між моніторами й комп'ютерами спільного користування) і мікропроцесорної системи (передає й приймає сигнали із клавіатури й миші й робить емуляцію наявних клавіатур і мишей).

Базова технологія й принципи дії всіх KVM однакові. Розглянуті перемикачі являють собою пристрої, що пропонують можливість керування декількома комп'ютерами, по черзі перемикаючись між ними. При цьому число комп'ютерів визначається можливостями KVM. Немає необхідності мати спеціальне програмне забезпечення, і відсутні традиційні громіздкі процедури підключення.

Переваги використання KVM-перемикачів

Можливість захищеного й надійного доступу до численних локальних і віддалених серверів і керування їхньою роботою.

Рішення на основі KVM-перемикачів – це значна економія засобів на додатковому встаткуванні, електроенергії, офісному просторі, а також вартості експлуатації й технічної підтримки системи.

Ви також заощаджуєте людські ресурси. Операторові не прийдеться витрачати час на переміщення від одного комп'ютера до іншого.

KVM-перемикачі використовують:

– Співробітники, що працюють у малих офісах і будинку.

– Системні адміністратори.

– У центрах по обробці даних: при моніторингу власних серверів або серверів керування для провайдерів Інтернет-сервісу, провайдерів сервісу додатків, іспитових лабораторій, фінансових організацій.

– При випробуваннях продукції: під час проведення перевірочних або відбраковочних випробувань комп'ютерних систем, плат VGA, мережних плат, RA-модулів.

– У промисловості, при моніторингу й контролі функціонування технологічних ліній, виробничих процесів і взаємодії між ними, систем безпеки, систем відеозображення.

– У науково-дослідних підрозділах, технологічних іспитових лабораторіях.

У корпоративному середовищі для обґрунтованого вибору рішення KVM у першу чергу необхідно з'ясувати наступне:

– Якій кількості адміністраторів необхідні консолі KVM, і де розташовані їхні робочі місця?

– Якими серверними платформами необхідно управляти й повинне чи керування поширюватися на послідовні сервери та інші мережні компоненти?

– Скільки серверів і інших пристроїв підлягають керуванню і як може змінитися ця картина в майбутньому?

– Які продукти KVM уже використовуються й чи передбачається їхнє включення в загальне рішення?

З відповідей на ці питання можна визначити найважливіші критерії й властивості, на яких буде базуватися рішення.

Спектр пропонованих на ринку перемикачів KVM дуже широкий.

Найпростіші варіанти розраховані лише на забезпечення пристроями уведення/виводу двох або декількох машин, а для з'єднань часто застосовуються нестандартні кабелі. Такий тип перемикачів KVM призначений для використання в малих офісах і будинку. Критичне значення в цьому випадку має якість зображення – особливо при високому дозволі, – а також функції й простота інтерфейсу керування, активізація якого відбувається за допомогою «гарячих» клавіш.

Широко поширені й перемикачі із кнопкою на лицьовій панелі – це досить практично, якщо управляти доводиться всього лише двома-чотирма персональними комп'ютерами. Ранні моделі KVM-перемикачів були в основному оснащені PS/2 роз’ємом. Більше нові пристрої для цієї цільової групи пропонують підключення для клавіатури й миші за допомогою USB. Живлення перемикачів початкового рівня простіше всього здійснюється безпосередньо через гнізда PS/2 або USB для клавіатури, тому окремий блок живлення для них не потрібний.

Більше складні моделі KVM-перемикачів являють собою пристрою на більшу кількість портів, мають більші функціональні можливості й, відповідно, відрізняються більше високою вартістю. Застосовуються вони, як правило, у середні по розмірі організаціях або великих компаніях, де обслуговується більша кількість комп'ютерів і серверів. До одного перемикача можна підключити 8, 16 комп'ютерів.

Компанії ростуть, постійно розширюються, відкривають філії, розкидані друг від друга на величезні відстані. Все це значно ускладнює процес контролю й керування комп'ютерами в корпоративній мережі. Більші відстані й далекість унеможливлюють використання аналогових KVM-перемикачів. Для таких цілей дуже зручно користуватися IP KVM-перемикачами. Зупинимося детальніше на рішеннях KVM-перемикачів на базі IP.

Недолік традиційних апаратних рішень KVM полягає в тому, що адміністратори не можуть звернутися до серверів з будь-якого місця. Їм необхідний фізичний доступ до перемикача KVM. Перемикачі молодшого класу часто припускають наявність лише одного адміністратора. Якщо ж потрібно управляти сотнями серверів, то це завдання, як правило, вирішується численною командою, члени якої не обов'язково повинні розташовуватися в одному приміщенні. Якщо всі перебувають в одному місці, то на території компанії можна використовувати різні види проводки для покриття необхідних відстаней. Якщо ж адміністратори розподілені по декількох філіях, то мова може йти тільки про цифрове рішення KVM на базі IP. Такі рішення припускають, що перемикач «збирає» сигнали від підключених до нього серверів і доставляє їхньому адміністраторові у вигляді пакетів IP. Таким чином, завдання керування можна вирішувати через Internet з будь-якого місця, де є доступ до мережі.

При виборі засобів досягнення дистанційного керування іноді задаються питанням: Що краще використовувати: KVM-перемикачі або програми з аналогічними функціями? Варто пам'ятати, що програми дистанційного керування працюють на сервері, тому якщо у функціонуванні сервера відбувся збій – саме в подібних випадках і необхідний віддалений доступ, – те досить імовірно, що програма дистанційного керування виявиться непрацездатною. З'єднання й інтерфейс KVM на базі IP реалізовані на базі спеціалізованих апаратних засобів і в працюючій операційній системі не мають потреби.

Для перемикачів KVM з підтримкою IP особливе значення мають функції забезпечення безпеки. Щоб при необхідності завжди можна визначити, хто й коли мав доступ до серверів і іншому мережному апаратному забезпеченню, усякий обіг користувача до системи рекомендується автентифікувати і протоколювати (з фіксацією часу події). У старшого адміністратора повинна бути можливість входу в сеанс іншого адміністратора і

його завершення. Ця функція служить свого роду «стоп-краном», коли з'ясовується, що сервер обслуговується неправильно або їм маніпулює хакер. Бажано, щоб продукт був сумісний з такими стандартами безпеки, як Data Encryption Standard (DES), Secure Sockets Layer (SSL) і сертифікати шифрування з відкритим ключем. Варто переконатися, що до KVM-З'єднань можна застосувати кілька рівнів безпеки й шифрування. Не можна допустити, щоб зломщик одержав доступ до консолі керування ключовими системами підприємства.

Потужне автоматичне шифрування (SSL з довжиною ключа як мінімум 128 біт) і автентифікація за допомогою сервера RADIUS повинні сприяти запобіганню перехоплення сигналів KVM при передачі по IP від перемикача до користувача. OSD для керування серверами в корпоративній області повинен мати великі функції конфігурування й забезпечення безпеки. До таким, наприклад, відносяться призначення імен серверам і визначення паролів – в ідеальному випадку разом з багатоступінчастою системою авторизації (приміром, певним адміністраторам дозволяється зчитувати інформацію тільки з екранів, у той час як інші мають права доступу до сервера). Перемикачі старшого класу звичайно пропонують диференційовані права доступу, а також профілі користувачів і систему користувальницьких прав.

Для обміну даними з перемикачем KVM використовується клієнтська програма, або браузер. Обидва підходи мають як свої достоїнства, так і недоліки; при виборі варто враховувати особливості конкретної реалізації. Якщо доступ до перемикача KVM потрібно надати лише декільком користувачам, то має сенс застосувати клієнтську програму. Але якщо доступ надається будь-якому адміністраторові незалежно від його місцезнаходження, те оптимальним рішенням буде клієнт на базі браузера.

Продуктивність багато в чому залежить від швидкості обробки відеосигналу. Варто з'ясувати, який метод стиску відеосигналу й інші міри економії смуги пропущення використовуються в перемикачі й клієнтській програмі. Добре, якщо постачальник надає доступ до демонстраційного перемикача, і користувачі можуть самостійно оцінити швидкодію й функціональність. При зіставленні продуктивності різних рішень потрібно обов'язково врахувати швидкість каналу зв'язку з демонстраційним перемикачем.

При виборі KVM-перемикача варто звертати увагу на наступні властивості:

– Багатоплатформеная сумісність: Вибирайте такий KVM-перемикач, що пропонує повну перехресну сумісність платформ (PC, MAC, Sun – з використанням адаптерів «Кабель категорії 5 –> PS/2» і «Кабель категорії 5 –> USB») і який працює з усіма апаратними засобами, операційними системами й прикладними програмами.

– Надійність: Можливість доступу на рівні базової системи уведення / виводу (BIOS), наявність засобів протокольно-незалежного доступу до мережі й доведені експлуатаційні якості. Не правильно думати, що всі KVM перемикачі створюються однаковими. Наприклад, інтерфейси уведення-виводу клавіатури й миші мають критичні вимоги до узгодження в часі, які можуть бути забезпечені інтелектуальною емуляцією, але виконання емуляції разюче відрізняються друг від друга залежно від фабричної марки перемикача. Переконаєтеся, що ви вибираєте високоякісний KVM перемикач, що може забезпечити оптимальне підвищення рівня відеосигналу – найбільш важкого для дублювання (відтворення) у сфері KVM технології.

– Гнучкість: Важливо вибирати такі KVM рішення, які пропонують широту номенклатури продукції, максимальне модульне нарощування виробів, підтримку багатоплатформеності, опції для локального й віддаленого доступу. Така важливість визначається постійними змінами у світі інформаційних технологій. Обране вами KVM-рішення повинне мати гнучкість, що дозволяє вам справлятися з усією складністю IT-операцій сьогодні й завтра.

– Нарощуваність: Зроблене KVM-рішення повинне вміти рости разом з ростом організації й міняти власний масштаб у міру того, як ви додаєте апаратні засоби й збільшуєте персонал, відповідальний за роботу інформаційного центра.

– Захищеність: Проблема захисту даних є головною турботою кожного мережного адміністратора. Ви повинні вибирати такі KVM перемикачі, які пропонують найвищий рівень захищеності, включаючи: керовані рівні безпечного доступу до серверів або груп серверів для одиничних або множинних користувачів; три типи шифрування даних, у яких використовуються найвищі стандарти брандмауерів; адресні фільтри із трирівневою ідентифікацією користувача.

– Опції доступу: Звертайте увагу на наявність самого повного набору опцій для KVM доступу з наявних на ринку сьогодні, для того, щоб обране вами рішення забезпечувало б оптимальну підтримку всіх операцій у вашім інформаційному центрі.

– Більше – не завжди краще: Існує безліч компаній, що пропонують KVM технології, – деякі із цих компаній більше по розмірі, чим інші. Існують інші компанії, менші по розмірі, які пропонують більше новацій, чим їх більші конкуренти. Ці компанії пишаються своїм високоякісним кредо й мають можливість поставляти найсучасніші KVM пристрою по значно меншої, у порівнянні з іншими, вартості.

Також варто звертати увагу на число одночасних сеансів, що обслуговуються перемикачем, габарити пристрою, тип кабелю для з'єднання із сервером і вплив відстані між перемикачем і серверами. Можливо, для підприємства будуть корисні додаткові функції, зокрема прості можливості моніторингу, оповіщення й дистанційного відключення живлення.

Існують два методи: каскадне з'єднання й шлейфове з'єднання.

Каскадне з'єднання KVM перемикачів

При каскадному з'єднанні KVM перемикачів обсяг KVM установки збільшується методом додатка перемикачів. У материнському KVM перемикачі виділяється комп'ютерний порт, до якого приєднується дочірній KVM перемикач. Тут численні дочірні перемикачі, що звисають долілиць із материнського, нагадують воду, що ніспадає каскадами у водоспаді.

Каскадне з'єднання перемикачів може істотно збільшити кількість комп'ютерів в установці. Однак, кожний материнський перемикач втрачає один порт для приєднання кожного каскадуємого KVM перемикача, що додається до установки.

При каскадному підключенні один з портів основного KVM-перемикача з'єднується з консольними роз'ємом додаткового. Подібним чином до основного KVM-перемикачу можна підключити трохи додаткових і істотно збільшити загальну кількість портів. Правда, у каскадного підключення є як мінімум два серйозних недоліки. По-перше, кожний з нижчестоящих KVM-перемикачів «віднімає» один порт в основного. По-друге, процедура вибору ПК, підключеного до порту KVM-перемикача нижнього рівня, не відрізняється зручністю – адже в цьому випадку необхідно виконати маніпуляції по перемиканню портів як на основному, так і на додатковому KVM-перемикачі.

Послідовне з'єднання KVM перемикачів

Більше зручним є шлейфове підключення: у цьому випадку трохи KVM-перемикачів з'єднуються в ланцюжок по спеціальній шині. Подібна можливість передбачена в ряді моделей сучасних KVM-перемикачів, орієнтованих на використання в корпоративному сегменті. При шлейфовому підключенні доступні для застосування всі порти як основного, так і додаткових KVM-перемикачів. Крім того, керування комутацією всіх портів можна здійснювати з меню основного KVM-перемикача.

При шлейфовому з'єднанні перемикачів збільшення ємності установки досягається методом її збільшення в обсязі. Перший у шлейфовому ланцюжку KVM перемикач називається провідної (Master), кожний наступний веденим (Slave). У типовій шлейфовій установці KVM перемикачі з'єднані один з одним як квітки ромашки в гірлянді, коли ви нарощуєте гірлянду, приплітаючи одну квітку до іншого.

Розробка структурної схеми

KVM-світчи підрозділяються на кілька категорій:

– KVM-світчи початкового рівня для домашнього застосування й невеликих офісів. Управляються за допомогою фізичної кнопки й не представляють особливого інтересу для зловмисника.

– KVM-світчи, що дозволяють перемикатися між приєднаними комп'ютерами за допомогою комбінації клавіш. Оскільки у визначенні натиснутих клавіш бере участь мікроконтролер, ці пристрої придатні для установки клавіатурного шпигуна.

– KVM-світчи, використовувані на підприємствах, які дозволяють більше щільну інтеграцію в різні системи. Ці пристрої набагато складніше й навіть можуть працювати на базі невеликих операційних систем. Тут у зловмисника найбільший простір для маневру.

У цій роботі ми будемо розглядати KVM-світч із другої категорії. Ситуація виникла під час одного із проектів, коли клієнт звернув увагу на порт RJ45 і попросив провести оцінку безпеки пристрою.

KVM-світч Belkin E Series OmniView 2-Port призначений для домашнього користування або невеликих офісів і дозволяє перемикатися між керованими комп'ютерами за допомогою комбінації гарячих клавіш. Ця модель була обрана як наочний зразок серед пристроїв даної категорії. Відповідно, результати аналізу застосовні до схожих моделей від інших виробників. На аукціоні eBay можна знайти екземпляри вартістю менш 10 фунтів.

Рисунок 1 – KVM-світч Belkin E Series OmniView 2-Port

Внутрішній пристрій світча

Усередині корпуса виявилися наступні компоненти:

– Мікроконтролер PIC16C57C. PIC-мікроконтролер (однократного програмування) випускаємий компанією Microchip Technology. Більша мікросхема, яка знаходиться в правій стороні задньої частини друкованої плати поруч із циліндричним чорним пристроєм, що видає звукові сигнали. Як видно на рисунку нижче, мікроконтролер вставлений у дворядний корпус, що сильно полегшує добування з метою наступного реверса-інжинірингу.

– 5 x 74HC4053D. Потрійні аналогові здвоєні мультиплексори, що випускаються компанією NXP. Подвійний мультиплексор може перемкнути одиночний вхід на один із двох виходів. Ці п'ять пристроїв, імовірно, формують основну логіку для перемикання клавіатури й миші PS/2 між одним із чотирьох вихідних портів.

Рисунок 2 – Внутрішній пристрій KVM-світча Belkin E Series OmniView 2-Port

Мікроконтролер PIC16C57C

Модель PIC16C57C належить сімейству популярних мікроконтролерів, що випускаються компанією Microchip Technology, які також популярні серед радіоаматорів. У мережі перебуває велика кількість доступної документації.

Документація містить відомості про програмування й протокол перевірки дійсності, що спрощує реверс-інжиніринг.

Аналіз прошивання

У специфікації по програмуванню/верифікації мікроконтролера PIC16C57C говориться про те, як виконати процедуру «швидкої верифікації». Потрібна наступна послідовність дій:

– Включити живлення (5В – пін Vdd, Земля – пін Vss).
– На піні T0CKI утримувати високий рівень.
– На піні OSC1 утримувати низький рівень.
– На піні Vpp подати напруга 13У (у цьому випадку мікроконтролер перейде в режим програмування й обнулится програмний лічильник).
– Значення поточного програмного лічильника можна вважати з пінів RA 0-RA3, RB 0-RB7 (в PIC16C57C використовується 12-бітне слово).
– На піні OSC1 установити високий рівень. Програмний лічильник збільшиться.
– На піні OSC1 установити низький рівень і повторити крок 5.
– Продовжувати доти, поки всі ділянки пам'яті не будуть лічені.

За допомогою цієї процедури спочатку буде лічений спеціальний конфігураційний регістр, що містить псевдо-адресу 0xFFF. Як тільки на піні OSC1 почнуть подаватися тактові імпульси (кроки 6 і 7), буде зчитується адреса 0x000, потім 0x001 і т.д.

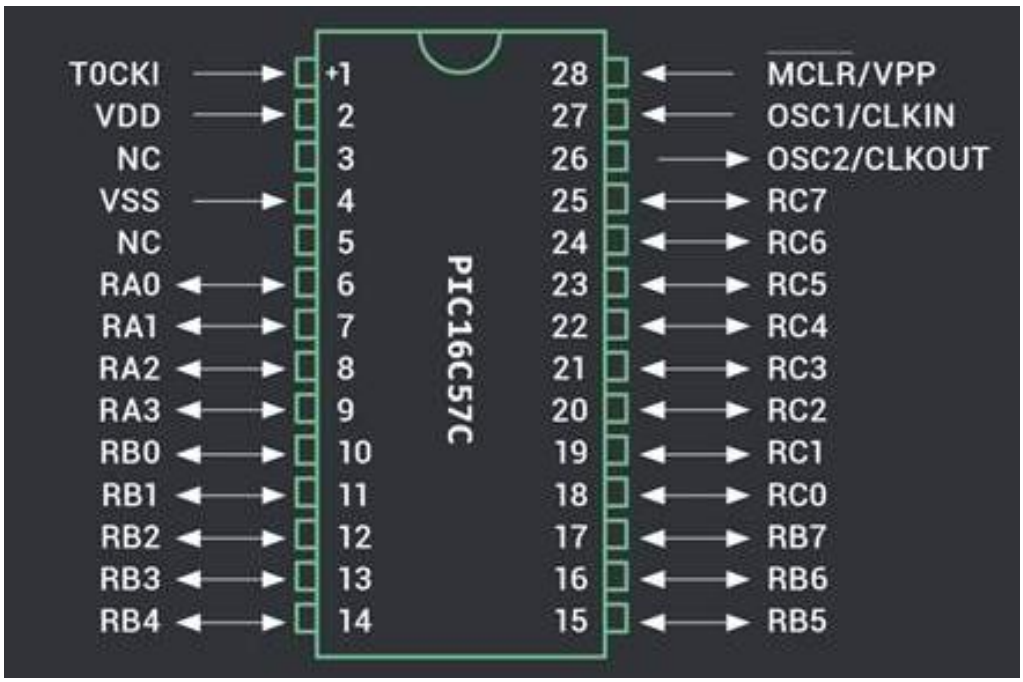


Рисунок 3 – Схема пінів мікроконтролера PIC16C57C

Створення верифікатора

Під час промислового програмування для читання вмісту пам'яті PIC-контролерів можна використовувати процедуру, описану вище. Є й інший шлях: відносно простий протокол-верифікатор на базі Arduino, системи розробки невеликих мікроконтролерів (або будь-якої іншої схожої системи з достатнім набором вхідних/вихідних пінів загального призначення, наприклад, Raspberry Pi). 13В потрібно підводити із зовнішнього джерела, оскільки в системах розробки на зразок Arduino і Raspberry Pi, передбачені напруги розміром 5В и нижче.

На рисунку нижче показана плата Arduino Uno, підключена до ZIF-сокету (Zero insertion force; з нульовим зусиллям зчленування) з підключеним мікроконтролером PIC16C57C, витягнутим з KVM-світча. Джерело живлення для подачі напруги 13В с метою активації режиму програмування також показаний. У наслідок обмежень плати Arduino Uno, можливе читання лише 4 бітів з мікроконтролера. Однак можна переконфігурувати пристрій так, щоб уважати інші біти й уміст PIC16C57C у кілька підходів. Інші плати (наприклад, Arduino Mega) мають досить кількість вхідних/вихідних пінів для одночасного зчитування всіх 12 бітів.

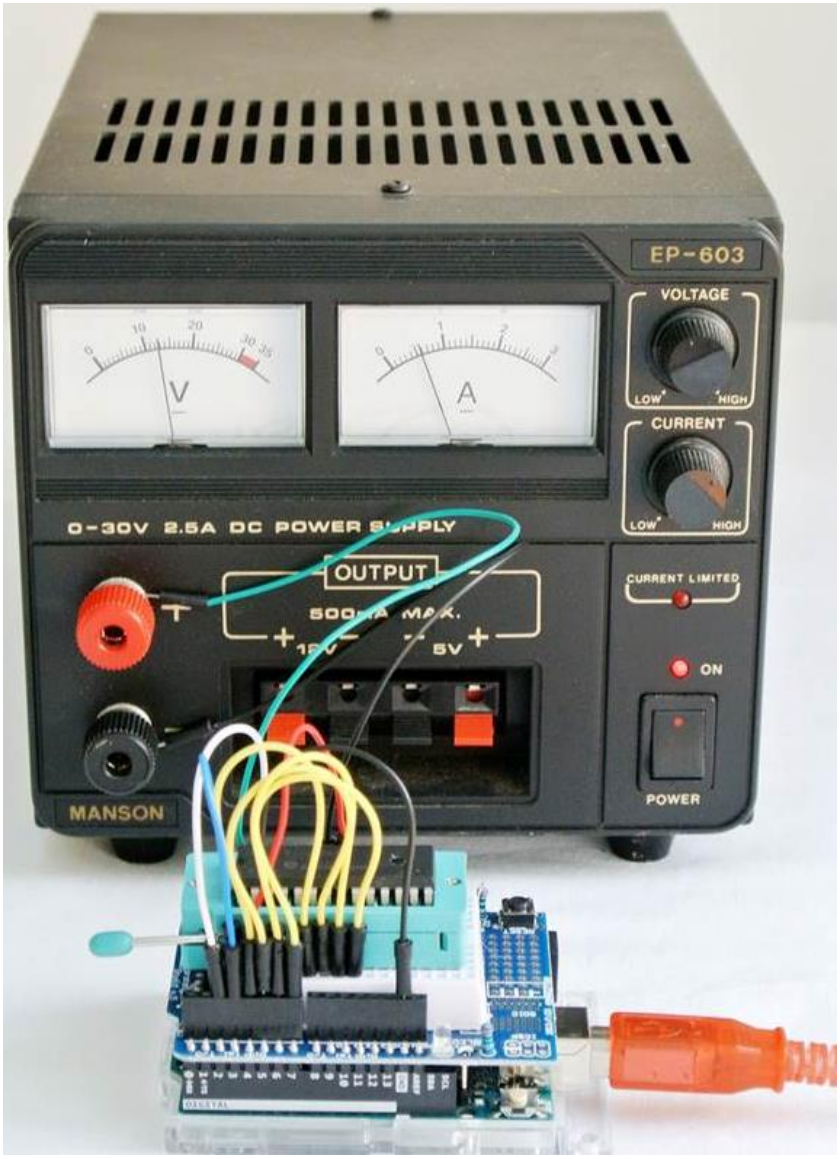


Рисунок 4 – Верифікація мікроконтролера PIC16C57C за допомогою Arduino

Захист коду

Перше, що потрібно вважати з мікроконтролера PIC16C57C, – уміст конфігураційного регістра, у якому перебуває інформація для системи безпеки й генератора, а також біт, пов'язаний із захистом коду. Якщо цей біт дорівнює нулю, захист коду включений, і в цьому випадку неможливо вважати вміст пам'яті (верифікація завершується успішно, але повертається значение, що, не містить інформацію, що перебуває по потрібній адресі в пам'яті).

На жаль, уміст конфігураційного біта в PIC16C57C, віддаленого з піддослідного KVM-світча, свідчило про те, що захист коду включений і вважати пам'ять неможливо.

Аналіз логіки роботи мікросхеми

Після аналізу прошивання в попередньому розділі стало зрозуміло, що вважати пам'ять мікроконтролера PIC16C57 неможливо. Таким чином, використання KVM-світча як клавіатурний шпигун можна домогтися двома способами:

– Проаналізувати логікові мікроконтролера PIC16C57C і перезаписати прошивання з нуля на еквівалентної PIC-мікросхемі.

– Проаналізувати частина логіки PIC16C57C і придумати спосіб, як підчепити другий мікроконтролер до набору пінів, використовуваних у пристрої, щоб відстежити натискання клавіш і реалізувати клавіатурний шпигун на базі другого мікроконтролера.

Дослідження призначення пінів

У мікроконтролері PIC16C57C є 20 вхідних/вихідних виводів загального призначення. Призначення цих пінів можна досліджувати за допомогою мультиметра, осцилографа або логічного аналізатора, приєднаних до потрібних виводів. Під час підключення до піну KVM-світч виконує певні функції й одночасно відслідковується сигнал на виводі з метою зіставлення виконуваної функції й вимірюваного сигналу. Перепади напруг на пінах можуть бути повільними (наприклад, коли включається/вимикається LED-підсвічування) або швидкими (наприклад, на інформаційній шині або шині, пов'язаної з такими сигналами). Швидкі перепади можна відстежити лише за допомогою осцилографа або логічного аналізатора.

Кожний пін повинен бути досліджений під час виконання різних функцій в KVM-світчі:

– Перемикання між вихідними портами.
– Набір на клавіатурі поки один з вихідних портів активний.
– Переміщення миші поки один з вихідних портів активний.
– Підключення системи до вихідного порту.
– Відключення системи з вихідного порту.

На рисунку нижче показаний підключений осцилограф, що використовувався для дослідження функціонального пінів під час натискань на клавіатурі.

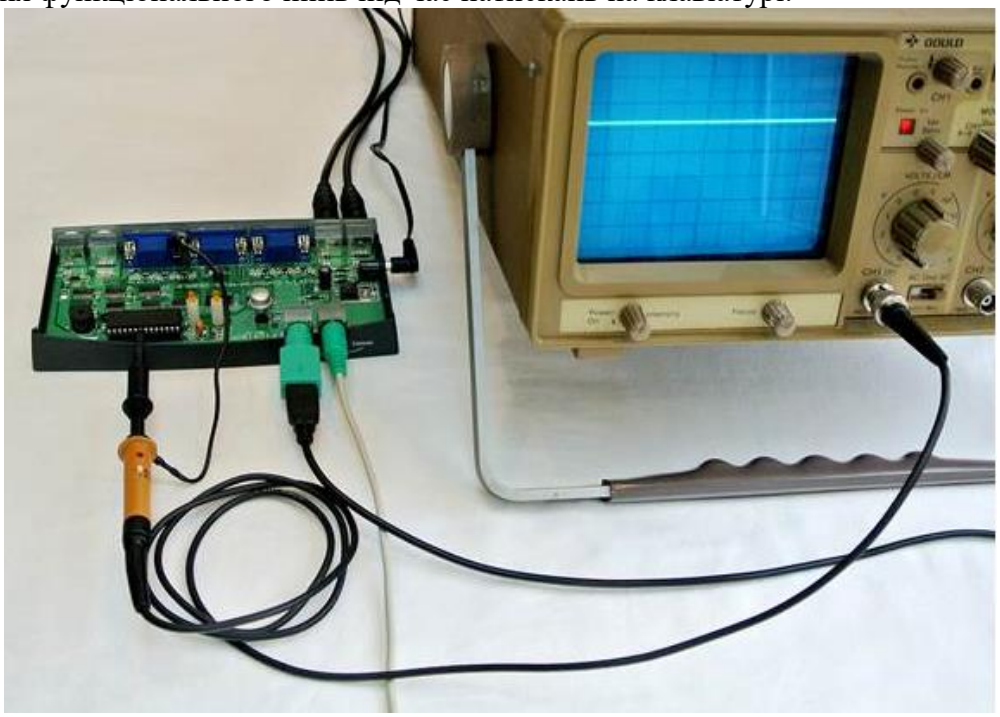


Рисунок 5 – Схема підключення осцилографа для дослідження функціональності пінів

Наступний аналіз друкованої плати можна зробити за допомогою мультиметра в режимі виміру опору, щоб визначити, які з пінів приєднані до інших компонентів. У випадку з KVM-світчем моделі Belkin дослідження значно полегшується, оскільки мікроконтролер PIC16C57C вставлений у рознімання, і ми можемо просто витягти мікросхему й виміряти опір між пінами й іншими компонентами.

Деякі піни мікроконтролера PIC16C57C мають незмінну функціональність (див. діаграму вихідного сигналу вище). Для нас особливий інтерес представляють вхідні/вихідні піни під номерами 6-25. Дослідження за допомогою осцилографа й мультиметра виявило наступне:

Піни 6-14

– Пін 6 – RA0 – Звичайно має високий рівень. Рівень знижується при натисканні на кнопковий перемикач. Швидше за все, це вхідний пін для кнопкового перемикача, використовуваний з метою зміни вихідного порту.

– Пін 7 – RA1 – Має низький рівень, коли обраний Порт 1, і високий – коли обраний Порт 2. Дослідження доріжок на друкованій платі виявило, що за змістом цей пін сполучається з виводами, пов'язаними з вибором вхідного сигналу, мультиплексорів 74HC4053D. Під час використання мультиметра в режимі виміру опору з'ясувалося, що цей пін з'єднано з виводами S1, S2, S3, пов'язаними з вибором вхідного сигналу, у мультиплексорах 74HC4053D (мікросхеми U7, U8, U9, U10). Таким чином, швидше за все, це вихідний пін, що вибирає вихідні Порти 1 і 2 в KVM-світче.

– Пін 8 – RA2 – Як і у випадку з Піном 7, при низькому рівні обраний Порт 1, при високому – Порт 2. При використанні мультиметра в режимі виміру опору з'ясувалося, що цей пін приєднано до виводів S1, S2 і S3 у мікросхемі U2, і до виводу OE1 мікросхеми U3 (функціональність схожа з мультиплексором). Таким чином, це ще один вихідний пін, що вибирає між вихідними Портами 1/2 світча. Поки до кінця не зрозуміло, чому Піни 7 і 8 мають схожу функціональність. Одна з версій: Пін 7 відповідає за керування й перемикання клавіатури й миші (рознімання PS/2), а Пін 8 – за перемикання відео. У цілому потрібно більше детальне розслідування.

– Пін 9 – RA 3 – Звичайно має високий рівень, але при перемиканні між портами KVM-світча спостерігаються зміни. Під час перемикання портів сигнал на цьому піні на осцилографі відображається у вигляді хвилі зі структурою приблизно 3 періоди на сантиметр при масштабі 1мс/см. Тобто в нас виходить хвиля із частотою 3кГц. Швидше за все, цей пін прямо управляє звуковим пристроєм. При певних обставинах (наприклад, при перемиканні між вихідними портами) KVM-світч видає короткий пронизливий звук (частотою близько 3 кГц).

– Пін 10 – RB0 – Високий рівень, якщо до вихідного Порту 1 світча підключений пристрій. Швидше за все, цей дозвіл на роботу із пристроєм, підключеним до Порту 1. Під час перемикання між портами, на цьому піні з'являється низький рівень протягом значного періоду (протягом приблизно 1 секунди), а потім знову з'являється високий рівень. У період низького рівня на цьому піні, на Порті 1 відсутні сигнали, хоча є активність на пінах 20-23 (миша/клавіатура). Примітний ще й той факт, що LED-підсвічування, що сигналізує про те, що порт обраний, також не міняється під час низького рівня (протягом приблизно однієї секунди).

– Пін 11 – RB1 – Високий рівень, якщо до вихідного Порту 2 світча підключений пристрій. Швидше за все, цей дозвіл на роботу із пристроєм, підключеним до Порту 2. Під час перемикання між портами, на цьому піні з'являється низький рівень протягом значного періоду (протягом приблизно 1 секунди), а потім знову з'являється високий рівень. У період низького рівня на цьому піні, на Порті 2 відсутні сигнали, хоча є активність на пінах 20-23 (миша/клавіатура). Примітний ще й той факт, що LED-підсвічування, що сигналізує про те, що порт обраний, також не міняється під час низького рівня (протягом приблизно однієї секунди).

– 12 – RB2 – Високий рівень – Активність відсутня – відсутні з'єднання на друкованій платі.

– 13 – RB3 – Низький рівень – Активність відсутня – відсутні з'єднання на друкованій платі.

– 14 – RB4 – Високий рівень – Активність відсутня. На друкованій платі присутня доріжка, що приблизно веде до Піну 14 мікросхеми U9. Гіпотеза підтверджена мультиметром у режимі виміру опору. Це вхідний пін 'Input 1' у мультиплексорі 74HC4053, що буде як перемикач між піном Порта 1 і Порта 2 засобами мультиплексора. Цей пін може бути вхідним або вихідним, і, таким чином, KVM-світч буде або відсилати сигнал коннектору PS/2, з'єднаному з вихідним портом, або одержувати сигнал назад. Однак активності на цьому піні виявлено не було при реалізації різних сценаріїв.

Піни 15-25

– Пін 15 – RB5 – Високий рівень – Активність відсутня – відсутні з'єднання на друкованій платі.

– Пін 16 – RB6 – Високий рівень – Активність відсутня – відсутні з'єднання на друкованій платі.

– Пін 17 – RB7 – Високий рівень – Активність відсутня – відсутні з'єднання на друкованій платі.

– Пін 18 – RC0 – Низький рівень – Активність відсутня – відсутні з'єднання на друкованій платі.

– Пін 19 – RC1 – Високий рівень – Активність відсутня – відсутні з'єднання на друкованій платі.

– Пін 20 – RC2 – Миша PS/2 – Тактові імпульси. Осцилограф показує стабільну серію імпульсів під час переміщення миші. Регулярність імпульсів натякає на те, що цей генератор призначений для миші. Деяка активність на цьому піні була виявлена під час перемикання між вихідними портами, але коли миша не рухалася.

– 21 – RC3 – Миша PS/2 – Дані. Осцилограф показує нерегулярні імпульси під час руху миші. Нерегулярність імпульсів натякає на те, що це інформаційний пін, призначений для миші. Деяка активність на цьому піні була виявлена під час перемикання між вихідними портами, але коли миша не рухалася. Див. коментарі нижче, що стосуються призначення пінів 10-11.

– 22 – RC4 – Клавіатура PS/2 – Тактові імпульси. Осцилограф показує стабільну серію імпульсів на цьому піні при натисканні або відпусканні клавіші. Регулярність імпульсів натякає, що цей генератор призначений для клавіатури.

– 23 – RC3 – Клавіатура PS/2 – Дані. Осцилограф показує нерегулярні імпульси під час натискання або відпускання клавіші. Нерегулярність імпульсів натякає на те, що це інформаційний пін, призначений для клавіатури.

– 24 – RC6 – LED1. Цей пін прямо пов'язаний зі станом LED для Порта 1. Швидше за все, вихідний пін для керування підсвічуванням.

– 25 – RC7 – LED2. Цей пін прямо пов'язаний зі стан LED для Порта 2. Швидше за все, вихідний пін для керування підсвічуванням.

Призначення пінів 10-11: Ізоляція виходів

Як було відзначено вище, на пінах 10-11 під час перемикання з'являється низький рівень. Крім того, під час перемикання була замічена активність на інформаційні й тактових пінах, пов'язаних з роз’ємом PS/2 (20-23). Швидше за все, KVM-світч тимчасово відключає виходи рознімання PS/2 і посилає сигнали скидання для миші й клавіатури, які беруть участь у процесі перемикання. Протокол, використовуваний роз’ємом PS/2, є двонаправленим, дозволяючи хосту управляти функціями підключеного пристрою. Наприклад, можна встановлювати індикатори стану клавіш Caps lock, Num lock і т.д. KVM-світчу потрібно стежити за цими налаштуваннями для кожного пристрою (клавіатури й миші) у розрізі по хосту/порту. При перемиканні між портами необхідно відновлювати останній збережений стан для кожного хоста. Щоб вирішити це завдання під час перемикання, KVM-світч виставляє на піні 10 або 11 низький рівень для відключення відповідного вихідного порту. Потім відбувається відсилання сигналів по шині PS/2 до підключеної миші або клавіатури для обнуління стану. Виставляння низького рівня на піні 10 або 11 необхідно для того, щоб хост, підключений до вихідного порту, не міг відслідковувати сигнал між KVM-світчем і мишею/клавіатурою.

Крім того, KVM-світч підтримує перемикання за допомогою гарячих клавіш. Вхід у цей режим здійснюється після подвійного натискання клавіші «Scroll Lock». Потім з'являється звуковий сигнал, що сигналізує, що пристрій перейшов у стан для зчитування гарячих клавіш, і світч очікує натискання додаткових клавіш протягом 1 секунди. Будь-яке натискання протягом цього часу інтерпретується KVM-світчем і не відсилається приєднаному комп'ютеру. Цей функціонал вимагає, щоб вихідні порти, підключені до шини

PS/2, були відключені в той час, поки світч очікує натискання гарячих клавіш, що досягається за допомогою виставляння на піні 10 або 11 низького рівня.

Неповний аналіз

Аналіз, проведений вище, виявив багато нового щодо функціональності KVM-світча. Однак залишилися деякі нез'ясовані моменти. На декількох пінах (12-19) не було замічено ніякої активності під час роботи з KVM-світчем. Якби на цих пінах завжди був високий рівень, що означає звичайно стандартний або неактивний стан, можна було б зробити припущення, що ці виводи не використовуються. Однак той факт, що на деяких пінах був низький рівень, натякає на те, що можливо дані виводи використовуються. Дослідження доріжок на друкованій платі показало, що приєднано тільки Пін 14, але поки з незрозумілим призначенням.

Оскільки аналіз є неповним, відновлення робочого прошивання з нуля, може стати непростим завданням. Виходить, для впровадження клавіатурного шпигуна в нас залишається другий варіант, пов'язаний з підключенням другого мікроконтролера.

Інтерфейс PS/2

Щоб одержати доступ до інформації, що вводиться із клавіатури, в інтерфейсах PS/2, використовуваних на KVM-світчі, необхідно розуміти, як улаштований цей протокол.

Інтерфейс PS/2 може управляти або хостом, або пристроєм, підключеним до вихідного порту. Електричні характеристики цього інтерфейсу мають на увазі, що можливо впровадити дані в шину PS/2 навіть, коли до неї підключені одночасно й хост і пристрій. Цей факт корисно взяти до уваги при впровадженні додаткового контролера в KVM-світч.

Реалізація клавіатурного шпигуна

З огляду на міркування вище, ми можемо підключити другий мікроконтролер до PIC16C57C для реалізації клавіатурного шпигуна. В ідеалі повинні використовуватися тільки сигнали на пінах мікроконтролера PIC16C57C, що дозволить реалізувати схожу функціональність у прошиванні додаткового контролера.

Знімання зібраної інформації варто реалізовувати на базі вже існуючих інтерфейсів KVM-світча. Згодом зловмисникові знадобиться лише фізичний доступ до KVM-світчу для добування зібраної інформації. На другому мікроконтролері потрібно реалізувати додаткову послідовність натиснутих клавіш, при активації якої буде відбуватися вивантаження записаних натискань у систему, підключену до KVM-світчу. Потім зловмисник може відкрити текстовий редактор на цільовій системі й нажати комбінацію гарячих клавіш для вивантаження записаної інформації в текстовий файл.

Обмеження по електричних характеристиках

Існує серйозне обмеження при підключенні другого мікроконтролера до PIC16C57C, що полягає в тому, що сигнал будь-якого пина, зконфигурованого як вихідного в PIC16C57C, не може бути переключений в інший стан додатковим мікроконтролером. Витримка з даташита на мікроконтролер PIC16C57C (розділ 7.6.1):

«Пін, що видає високий або низький рівень не повинен одночасно управлятися зовнішнім пристроєм для зміни рівня сигналу на цьому виводі (за допомогою елементів «Логічне Або», «Логічне І»). Результуючі вихідні струми можуть зіпсувати чип».

Цей факт означає, що реалізація клавіатурного шпигуна й вивантаження зібраної інформації повинна бути на базі пінів мікроконтролера PIC16C57C, які зконфігуровані як вхідні.

Спільне використання шини PS/2

Один з варіантів для добування інформації із клавіатурного шпигуна – відправлення даних як серії натиснутих клавіш на приєднаний хост. Щоб вирішити це завдання, KVM-світч повинен взяти на себе роль периферичного пристрою (клавіатури) на шині PS/2 і налагодити комунікацію з хостом від імені «підробленої» клавіатури. Однак у той же час шина PS/2 буде приєднана до справжньої клавіатури. Тут виникає закономірне питання, чи можливо добування інформації в при таких обставинах.

Шина PS/2 спроектована для прямого з'єднання між хостом і периферичним пристроєм. Це простий двоканальний протокол (тактові імпульси й інформаційна шина), що підтримує двосторонню комунікацію. Цей функціонал заснований на інтерфейсі з відкритим колектором для тактового й інформаційного пінів, дозволяючи або хосту, або периферичному пристрою встановлювати низький рівень на кожному з пінів.

Таким чином, чисто з позиції електричних характеристик другий периферичний пристрій (KVM-світч) може управляти тактовим і інформаційним пінами інтерфейсу PS/2. З погляду хоста, периферичні пристрої (справжня клавіатура або KVM-світч, що працює в якості «підробленої» клавіатури) будуть нерозрізнені. Однак тут виникає питання, чи буде провокувати активність «підробленої» клавіатури несподіване поводження справжньої клавіатури.

У протоколі PS/2 більша частина комунікацій відбувається між периферичним пристроєм і хостом. Тактові імпульси й інформацію більшу частину часу генерує периферичний пристрій. Якщо хосту потрібно відправити інформацію периферичному пристрою, наприклад, установити стан LED-Індикації для клавіші Caps Lock), то спочатку хост сповіщає периферичний пристрій про те, що планується пересилання інформації, за допомогою втримання низького рівня більше 100 мкс як частини сигналу для «запиту на відправлення». Таким чином, складність полягає в тому, що активність на шині PS/2 з боку KVM-світча, що функціонує в якості «підробленої» клавіатури, може бути інтерпретовано справжньої клавіатури як «запит на відправлення» від хоста.

При відсиланні сигналів по шині PS/2 периферичний пристрій генерує тактові імпульси в діапазоні 10-16.7 Кгц, і тривалість імпульсу 100 мкс буде відповідати найнижчій тактовій частоті (10 кГц). Таким чином, щоб активність підробленою клавіатурою не інтерпретувався як «запит на відправлення», потрібно знижувати рівень максимум на 50 мкс. У цьому випадку загальне використання шини PS/2 стає можливим.

Детектування натискання послідовності гарячих клавіш

Вивантаження знятої інформації буде активуватися за допомогою додаткового натискання послідовності гарячих клавіш. Спочатку потрібно двічі нажати клавішу «Scroll Lock» протягом певного часу. Потім PIC16C57C виставляє низький рівень на відповідному піні (10 або 11), пов'язаним з підключенням вихідних портів, протягом близько 1 секунди для запобігання відсилання натиснутих клавіш хосту. Протягом цього часу очікується натискання послідовності натиснутих клавіш. Наприклад, натискання клавіші «1» або «2» приведе до перемикання на вихідний порт 1 або 2 відповідно.

Існує два шляхи для реалізації натискання клавіш із метою добування збереженої інформації:

– Незалежно детектувати подвійне натискання клавіші «Scroll Lock» другим мікроконтролером.

– Детектувати низький сигнал на пінах, пов'язаним з підключенням вихідних портів, що сигналізує про натискання послідовності палаючих клавіш.

При незалежному детектуванні подвійного натискання «Scroll Lock» є ризик, що PIC16C57C і другий мікроконтролер не зможуть виявити цей факт у те саме час. Відповідно, потрібно використовуватися другий спосіб, пов'язаний зі станом пінів, що підключають вихідні порти, оскільки цей метод більше надійний для визначення того, що KVM-світч очікує натискання гарячих клавіш.

Експериментальне встаткування

При виготовленні експериментальної версії клавіатурного шпигуна використовувалася плата Arduino Uno. На цій платі є вхідні/вихідні піни й середовище програмування на базі мови C++, за допомогою якої можна одержувати доступ до виводів з метою установки прототипів.

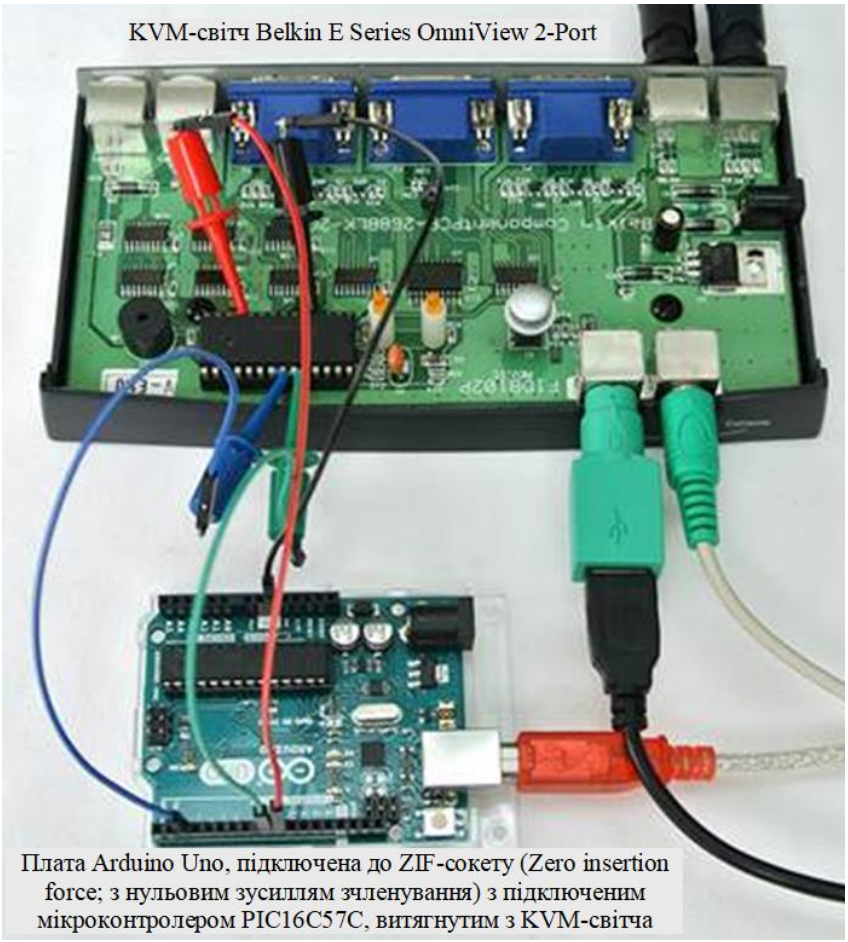


Рисунок 6 – Структурна схема системи

Експериментальна версія клавіатурного шпигуна на базі плати Arduino Uno, на рисунку вище, показана плата, підключена до мікроконтролера PIC16C57C, використовуваного KVM-світчем.

– Чорний щуп: Пін 4 у мікроконтролері PIC16C57C (земля). Відповідно, земля й на платі Arduino.

– Синій щуп: Пін 22 у мікроконтролері PIC16C57C (пін з тактовими імпульсами клавіатури PS/2). Цифровий I/O Пін 2 на платі Arduino.

– Зелений щуп: Пін 23 у мікроконтролері PIC16C57C (інформаційний пін клавіатури PS/2). Цифровий I/O Пін 8 на платі Arduino.

– Червоний щуп: Пін 11 у мікроконтролері PIC16C57C (розв'язний сигнал для вихідного порту 2 в KVM-світче). Цифровий I/O Пін 9 на платі Arduino.

В експериментальних цілях використовується тільки шина, що включає Порт 2.

Висновок. У статті розглянуто та проаналізовано програмне забезпечення, створене в результаті виконання роботи, призначено для клавіатурного шпигуна в KVM-switch побудованого на базі мікроконтролера PIC16C57C. В межах України в недостатній мірі представлені вітчизняні розробки в цій області. У роботі наведені теоретичне узагальнення й рішення наукового завдання дослідження методів реалізації клавіатурного шпигуна в KVM-switch побудованого на базі мікроконтролера PIC16C57C. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем реалізації клавіатурного шпигуна в KVM-switch побудованого на базі мікроконтролера PIC16C57C; Досліджена система реалізації клавіатурного шпигуна в KVM-switch побудованого на базі мікроконтролера PIC16C57C; На основі отриманих результатів досліджень створена програмна реалізація клавіатурного шпигуна в KVM-switch побудованого на базі мікроконтролера PIC16C57C. Розроблені під час виконання роботи алгоритми дозволяють

успішно вирішувати завдання реалізації клавіатурного шпигуна в KVM-switch побудованого на базі мікроконтролера PIC16C57C. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки. Розроблене програмне забезпечення має простий, дружній та зручний інтерфейс користувача, що забезпечує легкість у освоєнні роботи програмного продукту, зручність у використанні, і не потребує особливих спеціальних знань. При створені програмного забезпечення було використано об'єктно-орієнтований підхід, що відповідає сучасним тенденціям у галузі розробки комерційних програмних систем. Програма реалізована на мові високого рівня C++. Дана мова програмування дозволяє найбільш ефективно обробляти дані. Це дозволило мінімізувати строк розробки програмного забезпечення, і, як слід, зменшити витрати на його розробку. Запропоноване програмне забезпечення ділиться на загальне програмне забезпечення, що поставляється із засобами обчислювальної техніки й спеціальне програмне забезпечення, що спеціально розроблене для даної конкретної системи й включає програми, що реалізують її функції. Програма призначена для виконання на KVM-світчі на базі платформи Arduino. Даються необхідні рекомендації з установки розробленого програмного забезпечення. Для підвищення рівня безпеки запропоновано застосовувати алгоритм RSA.

Список літератури

1. Смирнов А.А. Математическая формализация процесса проектирования объектно-ориентированного программного обеспечения информационных систем / А.А. Смирнов, А.П. Доренський // Информационные технологии и системы в управлении, образовании, науке: монография под ред. проф. В.С. Пономаренко. – Х.: Цифрова друкарня № 1, 2014. – С. 22-36. – ISBN 978-617-7188-50-5.
2. Смірнов О.А. Дослідження впливу ступеня стиснення зображень на оперативність їх доставки у телекомунікаційній системі / О.А. Смірнов, О.М. Дрєєв, О.П. Доренський // Системи обробки інформації. – 2013. – Вип. 8(115). – С. 234-239.
3. Смірнов О.А. Аналіз процесів стиснення та відновлення зображень на основі цифрових методів // О.А. Смірнов, О.П. Доренський, О.М. Дрєєв // Наука і техніка Повітряних сил Збройних Сил України. – 2013. – № 3(12). – С.122-127.
4. Доренський О.П. Формалізація процесу зміни станів програмних об'єктів складних систем на основі формального апарату скінченних автоматів Мура / О.П. Доренський, О.А. Смірнов // Зв'язок : Науково-виробничий журнал. – 2014. – № 3 (109) – С. 27-31.
5. Доренський О.П. Синтез структури інтегрованої моделі об'єктно-орієнтованого програмного забезпечення / О.П. Доренський // Системи обробки інформації. – 2014. – Т. 2, Вип. 2(118). – С. 68-72.
6. Dorensky O. Method of the Models' Synthesis for Software Automated System Objects' States in Digital Images Processing / Oleksandr Dorensky // Збірник наукових праць Кіровоградського національного технічного університету: Техніка в сільськогосподарському виробництві, галузеве машинобудування, автоматизація. – 2014. – Вип. 27. – С. 283-292.
7. Доренський О.П. Метод синтезу тестових структур взаємодії програмних об'єктів під час проектування програмного забезпечення на основі об'єктно-орієнтовної технології / О.П. Доренський // Системи управління, навігації та зв'язку. – Полтава: ПолтНТУ, 2014. – Вип. 3 (31). – С. 107–114.
8. Доренський О.П. Метод синтезу тестових моделей поведінки програмних об'єктів інформаційно-телекомунікаційної системи спеціального призначення / О.П. Доренський // Збірник наукових праць Харківського університету Повітряних Сил. – 2014. – Вип. 3(40). – С. 109-112.
9. Dorensky O. Development of the theoretical bases of logical domain modeling of a complex software system / Oleksandr Dorensky, Alexey Smirnov // International Journal of Computational Engineering Research (IJCER). – India, Delhi, 2014. – Vol. 4, Issue 4. – P. 19-23.
10. Доренський О.П. Дослідження помилок програмного забезпечення // О.П. Доренський, О.М. Змеул // Актуальні задачі сучасних технологій : Міжнар. наук.-техн. конф., 19-20 груд, 2012 р. : збірн. тез доп. – Тернопіль, 2012. – С. 187-188.

УДК 004

В. Данчул, магістр гр. КН-18-1,4
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ ЗАХИСТУ КОРПОРАТИВНОЇ МЕРЕЖІ З ЗАСТОСУВАННЯМ SPI FIREWALL

У статті розроблено програмне забезпечення, яке призначено для системи захисту корпоративної мережі з застосуванням SPI Firewall. Метою розробки є дослідження та програмна реалізація системи захисту корпоративної мережі з застосуванням SPI Firewall. Об'єктом дослідження є процес захисту корпоративної мережі з застосуванням SPI Firewall. Предметом дослідження є методи захисту корпоративної мережі з застосуванням SPI Firewall. Методи дослідження базуються на методах захисту інформації, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи захисту корпоративної мережі з застосуванням SPI Firewall. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

комп'ютерні науки, захист корпоративної мережі, SPI Firewall

Постановка проблеми. SPI (stateful packet inspection) – це функція Інтернет-маршрутизаторів, при включенні якої відбувається додаткова перевірка пакетів на приналежність існуючому з'єднанню. При встановленні будь-якої сесії TCP/IP NAT відкриває для неї порт. Після завершення сесії порт ще кілька хвилин залишається відкритим. Теоретично, якщо в цей момент відбувається атака на роутер шляхом сканування відкритих портів, то з'являється можливість проникнення у внутрішню мережу. Або ж атакуючий може намагатися посилати пакети на цей відкритий порт протягом сесії. При включенні функції SPI відбувається запам'ятовування інформації про поточний стан сесії й відбувається аналіз всіх вхідних пакетів для перевірки їхньої коректності.

У випадку некоректності вхідного пакета (наприклад, адреса відправника не дорівнює адресі, до якого посилав запит або номер пакета не відповідає очікуваному) – такий пакет блокується й у лозі з'являється запис про таку подію.

Для включення SPI спочатку потрібно настроїти підключення до інтернет-маршрутизатору по локальній мережі, підключитися веб-браузером по IP-адресі інтернет-маршрутизатора, увести ім'я й пароль для входу на сторінку налаштувань (відповідно до прикладеного до нього документації).

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у системі захисту корпоративної мережі з застосуванням SPI Firewall.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи захисту корпоративної мережі з застосуванням SPI Firewall.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем захисту корпоративної мережі з застосуванням SPI Firewall.
– Дослідження системи захисту корпоративної мережі з застосуванням SPI Firewall.
– Програмна реалізація системи захисту корпоративної мережі з застосуванням SPI Firewall.

Об'єктом дослідження є процес захисту корпоративної мережі з застосуванням SPI Firewall.

Предметом дослідження є методи захисту корпоративної мережі з застосуванням SPI Firewall.

Методи дослідження базуються на методах захисту інформації, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Необхідність захисту інформації стала причиною створення окремого напрямку в комп'ютерній індустрії, немаловажну роль у якому грає розвиток технології Firewall. Сьогодні жоден комп'ютер, що має доступ у мережу Інтернет, не може обійтися без міжмережевого екрана (SPI Firewall) і антивірусу. SPI Firewall сьогодні – це фундамент системи інформаційної безпеки (ІБ), саме тому необхідно знати про актуальні тенденції у світі ІБ, про те як розвивався SPI Firewall, які зміни перетерпів на своєму еволюційному шляху, як сьогодні застосовується в сучасних технологіях і які його подальші перспективи.

Розвиток технології

Технології SPI Firewall спочатку будувалися на фільтрації пакетів, що здійснювалася на основах статичних даних у заголовках. Кожний IP-пакет перевірявся на відповідність інформації в заголовку із припустимими правилами, записаними в SPI Firewall. Якщо заголовок пакета не задовольняв заданим критеріям, він не пропускався в захищену мережу. Даний метод фільтрації був досить недосконалий, оскільки не давав можливості перевіряти вміст пакетів. Тому згодом з'явилися міжмережеві екрани на основі проксі-фільтрів, здатні аналізувати не тільки заголовки пакетів, але й пересилаються данние, що. Це дало можливість управляти інформацією про сесію передачі даних і контролювати її.

Повноцінне UTM-пристрій повинне в першу чергу забезпечувати багаторівневий захист мережі, для чого в ньому повинні бути реалізовані функції міжмережевого екрана й системи виявлення вторгнень, що дозволяють проводити глибокий аналіз потоку даних і передавати інформацію про підозрілий трафік різним рівням пристрою.

Список небезпек, що загрожують мережам, розширювався, погрози ставали складніше й постійно змінювалися. Захист від них, безумовно, була, але реалізовувалася вона у вигляді незалежних друг від друга рішень, кожне з яких необхідно було встановлювати, набудовувати й обслуговувати окремо. Щоб збільшити продуктивність систем захисту й полегшити керування ними, були розроблені спеціальні пристрої для об'єднаного керування погрозами – універсальні апаратні рішення, які могли захистити локальну мережу від більшості погроз. Такий клас устаткування для захисту мережних ресурсів одержав назву UTM-рішень (Unified Threat Management) – багатофункціональні програмно-апаратні комплекси, у яких сполучені функції різних пристроїв: міжмережевого екрана з функціями антивірусного фільтра, системи запобігання вторгнень, системи боротьби зі спамом, системи URL-фільтрації, а також VPN-технології.

Погрози й захист

Іншою обов'язковою функцією є антивірус, що перевіряє трафік на віруси, чирви, шпигунське ПЗ та інші шкідливі коди на основах бази даних сигнатур. Небезпечний трафік визначається й зупиняється в режимі online, перш ніж він зможе ушкодити мережа.

Окремо варто відзначити додаткові можливості по захисту від небезпечних Web-сайтів і спаму. Служба URL-фільтрації дозволяє заборонити співробітникам компанії відвідувати небезпечні сайти, які можуть бути джерелами різного виду погроз.

Споконвічно SPI Firewall сформувався як комплекс програмних засобів, що коштує між мережним адаптером і операційною системою. Але проблеми сумісності апаратних компонентів, операційної системи й програмного забезпечення SPI Firewall привели до того, що паралельно із програмними міжмережевими екранами стали розвиватися програмно-апаратні комплекси захисту, які являли собою апаратні пристрої з попередньо встановленим і зконфігурованим на них програмним забезпеченням міжмережевого екрана й операційною системою. Ці пристрої володіли набагато більше стабільними параметрами продуктивності, розширеними мережними можливостями, посиленими функціями безпеки, а також значно збільшеною надійністю.

Якщо говорити про спам, то він не тільки може нести в собі потенційну небезпеку, але також здатний перевантажити мережні ресурси й знизити продуктивність праці співробітників. Використання виділеної служби блокування спаму дозволяє зупинити зайвий трафік на мережному шлюзі, перш ніж він досягне внутрішнього поштового сервера.

Переваги

Необхідно відзначити, що в порівнянні з використанням окремих систем робота з комплексом UTM має цілий ряд переваг, першим з яких є вартість його впровадження. Інтегровані системи використовують набагато менше встаткування на відміну від рішень багаторівневої безпеки, які будуються за допомогою безлічі окремих пристроїв. Це, безумовно, відбивається на підсумковій вартості.

Програмно-апаратні комплекси сьогодні є основою для побудови захисту корпоративної мережі, у той час як програмні в більшій мері використовуються для забезпечення безпеки приватних користувачів.

Другою перевагою використання концепції UTM є те, що зупинка вторгнень здійснюється на мережному шлюзі, а не на сервері або робочій станції. Таким чином, швидкість трафіку не знижується, і чутливі до швидкості застосунку залишаються доступними для роботи.

По-третє, простота установки й конфігурації захисту. Керування пристроями й службами легко налаштовується за допомогою інтегрованих систем із централізованим керуванням, що значно спрощує роботу адміністраторів і скорочує кількість необхідних людських ресурсів.

Відповідь викликам часу

Концепція UTM-пристроїв для побудови системи ІБ на сьогоднішній день є стандартною й загальновизнаною. Подібні рішення розраховані на мережі різного масштабу й дають можливість багатьом компаніям перейти на більше високий рівень захисту своїх мереж. Але сучасні тенденції в розвитку UTM-пристроїв такі, що сьогодні ринку потрібні рішення наступного покоління з розширеними функціями керування й забезпечення безпеки, підвищеним рівнями продуктивності, масштабованості, надійності й економічності.

SPI Firewall (firewall; брандмауер або міжмережевий екран) – це один з основних компонентів, необхідних для організації захисту периметра мережі й персональних комп'ютерів окремих користувачів. Функція SPI Firewall полягає в тому, щоб контролювати взаємодія зовнішньої й внутрішньої мережі за допомогою фільтрації всього вхідного й вихідного трафіку, ґрунтуючись на заданих правилах.

Тому деякі розроблювачі розширили поняття комплексного захисту комп'ютерних мереж від погроз, доповнивши категорію UTM новим визначенням XTM (eXtensible Threat Management) – розширюване керування погрозами. Розширюваність має на увазі можливість додавання окремих компонентів, тобто пристрою XTM адаптуються до динамічного мережного оточення й одночасно захищають мережу від раніше невідомих погроз. У концепції XTM поліпшений і розширений ряд функціональних характеристик UTM. XTM-пристрої здатні проводити глибоку перевірку HTTPS-трафіку, перехоплюючи, обробляючи й перебудовуючи потоки даних HTTPS із застосуванням контентної фільтрації, створюючи списки виключень для відвідування потенційно небезпечних сайтів. Крім того, у зв'язку з поширенням технології VoIP у бізнес-секторі XTM-пристрою запропонували убудований захист VoIP-протоколу.

Нові функції

У рішення XTM додані засоби аналізу репутації інтернет-сайтів, реалізовані на основі хмарних технологій – функція Reputation Enabled Defense (RED). Служба RED заснована на технології хмарного середовища, що являє собою спеціалізовані сервери зберігання репутаційних оцінок публічних хостів. Якщо користувач намагається встановити з'єднання із сайтом з низькою репутацією, RED передає команду сервісу URL-фільтрації на виконання блокування доступу. Якщо ж здійснюється підключення до сайту з позитивною репутацією, то дані, передані між користувачем і сайтом, не піддаються антивірусній перевірці, що

прискорює Web-доступ до ресурсу. Подібна функція дозволяє оптимізувати пропускну здатність і звільнити мережні ресурси для обробки тільки законного, нешкідливого трафіку.

Засобами Application Control можна дозволити використання програми Google Talk для обміну миттєвими повідомленнями, але заборонити в даному додатку передачу файлів між користувачами. SPI Firewall з функцією Application Control здатний також виявляти всі застосунки, що намагаються проникнути в мережу, у тому числі й зашифровані – спеціально розроблені для обходу стандартних мір безпеки.

Новітня й перспективна функція, реалізована в пристроях серії XTM, – це контроль застосунків (Application Control). Новий сервіс дозволяє відстежити, які застосунки використовуються в компанії, хто їх використовує й коли.

Тепер міжмережевий екран одержує додаткові функції: з його допомогою можна не тільки управляти доступом у мережу, але й вибірково дозволяти або забороняти роботу певних мережних застосунків або навіть окремих їхніх функцій, розмежовуючи доступ по відділах компанії, посадовим обов'язкам співробітників і часу доби.

Сервіс Application Control дає можливість створювати звіти з відображенням хронології запуску застосунків, що дозволяє перевіряти дотримання політики безпеки й оцінювати потреби користувачів.

Це дозволить компаніям уникнути значної частки ризиків і забезпечити безпека локальної мережі. Крім того, маючи повний звіт про використання застосунків, організація має можливість регулювати витрати на ПЗ: якщо додаток не використовується співробітниками, то не має змісту продовжувати на нього ліцензію. А оскільки придбання ліцензійного програмного забезпечення найчастіше зв'язано зі значними фінансовими вкладеннями, то за допомогою Application Control організації зможуть мінімізувати свої витрати на ліцензійну політику. Сьогодні вкладення в ІБ стають не витратами, а інструментами, що допомагають заощадити засобу з метою вкладення їх у подальший розвиток бізнесу.

Таким чином, розвиток технологій поступово приходить до того, що засобу мережного захисту починають відслідковувати не периметр мережі, а самі дані, що проходять через нього. Подібні зміни пов'язані з тим, що сьогодні мережа вже не має чітких границь: багато організацій надають своїм співробітникам і партнерам віддалений доступ до корпоративної мережі, забезпечуючи їм волю й мобільність. Але повсюдне поширення мобільних комп'ютерів піддає ІБ компанії великому ризику, оскільки контроль за периметром мережі стає дуже складним завданням, для рішення якої традиційних методів захисту вже недостатньо. Саме тому однією із самих актуальних тенденцією в сфері ІБ на сьогоднішній день є керування даними й контроль за всією переміщуваною інформацією за допомогою технології Application Control, що надає безпрецедентний рівень контролю застосунків у єдиному, економічно вигідному рішенні для забезпечення мережної безпеки, що і визначає майбутнє систем ІБ.

Розробка структурної схеми

Існує п'ять варіантів рішення завдання організації доступу до сервісів корпоративної мережі з Інтернет і вибір того варіанта, що відповідає поставленим вимогам. У рамках огляду приводиться аналіз варіантів на предмет безпеки й реалізуємості, що допоможе розібратися в суті питання, освіжити й систематизувати свої знання як починаючим фахівцям, так і більше досвідченим. Матеріали розділу можна використовувати для обґрунтування проектних рішень.

При розгляді варіантів як приклад візьмемо мережу, у якій потрібно опублікувати:

- Корпоративний поштовий сервер (Web-mail).
- Корпоративний термінальний сервер (RDP).
- Extranet сервіс для контрагентів (Web-API).

Варіант 1. Плоска мережа

У даному варіанті всі вузли корпоративної мережі втримуються в одній, загальної для всіх мережі («Внутрішня мережа»), у рамках якої комунікації між ними не обмежуються.

Мережа підключена до Інтернет через прикордонний маршрутизатор/міжмережевий екран (далі – IFW).Доступ вузлів в Інтернет здійснюється через NAT, а доступ до сервісів з Інтернет через Port forwarding.

Переваги варіанта:

– Мінімальні вимоги до функціонала IFW (можна зробити практично на будь-якому, навіть домашньому роутері).

– Мінімальні вимоги до знань фахівця, що здійснює реалізацію варіанта.

Недоліки варіанта:

– Мінімальний рівень безпеки. У випадку злому, при якому Порушник одержить контроль над одним з опублікованих в Інтернеті серверів, йому для подальшої атаки стають доступні всі інші вузли й канали зв'язку корпоративної мережі.

Аналогія з реальним життям.

Подібну мережу можна зрівняти з компанією, де персонал і клієнти перебувають в одній спільній кімнаті (open space)

Варіант 2. DMZ

Для усунення зазначеного раніше недоліку вузли мережі, доступні з Інтернет, поміщають у спеціально виділений сегмент – демілітаризовану зону (DMZ). DMZ організується за допомогою міжмережевих екранів, що відокремлюють її від Інтернет (IFW) і від внутрішньої мережі (DFW).

При цьому правила фільтрації міжмережевих екранів виглядають у такий спосіб:

– Із внутрішньої мережі можна ініціювати з'єднання в DMZ і в WAN (Wide Area Network).

– З DMZ можна ініціювати з'єднання в WAN.

– З WAN можна ініціювати з'єднання в DMZ.

– Ініціація з'єднань із WAN і DMZ до внутрішньої мережі заборонена.

Переваги варіанта:

– Підвищена захищеність мережі від зломів окремих сервісів. Навіть якщо один із серверів буде зламаний, Порушник не зможе одержати доступ до ресурсів, що перебуває у внутрішній мережі (наприклад, мережним принтерам, системам відеоспостереження й т.д.).

Недоліки варіанта:

– Сам по собі винос серверів в DMZ не підвищує їхня захищеність.

– Необхідний додатковий МЕ для відділення DMZ від внутрішньої мережі.

Аналогія з реальним життям.

Даний варіант архітектури мережі схожий на організацію робочої й клієнтської зон у компанії, де клієнти можуть перебувати тільки в клієнтській зоні, а персонал може бути як у клієнтської, так і в робочих зонах. DMZ сегмент – це саме і є аналог клієнтської зони.

Варіант 3. Поділ сервісів на Front-End і Back-End

Як ми вже відзначали раніше, розміщення сервера в DMZ жодним чином не поліпшує безпека самого сервісу. Одним з варіантів виправлення ситуації є поділ функціонала сервісу на дві частини: Front-End і Back-End. При цьому кожна частина розташовується на окремому сервері, між якими організується мережну взаємодію. Сервера Front-End, що реалізують функціонала взаємодії із клієнтами, що перебувають в Інтернет, розміщають в DMZ, а сервера Back-End, що реалізують інший функціонал, залишають у внутрішній мережі. Для взаємодії між ними на DFW створюють правила, що дозволяють ініціацію підключень від Front-End до Back-End.

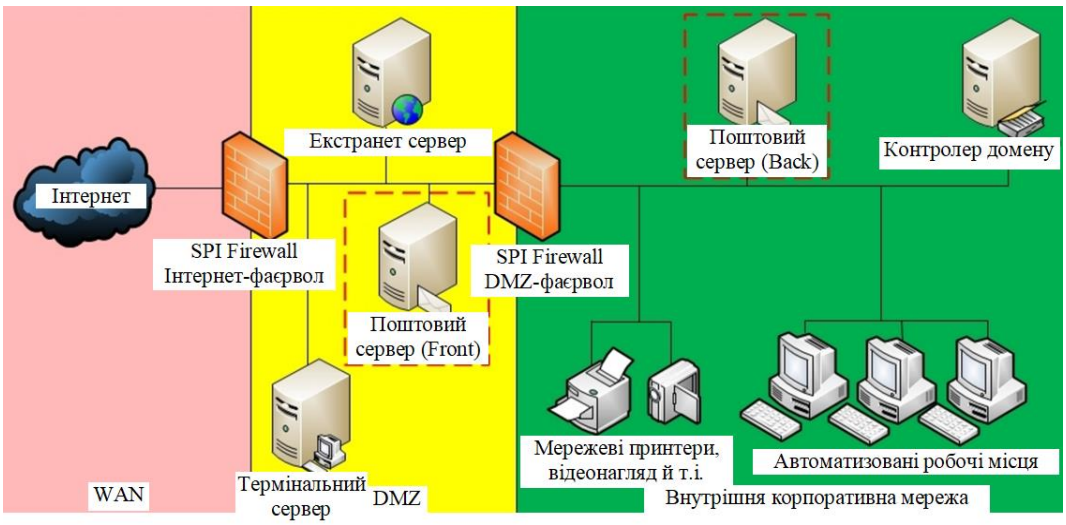


Рисунок 1 – Структурна схема системи

Як приклад розглянемо корпоративний поштовий сервіс, що обслуговує клієнтів як зсередини мережі, так і з Інтернет. Клієнти зсередини використовують POP3/SMTP, а клієнти з Інтернет працюють через Web-інтерфейс. Звичайно на етапі впровадження компанії вибирають найбільш простий спосіб розгортання сервісу й ставлять всі його компоненти на один сервер. Потім, у міру усвідомлення необхідності забезпечення інформаційної безпеки, функціонал сервісу розділяють на частині, і та частина, що відповідає за обслуговування клієнтів з Інтернет (Front-End), виноситься на окремий сервер, що по мережі взаємодіє із сервером, що реалізує функціонал, що залишився (Back-End). При цьому Front-End розміщають в DMZ, а Back-End залишається у внутрішньому сегменті. Для зв'язку між Front-End і Back-End на DFW створюють правило, що дозволяє, ініціацію з'єднань від Front-End до Back-End.

Переваги варіанта:

– У загальному випадку атаки, спрямовані проти сервісу, що захищається, можуть «спіткнутися» про Front-End, що дозволить нейтралізувати або істотно знизити можливий збиток. Наприклад, атаки типу TCP SYN Flood або slow http read, спрямовані на сервіс, приведуть до того, що Front-End сервер може виявитися недоступний, у той час як Back-End буде продовжувати нормально функціонувати й обслуговувати користувачів.

– У загальному випадку на Back-End сервері може не бути доступу в Інтернет, що у випадку його злому (наприклад, локально запущеним шкідливим кодом) утруднить віддалене керування їм з Інтернет.

– Front-End добре підходить для розміщення на ньому міжмережевого екрана рівня застосунків (наприклад, Web application firewall) або системи запобігання вторгнень (IPS, наприклад snort).

Недоліки варіанта:

1. Для зв'язку між Front-End і Back-End на DFW створюється правило, що дозволяє ініціацію з'єднання з DMZ у внутрішню мережу, що породжує погрози, пов'язані з використанням даного правила з боку інших вузлів в DMZ (наприклад, за рахунок реалізації атак IP spoofing, ARP poisoning і т.д.)

– Не всі сервіси можуть бути розділені на Front-End і Back-End.

– У компанії повинні бути реалізовані бізнес-процеси актуалізації правил міжмережевого екранування.

– У компанії повинні бути реалізовані механізми захисту від атак з боку Порушників, що одержали доступ до сервера в DMZ.

Примітки.

– У реальному житті навіть без поділу серверів на Front-End і Back-End серверам з DMZ дуже часто необхідно звертатися до серверів, що перебуває у внутрішній мережі, тому зазначені недоліки даного варіанта будуть також справедливі й для попереднього розглянутого варіанта.

– Якщо розглядати захист застосунків, що працюють через Web-інтерфейс, то навіть якщо сервер не підтримує рознесення функцій на Front-End і Back-End, застосування http reverse proxy сервера (наприклад, nginx) у якості Front-End дозволить мінімізувати ризики, пов'язані з атаками на відмову в обслуговуванні. Наприклад, атаки типу SYN flood можуть зробити http reverse proxy недоступним, у той час як Back-End буде продовжувати працювати.

Аналогія з реальним життям.

Даний варіант по суті схожий на організацію праці, при якій для високо завантажених працівників використовують помічників – секретарів. Тоді Back-End буде аналогом завантаженого працівника, а Front-End аналогом секретаря.

Варіант 4. Захищений DMZ

DMZ це частина мережі, доступна з Internet, і, як наслідок, підданий максимальному ризику компрометації вузлів. Дизайн DMZ і застосовувані в ній підходи повинні забезпечувати максимальну живучість в умовах, коли Порушник одержав контроль над одним з вузлів в DMZ. Як можливі атаки розглянемо атаки, яким піддані практично всі інформаційні системи, що працюють із налаштуваннями за замовчуванням:

– CAM-table overflow.
– ARP poisoning.
– Rogue DHCP Server.
– DHCP starvation.
– VLAN hopping.
– MAC flood.
– UDP flood.
– TCP SYN flood.
– TCP session hijacking.
– TCP reset.
– Атаки на Web-застосунки.
– Атаки на обхід засобів автентифікації й авторизацію від імені легітимного користувача (наприклад, підбор паролів, PSK і т.д.).
– Атаки на уразливості в мережних службах, наприклад:.
– Атака на Web-сервер – slow reading.
– DNS cache poisoning.

Більша частина зазначених атак (принаймні з 1 по 10) базується на уразливістях архітектури сучасних Ethernet/IP мереж, що полягають у можливості Порушника підробляти в мережних пакетах MAC і IP адреси. Експлуатацію даних уразливістей іноді виділяють в окремий види атак:

– MAC spoofing;
– IP spoofing.

Тому побудова системи захисту DMZ почнемо з розгляду способів захисту від IP і MAC spoofing.

Примітка .

Наведені нижче способи захисту від даних атак не є єдино можливими. Існують і інші способи.

Захист від MAC spoofing

Нейтралізацією даної атаки може бути фільтрація MAC-адрес на портах комутатора. Наприклад, трафік по порту 3 повинен проходити тільки у випадку, якщо в адресі джерела

або в адресі призначення зазначена MAC-адреса DE:AD:BE:AF:DE:AD або широкомовна адреса (у деяких випадках).

Захист від IP spoofing

Схема атаки IP spoofing схожа на попередню, за винятком того, що Порушник підробляє не MAC, а IP-адресу. Захист від IP spoofing може бути реалізована шляхом поділу IP-мережі DMZ на більше дрібні IP-підмережі й подальшою фільтрацією трафіку на інтерфейсах маршрутизатора за аналогією з розглянутої раніше MAC-фільтрацією.

В DMZ розташовується 3 вузли:

- Термінальний сервер (192.168.100.2).
- Поштовий сервер (192.168.100.5).
- Extranet сервер (192.168.100.9).

Для DMZ виділена IP-мережа 192.168.100.0/24, у даній мережі виділяються 3 IP-підмережі (по числу серверів):

- Підмережа 1 - 192.168.100.0/30 для термінального сервера (192.168.100.2).
- Підмережа 2 - 192.168.100.4/30 для поштового сервера (192.168.100.5).
- Підмережа 3 - 192.168.100.8/30 для поштового сервера (192.168.100.9).

На практиці поділ мережі на подібні підмережі реалізують за допомогою технології VLAN. Однак, її застосування породжує ризики, захист від яких зараз розглянемо.

Захист від VLAN hopping

Для захисту від цієї атаки на комутаторі відключають можливість автоматичного узгодження типів (trunk / access) портів, а самі типи адміністратор призначає вручну. Крім того, організаційними мірами забороняється використання так званого native VLAN.

Захист від атак, пов'язаних з DHCP

Незважаючи на те, що DHCP призначений для автоматизації конфігурування IP-адрес робочих станцій, у деяких компаніях зустрічаються випадки, коли через DHCP видаються IP-адреси для серверів, але це досить погана практика. Тому для захисту від Rogue DHCP Server, DHCP starvation рекомендується повна відмова від DHCP в DMZ.

Захист від атак MAC flood

Для захисту від MAC flood проводять налаштування на портах комутатора на предмет обмеження граничної інтенсивності широкомовного трафіку (оскільки звичайно при даних атаках генерується широкомовний трафік (broadcast)). Атаки, пов'язані з використанням конкретних (unicast) мережних адрес, будуть заблоковані MAC фільтрацією, що розглянули раніше.

Захист від атак UDP flood

Захист від даного типу атак відбувається аналогічно захисту від MAC flood, за винятком того, що фільтрація здійснюється на рівні IP (L3).

Захист від атак TCP SYN flood

Для захисту від даної атаки можливі варіанти:

- Захист на вузлі мережі за допомогою технології TCP SYN Cookie.
- Захист на рівні міжмережевого екрана (за умови поділу DMZ на підмережі) шляхом обмеження інтенсивності трафіку, що містить запити TCP SYN.

Захист від атак на мережні служби й Web-застосунку

Універсального рішення даної проблеми ні, але устояною практикою є впровадження процесів керування уразливістями ПЗ (виявлення, установка патчей і т.д., наприклад, так), а також використання систем виявлення й запобігання вторгнень (IDS/IPS).

Захист від атак на обхід засобів автентифікації

Як і для попереднього випадку універсального рішення даної проблеми немає.

Звичайно у випадку великої кількості невдалих спроб авторизації облікові записи, для запобігання підборів автентифікаційних даних (наприклад, пароля) блокують. Але подібний підхід досить спірний, і от чому.

По-перше, Порушник може проводити підбор автентифікаційної інформації з інтенсивністю, що не приводить до блокування облікових записів (зустрічаються випадки, коли пароль підбирався в плині декількох місяців з інтервалом між спробами в кілька десятків хвилин).

По-друге, дану особливість можна використовувати для атак типу відмова в обслуговуванні, при яких Порушник буде навмисне проводити велику кількість спроб авторизації для того, щоб заблокувати облікові записи.

Найбільш ефективним варіантом від атак даного класу буде використання систем IDS/IPS, які при виявленні спроб підбора паролів будуть блокувати не обліковий запис, а джерело, звідки даний підбор відбувається (наприклад, блокувати IP-адресу Порушника).

Підсумковий перелік захисних заходів для даного варіанта:

– DMZ розділяється на IP-підмережі з розрахунку окрема підмережа для кожного вузла.

– IP адреси призначаються вручну адміністраторами. DHCP не використовується.

– На мережних інтерфейсах, до яких підключені вузли DMZ, активується MAC і IP фільтрація, обмеження по інтенсивності широкомовного трафіку й трафіку, що містить TCP SYN запити.

– На комутаторах відключається автоматичне узгодження типів портів, забороняється використання native VLAN.

– На вузлах DMZ і серверах внутрішньої мережі, до яких дані вузли підключаються, налаштовується TCP SYN Cookie.

– Відносно вузлів DMZ (і бажано іншої мережі) впроваджується керування уразливістями ПЗ.

– В DMZ-сегменті впроваджуються системи виявлення й запобігання вторгнень IDS/IPS.

Переваги варіанта:

– Високий ступінь безпеки.

Недоліки варіанта:

– Підвищені вимоги до функціональних можливостей устаткування.

– Працезатрати у впровадженні й підтримці.

Аналогія з реальним життям.

Якщо раніше DMZ зрівняли із клієнтською зоною, оснащеної диванчиками й пуфиками, то захищений DMZ буде більше схожий на броньовану касу.

Варіант 5. Back connect

Розглянуті в попередньому варіанті міри захисти були засновані на тому, що в мережі був присутнє пристрій (комутатор / маршрутизатор / міжмережевий екран), здатний їх реалізовувати. Але на практиці, наприклад, при використанні віртуальної інфраструктури (віртуальні комутатори найчастіше мають дуже обмежені можливості), подібного пристрою може й не бути.

У цих умовах Порушникові стають доступні багато хто з розглянутих раніше атак, найнебезпечнішими з яких будуть:

– атаки, що дозволяють перехоплювати й модифікувати трафік (ARP Poisoning, CAM table overflow + TCP session hijacking і ін.);

– атаки, пов'язані з експлуатацією уразливістей серверів внутрішньої мережі, до яких можна ініціювати підключення з DMZ (що можливо шляхом обходу правил фільтрації DFW за рахунок IP і MAC spoofing).

Наступною немаловажною особливістю, що раніше не розглядали, але яка не перестає бути від цього менш важливої, це те, що автоматизовані робочі місця (АРМ) користувачів теж можуть бути джерелом (наприклад, при зараженні вірусами або троянами) шкідливого впливу на сервера.

Таким чином, перед нами встає завдання захистити сервера внутрішньої мережі від атак Порушника як з DMZ, так і із внутрішньої мережі (зараження АРМа трояном можна інтерпретувати як дії Порушника із внутрішньої мережі).

Пропонований далі підхід спрямований на зменшення числа каналів, через які Порушник може атакувати сервера, а таких каналу як мінімум два. Перший це правило на DFW, що дозволяє доступ до сервера внутрішньої мережі з DMZ (нехай навіть і з обмеженням по IP-адресах), а другий – це відкритий на сервері мережний порт, по якому очікуються запити на підключення.

Закрити зазначені канали можна, якщо сервер внутрішньої мережі буде сам будувати з'єднання до сервера в DMZ і буде робити це за допомогою криптографічно захищених мережних протоколів. Тоді не буде ні відкритого порту, ні правила на DFW.

Але проблема в тому, що звичайні серверні служби не вміють працювати подібним чином, і для реалізації зазначеного підходу необхідно застосовувати мережне тунелювання, реалізоване, наприклад, за допомогою SSH або VPN, а вже в рамках тунелів дозволяти підключення від сервера в DMZ до сервера внутрішньої мережі.

Загальна схема роботи даного варіанта виглядає в такий спосіб:

– На сервер в DMZ інсталюється SSH/VPN сервер, а на сервер у внутрішній мережі інсталюється SSH/VPN клієнт.

– Сервер внутрішньої мережі ініціює побудова мережного тунелю до сервера в DMZ. Тунель будується із взаємною автентифікацією клієнта й сервера.

– Сервер з DMZ у рамках побудованого тунелю ініціює з'єднання до сервера у внутрішній мережі, по якому передаються захит данние, що.

– На сервері внутрішньої мережі налаштовується локальний міжмережевий екран, що фільтрує трафік, що проходить по тунелі.

Використання даного варіанта на практиці показало, що мережні тунелі зручно будувати за допомогою OpenVPN, оскільки він має наступні важливі властивості:

– Кроссплатформеність. Можна організовувати зв'язок на серверах з різними операційними системами.

– Можливість побудови тунелів із взаємної автентифікацією клієнта й сервера.

– Можливість використання сертифікованої криптографії.

На перший погляд може здатися, що дана схема зайво ускладнена й що, раз на сервері внутрішньої мережі однаково потрібно встановлювати локальний міжмережевий екран, то простіше зробити, щоб сервер з DMZ, як звичайно, сам підключався до сервера внутрішньої мережі, але робив це по шифрованому з'єднанню. Дійсно, даний варіант закриє багато проблем, але він не зможе забезпечити головного – захист від атак на уразливості сервера внутрішньої мережі, чинених за рахунок обходу міжмережевого екрана за допомогою IP і MAC spoofing.

Переваги варіанта:

– Архітектурне зменшення кількості векторів атак на сервер, який захищається, внутрішньої мережі.

– Забезпечення безпеки в умовах відсутності фільтрації мережного трафіку.

– Захист даних, переданих по мережі, від несанкціонованого перегляду й зміни.

– Можливість вибірного підвищення рівня безпеки сервісів.

– Можливість реалізації двоконтурної системи захисту, де перший контур забезпечується за допомогою міжмережевого екранування, а другий організується на базі даного варіанта.

Недоліки варіанта:

– Впровадження й супровід даного варіанта захисту вимагає додаткових трудових витрат.

– Несумісність із мережними системами виявлення й запобігання вторгнень (IDS/IPS).

– Додаткове обчислювальне навантаження на сервера.

Аналогія з реальним життям.

Основний зміст даного варіанта в тому, що довірена особа встановлює зв'язок з не довіреним, що схоже на ситуацію, коли при видачі кредитів Банки самі передзвонюють потенційному позичальникові з метою перевірки даних.

Який із варіантів краще, який гірше – сказати складно, оскільки все залежить, в остаточному підсумку, від тої інформації, яку необхідно захистити, і тих ресурсів, якими компанія розташовує для захисту. Якщо ні ресурсів, ні знань ні, то оптимальним буде перший варіант. Якщо ж інформація дуже коштовна, то комбінація четвертого й п'ятого варіантів дасть неперевершений рівень безпеки.

Висновок. У статті розглянуто програмне забезпечення, призначено для системи захисту корпоративної мережі з застосуванням SPI Firewall. В межах України в недостатній мірі представлені вітчизняні розробки в цій області. У роботі наведені теоретичне узагальнення й рішення наукового завдання дослідження методів захисту корпоративної мережі з застосуванням SPI Firewall. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем захисту корпоративної мережі з застосуванням SPI Firewall; Досліджена система захисту корпоративної мережі з застосуванням SPI Firewall; На основі отриманих результатів досліджень створена програмна реалізація системи захисту корпоративної мережі з застосуванням SPI Firewall. Розроблені під час виконання роботи алгоритми дозволяють успішно вирішувати завдання захисту корпоративної мережі з застосуванням SPI Firewall. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки. Розроблене програмне забезпечення має простий, дружній та зручний інтерфейс користувача, що забезпечує легкість у освоєнні роботи програмного продукту, зручність у використанні, і не потребує особливих спеціальних знань. При створені програмного забезпечення було використано об’єктно-орієнтований підхід, що відповідає сучасним тенденціям у галузі розробки комерційних програмних систем. Програма реалізована на мові високого рівня Visual C++. Дана мова програмування дозволяє найбільш ефективно обробляти дані. Це дозволило мінімізувати строк розробки програмного забезпечення, і, як слід, зменшити витрати на його розробку. Запропоноване програмне забезпечення ділиться на загальне програмне забезпечення, що поставляється із засобами обчислювальної техніки й спеціальне програмне забезпечення, що спеціально розроблене для даної конкретної системи й включає програми, що реалізують її функції. Даються необхідні рекомендації з установки розробленого програмного забезпечення. Для підвищення рівня безпеки запропоновано застосовувати алгоритм RSA. В цілому створене програмне забезпечення підтверджує правильність використаних проектних рішень та повністю відповідає вимогам технічного завдання. Створене програмне забезпечення має потенційну можливість для подальшого вдосконалення і застосування у різних галузях.

Список літератури

1. Смирнов А.А. Анализ и сравнительное исследование перспективных направлений развития цифровых телекоммуникационных систем и сетей / А.А.Смирнов, В.В.Босько, Е.В.Мелешко // Системи обробки інформації. – Х.: ХУ ПС, 2008. – Вип.7(74). – С.120-123.
2. Смирнов А.А. Усовершенствование метода управления очередями в многопротокольных узлах телекоммуникационной сети / А.А.Смирнов, Е.В.Мелешко // Збірник тез та доповідей другої всеукраїнської науково-практичної конференції «Системний аналіз. Інформатика. Управління». Запоріжжя. Тези доповідей. Запоріжжя: КПУ, 2011.
3. Смирнов С.А. метод безопасной маршрутизации метаданных в облачные антивирусные системы / А.К. Дидык, С.А. Смирнов // Информационные технологии в управлении, образовании, науке и промышленности: монография / Под редакцией профессора В.С. Пономаренко. – Х.: Видавець Рожко С.Г., 2016. – 566 с.

4. Смирнов С. А. Сравнительные исследования математических моделей технологии распространения компьютерных вирусов в информационно-телекоммуникационных сетях / Мохамад Абу Таам Гани, А. А. Смирнов, А. В. Коваленко, С. А. Смирнов // Системи обробки інформації: зб. наук. праць. – Х.: ХУПС, 2014. – Вип. 9(125). – 105-110.
5. Смирнов С. А. Математическая модель интеллектуального узла коммутации с обслуживанием информационных пакетов различного приоритета / Мохамад Абу Таам Гани, А. А. Смирнов, Н. С. Якименко, С. А. Смирнов // Збірник наукових праць Харківського університету Повітряних Сил. – Харків: ХУПС, 2014. – Вип. 4 (41). – С. 48-52.
6. Смирнов С. А. Исследование показателей качества функционирования интеллектуальных узлов коммутации в телекоммуникационных системах и сетях / Мохамад Абу Таам Гани, А. А. Смирнов, Н. С. Якименко, С. А. Смирнов // Наука і техніка Повітряних Сил Збройних Сил України: наук. журн. – Х.: ХУПС, 2014. – № 4(17). – С. 90-95.
7. Смирнов С. А. Усовершенствованный алгоритм управления доступом к «облачным» телекоммуникационным ресурсам / Мохамад Абу Таам Гани, А. А. Смирнов, Н. С. Якименко, С. А. Смирнов // Системи обробки інформації: зб. наук. праць. – Х.: ХУПС, 2015. –Вип. 1(126). – С. 150-153.
8. Smirnov S.A. Method of controlling access to intellectual switching nodes of telecommunication networks and systems / A.A. Smirnov, Mohamad Abou Taam, S.A. Smirnov // International Journal of Computational Engineering Research (IJCER). – **Volume 5, Issue 5. –** India. Delhi. – 2015. – P. 1-7.
9. Смирнов С. А. Анализ и исследование методов управления сетевыми ресурсами для обеспечения антивирусной защиты даннях / Мохамад Абу Таам Гани, А. А. Смирнов, С. А. Смирнов // Системи озброєння і військова техніка: наук. журн. – Х.: ХУПС, 2015. – № 3(43). – С. 100-107.
10. Смирнов С. А. Исследование эффективности метода управления доступом к облачным антивирусным телекоммуникационным ресурсам / Мохамад Абу Таам Гани, А. А. Смирнов, С. А. Смирнов // Наука і техніка Повітряних Сил Збройних Сил України: наук. журн. –Х.: ХУПС, 2015. –№ 3(20). – С. 134-141.
11. Смирнов С. А. Комплекс gert-моделей технологии облачной антивирусной защиты телекоммуникационной системы / А. А. Смирнов, А. К. Дидык, А. Н. Дреев, С. А. Смирнов // Безпека інформації: наук. - практ. журн. – К.: НАУ, 2015. – Т. 21, № 3. – С. 251-262.

УДК 004

Д. Демченко, магістр гр. КІ-18-1,4
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ ВІДЕОТЕХНОЛОГІЙ ДЛЯ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ З ПІДТРИМКОЮ WI-FI

У статті розроблено програмне забезпечення, яке призначено для відеотехнологій для цифрової трансформації з підтримкою Wi-Fi. Метою розробки є дослідження та програмна реалізація відеотехнологій для цифрової трансформації з підтримкою Wi-Fi. Об’єктом дослідження є процес цифрової трансформації з підтримкою Wi-Fi. Предметом дослідження є методи цифрової трансформації з підтримкою Wi-Fi. Методи дослідження базуються на методах кодування інформації, теорії бездротової передачі даних, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація відеотехнологій для цифрової трансформації з підтримкою Wi-Fi.
комп’ютерна інженерія, цифрова трансформація, Wi-Fi

Постановка проблеми. Робочі місця стають усе більше неформальними: люди трудяться сьогодні з дому, з готелів, у транспорті й т.д. Відповідно, сучасні засоби відео-конференц-зв'язку (ВКЗ) і спільної роботи повинні відповідати цим новим вимогам. Але й потенціал традиційної сфери застосування ВКЗ далекий від вичерпання: лише одна з кожних десяти переговірних кімнат обладнана засобами відеозв'язку.

У числі важливих тенденцій 2018 року – усе більше широке застосування протоколу WebRTC, бездротових технологій для спільного використання контенту, інтелектуальних засобів.

Такі засоби уже реалізовані, вони дозволяють, зокрема, визначати присутність людей у переговірній, підраховувати їхнє число, автоматично наводити камеру на того, хто розмовляє.

Замороження ІТ-бюджетів в останні роки веде до нагромадження відкладеного попиту, а криза – це, скоріше, каталізатор процесів розвитку рішень ВКЗ. У числі найбільш значимих тенденцій ринку перехід від спеціалізованих апаратних платформ інфраструктурного встаткування ВКЗ до програмних рішень, що працюють на базі стандартних Intel-серверів, а також віртуалізація рішень і ріст популярності хмарних моделей.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні програмної реалізації відеотехнологій для цифрової трансформації з підтримкою Wi-Fi T.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація відеотехнологій для цифрової трансформації з підтримкою Wi-Fi.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем цифрової трансформації з підтримкою Wi-Fi.
– Дослідження відеотехнологій для цифрової трансформації з підтримкою Wi-Fi.
– Програмна реалізація відеотехнологій для цифрової трансформації з підтримкою Wi-Fi.

Об'єктом дослідження є процес цифрової трансформації з підтримкою Wi-Fi.

Предметом дослідження є методи цифрової трансформації з підтримкою Wi-Fi.

Методи дослідження базуються на методах кодування інформації, теорії бездротової передачі даних, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Час є, імовірно, найціннішим ресурсом у сучасному суспільстві. За результатами досліджень, проведених Національною радою по статистиці США, в Америці щодня проходить близько 11 мільйонів ділових зустрічей і до 37% робочого часу службовців витрачається на такі зустрічі й наради. Було також установлене, що участь у чотиригодинному заході вимагає приблизно 16 годин планування, підготовки, пересування й т.д. При цьому левову частину загальних витрат становлять транспортні витрати.

Щоб зменшити транспортні витрати, збільшити оперативність і розширити сферу послуг, багато компаній у Росії використовують сьогодні відеододатки. Для ряду підприємств і установ відеоконференції стали повсякденним явищем.

Стандарти ITU-T в області відеоконференцій

У цей час прийнято кілька стандартів (називаних рекомендаціями ITU-T (Сектор стандартизації телекомунікацій Міжнародного союзу електрозв'язку) серії H "Аудіовізуальні й мультимедійні системи") для різних середовищ зв'язку. Найбільш широке поширення з них одержали рекомендації H.320 "Вузькополосні відеотелефонні системи й термінальне встаткування" – для мереж ISDN і інших мереж з гарантованою якістю обслуговування, і H.323 версія 2, "Мультимедійні системи зв'язку для мереж з комутацією пакетів" – для IP-мереж і ним подібних з негарантованою якістю обслуговування.

Слід зазначити, що системи стандарту H.320 з'явилися значно раніше, і довгий час безроздільно домінували на ринку встаткування відеоконференцій. Однак останнім часом пріоритет всі частіше віддається значно більше економічним системам стандарту H.323. Це зв'язано як з інтенсивним розвитком локальних, корпоративних і глобальних обчислювальних мереж і застосуванням у них технологій, що забезпечують необхідну якість обслуговування, так і зі зниженням витрат на додаткове комунікаційне встаткування.

Основою для побудови мережі відеоконференцій служать термінали – робочі станції, головним завданням яких є кодування й декодування відео- і аудіосигналів і їхня передача й

прийом відповідно до правил, прийнятими для даного стандарту відеоконференції й зв'язковий середовища.

Порівняння програмних і апаратних рішень для відеоконференцій

Зараз на ринку систем відеоконференцій для ЛОМ є велика кількість як чисто програмних рішень, так і програмно-апаратних комплексів для реалізації терміналів відеоконференцій. Під програмним рішенням розуміється реалізація процесів відео- і аудіокодування й декодування за допомогою програмного забезпечення, що використовує тільки центральний процесор комп'ютера. Програмно-апаратні рішення ґрунтуються на використанні потужних спеціалізованих процесорів кодування/декодування. Вартість програмних реалізацій менше, ніж апаратних і вони можуть бути встановлені практично на будь-якому сучасному персональному комп'ютері, що має звукову плату й володіє можливість відеозахвата (підключена відеокамера й драйвер Video for Windows). Типовими представниками таких програм є Microsoft NetMeeting і White Pine CU-SeeMe.

Незважаючи на зовнішню привабливість такого рішення, необхідної якості відео в них досягти не вдається. Справа в тому, що кодування відеопотоку висуває високі вимоги до обчислювальних ресурсів термінала. Нагадаємо, що відповідно до прийнятого в рамках рекомендацій H.320 і H.323 стандартом кодування відео H.261 необхідно забезпечити стиск у реальному часі вихідного сигналу з коефіцієнтом від 100 до 1000. І навіть стрімке збільшення потужностей процесорів загального призначення не в змозі забезпечити якісне кодування й декодування сигналу відеоконференції.

Щоб якось реалізувати ці функції у своїх програмних продуктах, фірми-розроблювачі програм змушені встановлювати певні обмеження для процесу кодування: використовувати низьку частоту кадрів, спрощені алгоритми перетворення відео, що ведуть до зменшення розміру зображення, зниженню чіткості й погіршенню передачі кольору.

Намагаючись вийти за межі твердих рамок міжнародних стандартів і спростити процес кодування, творці програм пропонують передавати зображення чорно^-білим і використовувати свої, ні з ким не сумісні алгоритми. Якщо наступний кадр надходить на програмний декодер до закінчення обробки поточного, він ігнорується. Відеоінформація губиться, зображення розпадається на частині й картинка стає незадовільною. Тому при кодуванні необхідно враховувати не тільки власні обчислювальні можливості, але й продуктивність декодера на протилежній стороні. У результаті прийнятної якості можна досягти лише при маленькому розмірі відеокадру (QCIF) і порівняно низкою частоті кадрів (близько 10).

Перевага програмних рішень проявляється при використанні вузькополосних каналів, наприклад, при модемному зв'язку зі швидкістю до 56 Кбіт/с. Оскільки смуга каналу маленька, обсяг інформації, оброблюваний кодеком, теж невеликий і програмний термінал з ним успішно справляється. Але про якість відеоконференції тут говорити не доводиться: звук глухий, швидкість передачі від декількох відеокадрів у секунду до одного в кілька секунд, що скоріше нагадує показ слайдів.

Слід також зазначити, що програмні рішення є дуже спрощеними аналогами повноцінних апаратних рішень і по функціональних можливостях. Як правило, у них відсутні такі функції, як використання керованої камери й контроль за нею із протилежної сторони, додаткові аудіо- і відеовходи й виходи, мікшування різних сигналів, вивід відео на TV монітор, багатоадресна передача, налаштування синхронізації відео й аудіо, буферизації й т.п.

У цілому, чисто програмні реалізації відеотерміналів через обмеженість їхньої функціональності й невисокої якості не в змозі забезпечити професійні рішення в області відеоконференцій.

На іншому кінці цього своєрідного ряду термінальних пристроїв відеоконференцій перебувають так звані "закінчені рішення", що представляють собою повністю замкнуті системи з апаратною реалізацією процесу кодування – декодування й заводською установкою програмного забезпечення. Дані пристрої, володіючи, як правило, високими

якісними характеристиками, все-таки мають дві серйозних вади. Це недостатня гнучкість системи, необхідна, наприклад, при використанні її для спеціальних додатків, і висока вартість (10 тис. діл. США й вище).

Устаткування для багатоточкових відеоконференцій

Бажання проводити сеанси відеозв'язку за участю декількох користувачів одночасно (по типі відеоселекторних нарад) змушує включити до складу використовуваного встаткування пристрою керування багатоточковою відео-конференц-зв'язком (MCU). Загальним принципом роботи цих пристроїв є такий спосіб організації багатоточкового зв'язку, при якому аудіопотоки змішуються, що дозволяє учасникам чути один одного, а відеопотоки перемикаються таким чином, що всі бачать тільки одного учасника зв'язку, причому вибір може бути зроблений головою відеоконференції, оператором або зроблений автоматично по голосовій активності.

MCU, як і відеотермінал, можливо реалізувати програмно або апаратно. Наприклад, фірма White Pine пропонує програмну реалізацію конференцсерверу MeetingPoint (не плутати з ПЗ для терміналів відеоконференцій VCON MeetingPoint). Для організації зв'язку потрібен виділений сервер з ОС Windows NT 4.0 або Sun Solaris. Одне із самих трудомістких завдань сервера – перекодування відео- і аудіосигналів. Як і у випадку із програмної реалізацій відеотерміналів, потужності процесора загального призначення для якісного рішення поставленого завдання недостатньо. І тому неминучі всі ті обмеження, про які згадувалося під час обговорення програмних реалізацій видеокодеків. Більше того, оскільки задіються всі обчислювальні ресурси системи, підключення нового учасника до багатоточкової конференції веде до погіршення якості одержуваного відео- і аудіопотоків.

Кращими виробниками на ринку апаратних MCU для високоякісних відеоконференцій є компанії RADVision, Ezenia! (раніше називалася VideoServer), Lucent Technology. Для мереж відеоконференцій, що нараховують порівняно невелике число користувачів, найбільш економічним рішенням буде використання MCU RADVision MCU-323 або Ezenia! Encounter NetServer вартістю від 3 до 4 тис. дол. США на кожний з, що беруть участь у сеансі відеоконференції користувача при швидкості зв'язку 384 – 768 Кбіт/с. Підключення – стандартний інтерфейс Ethernet 10/100 Mbps.

Звичайно, якщо мова йде про невелику мережу відеоконференцій з десятком користувачів, 50-80% витрат будуть доводитися на MCU. Тому, для зниження витрат на організацію такої мережі провідні виробники терміналів відеоконференцій пропонують нову технологію – Interactive Multicast. Вона заснована на груповій адресації інформаційного потоку. Використовуючи кодеки, що підтримують цю технологію, можна організувати багатоточкову відеоконференцію без допомоги MCU. Реалізація даної технології має на увазі можливість для одного з учасників, що займає пост голови, зі своєї ініціативи або за запитом інших учасників вибирати активний термінал для трансляції аудіо- і відеопотоку на всі інші. Достоїнством такого способу є його дешевина при високій якості відео, недоліками – неможливість мікшування звуку й істотна, залежна від навичок голови, затримка в перемиканні відео. Поліпшуючи цю технологію, VCON увів функцію автоматичного перемикання активного термінала за запитом, залишивши голові можливість при необхідності втручатися в цей процес.

Відеоконференції й мережна трансляція

Широке поширення в цей час здобуває мережне віщання, тобто трансляція в мережі за допомогою групової адресації записаних заздалегідь або "живих" відеопрограм. Для організації повноцінного сервера віщання необхідно мати досить дорогий комплекс устаткування, зате приймаюча сторона може обійтися (без більших претензій на якість) лише програмою перегляду. Загальновизнаний лідер у цій області – проект Cisco IP/TV. Однак у багатьох випадках можна обійтися без дорогого сервера віщання, замінивши його звичайним апаратним кодеком, сумісним з Cisco IP/TV. Наприклад, навіть використовуючи самий економічний кодек VCON Escort 25 і Cisco IP/TV Viewer, можна влаштувати міні-студію для мережного віщання зображення, одержуваного через відеокамеру або з відеомагнітофона.

При спільному використанні цих продуктів термінали можуть служити джерелом відеозображення, переданий на будь-який персональний комп'ютер, де встановлена програма перегляду Cisco IPTV Viewer. Умовно безкоштовне поширення цього програмного продукту робить таке сполучення надзвичайно привабливим у тих випадках, коли потрібна трансляція сеансу відеоконференції необмеженому колу користувачів, наприклад, у процесі спостереження й навчання.

Таким чином, сукупність пропонованих сьогодні на ринку термінальних і спеціалізованих мережних пристроїв і технологій передачі мультимедійної інформації дає можливість зробити цілком доступним впровадження систем відеоконференцій у практику роботи компаній і організацій, що розташовують обчислювальними мережами.

Розробка структурної схеми

При виборі приміщень для проведення нарад з віддаленими співробітниками за допомогою ВКЗ акцент зміщається з більших конференц-залів на невеликі переговірні кімнати (huddle room). На це вказують як аналітичні дослідження Wainhouse Research, так і дані інтеграторів. Надходить усе більше замовлень на встаткування маленьких переговірних. Для таких рішень пріоритетом є невисока ціна й компактність.

Завдання оснащення невеликих переговірних ефективно вирішуються за допомогою відеокамер з інтегрованими аудіофункціями. Таких продуктів на ринку стає усе більше. Приведемо продукт ConferenceSHOT AV компанії Vaddio. Це рішення поєднує в одному пристрої PTZ-камеру (з інтерфейсом USB 3.0) з 10-кратним збільшенням і акустичною системою з можливістю додавання до двох мікрофонів і зовнішнього динаміка. Для невеликих переговірних кімнат компанія пропонує комплект із камери ConferenceSHOT AV з одним настільним/стельовим мікрофоном; для охвату приміщень більшого розміру розроблена система із двома мікрофонами.

Інший варіант комплексного оснащення переговірної – рішення VC-B20UA компанії Lumens Integration. VC-B20UA складається з USB-камери й USB-спікерфона. PTZ-камера оснащена інтерфейсом USB 3.0, що дозволяє передавати незжате відео 1080p60 без відчутної затримки. Вхідний у комплект професійний USB-спікерфон Jabra з убудованим всеспрямованим мікрофоном забезпечує 360-градусне покриття й дозволяє комфортно спілкуватися по голосному зв'язку.

Багато сучасних рішень дозволяють взагалі відмовитися від окремих настільних мікрофонів. Одне з них – стельовий мікрофонний масив Microflex Advance компанії Shure. Маючи розмір зі стандартну плитку фальшпотолка, він забезпечує формування до восьми аудіолучів для рівномірного акустичного покриття приміщення. Масив можна настроїти так, щоб кожний промінь був спрямований убік конкретного учасника. Масив підключається за допомогою звичайної кручений пари, але при цьому використовується не стандартний Ethernet, а технологія Dante.

При спільній роботі в переговірній дуже зручно мати можливість вивести на загальний екран інформацію з персонального пристрою (ноутбука, планшета, смартфона), не витрачаючи час на пошук необхідного для підключення шнура, розеток та ін. Таку можливість надають сучасні продукти, що підтримують Wi-Fi. Розроблене в роботі програмне забезпечення, ставиться саме до цієї категорії. Структурна схема системи відображена на рисунку 3.1. Це рішення працює з усіма основними типами персональних пристроїв (з ОС Windows, OSX, Apple iOS і Android), дозволяючи виводити зображення з них на загальний дисплей. Використовувати можна практично з будь-якими дисплеями, що мають порт HDMI.

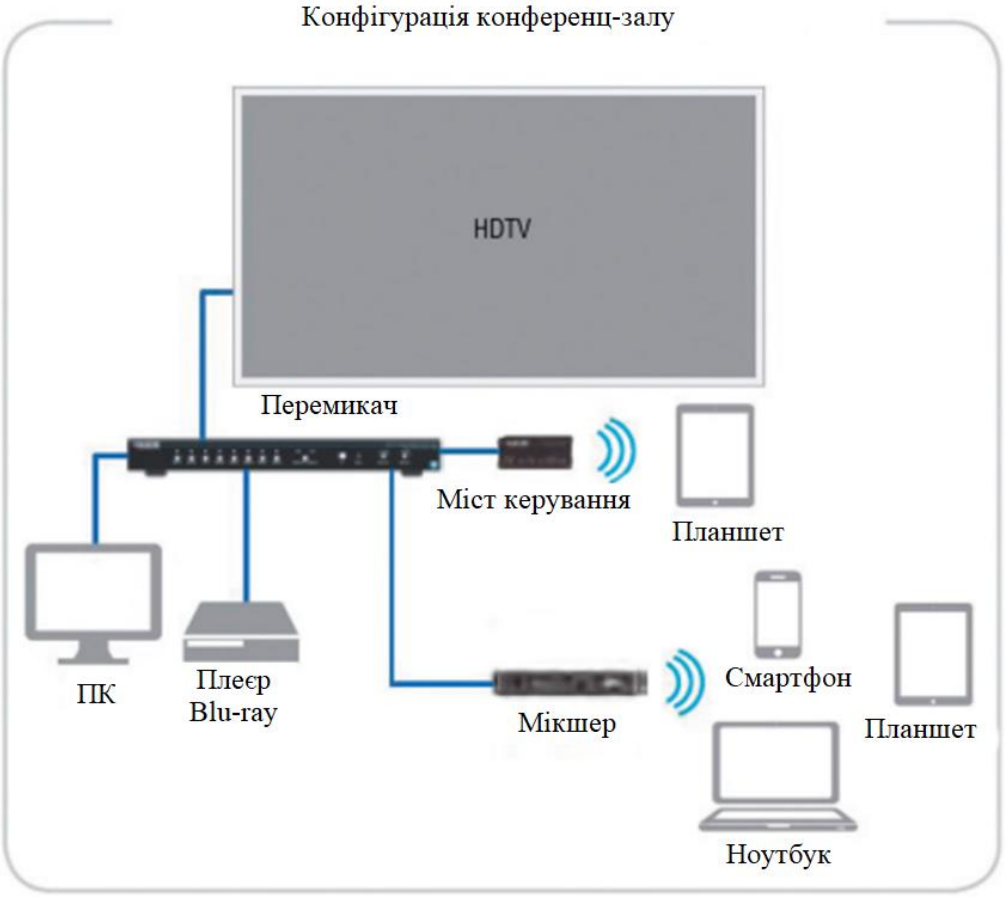


Рисунок 1 – Структурна схема системи

Ще один продукт вирішує, по суті, зворотне завдання: він дозволяє транслювати показуване на загальному екрані зображення на будь-які пристрої в аудиторії. Але це рішення буде, швидше за все, затребувано в великих залах. Маленька коробочка підключається між ноутбуком доповідача й засобом відображення (екраном або проектором). Пристрій по суті перехоплює передане на екран відео й транслює його по Wi-Fi на персональні пристрої слухачів. Дуже корисний прилад, особливо якщо ви змогли знайти місце тільки в глибині залу й інформація на загальному екрані видна погано.

Технології віртуальної й доповненої реальності для бізнесу

Технології віртуальної реальності (VR) припускають занурення користувача у віртуальний мир (за допомогою спеціальних окулярів або шоломів) і повне відключення від реального оточення, тоді як системи доповненої реальності (AR) передбачають доповнення реального оточення віртуальними зображеннями, з якими можлива взаємодія.

По даним IDC, якщо в 2016 році обсяг світового ринку VR-пристроїв і контенту становив 5,2 млрд доларів, то до 2021 року він виросте приблизно в 30 разів – до 162 млрд доларів. Український ринок також розвивається швидкими темпами. Так, за 2016 рік число компаній, що займаються технологіями VR і AR в Україні, виросло приблизно в чотири рази. Сьогодні таких компаній нараховують близько 200, але кістяк становлять порядку 15 компаній, які роблять великі проекти.

Основні напрямки роботи компаній, що займаються проектами VR і AR на ринку, – це туризм, розваги й реклама. Усе більш активно дані технології починають застосовуватися в утворенні. Активно застосовуються технології VR і в області торгівлі нерухомістю. Зокрема, вони дозволяють візуалізувати об'єкт, продемонструвавши потенційному покупцеві ще не побудовану або розташовану далеко нерухомість. Надягши шолом, покупець зможе пройтися по майбутній квартирі, оцінити варіанти планування, вид з вікна та ін. У цілому

сфера застосувань технології VR і AR широка й включає медицину, військово-промисловий комплекс, промисловість та ін.

Рекомендації H.323

Протоколи сімейства H.32x

В 1990 році був схвалений перший міжнародний стандарт в області відео-конференц-зв'язку – специфікація H.320 для підтримки відеоконференцій по ISDN. Потім ITU схвалив ще цілу серію рекомендацій, що ставляться до відео-конференц-зв'язку. Ця серія рекомендацій, часто називана H.32x, крім H.320, містить у собі стандарти H.321-H.324, які призначені для різних типів мереж.

У другій половині 90-х років інтенсивний розвиток одержали IP мережі й Інтернет. Вони перетворилися в економічне середовище передачі даних і стали практично повсюдними. Однак, на відміну від ISDN, IP мережі погано пристосовані для передачі аудіо й відеопотоків. Прагнення використовувати сформовану структуру IP мереж привело до появи в 1996 році стандарту H.323 (Visual Telephone Systems and Terminal Equipment for Local Area Networks which Provide a Non-Guaranteed Quality of Service, Відеотелефони й термінальне встаткування для локальних мереж з негарантованою якістю обслуговування). В 1998 році була схвалена друга версія цього стандарту H.323 v.2 (Packet-based multimedia communication systems, Мультимедійні системи зв'язку для мереж з комутацій пакетів), у вересні 1999 року була схвалена третя версія рекомендацій, 17 листопада 2001 року була схвалена четверта версія стандарту H.323. Зараз H.323 – один з найважливіших стандартів із цієї серії. H.323 – це рекомендації ITU-T для мультимедійних додатків в обчислювальних мережах, що не забезпечують гарантовану якість обслуговування (QoS). Такі мережі містять у собі мережі пакетної комутації IP і IPX на базі Ethernet, Fast Ethernet і Token Ring.

Рекомендації H.323 передбачають:

- Керування смугою пропущення.
- Можливість взаємодії мереж.
- Платформну незалежність.
- Підтримку багатоточкових конференцій.
- Підтримку багатоадресної передачі.
- Стандарти для кодеків.
- Підтримку групової адресації.

Керування смугою пропущення

Передача аудіо- і відеоінформації досить інтенсивно навантажує канали зв'язку, і, якщо не стежити за ростом цього навантаження, працездатність критично важливих мережних сервісів може бути порушена. Тому рекомендації H.323 передбачають керування смугою пропущення. Можна обмежити як число одночасних з'єднань, так і сумарну смугу пропущення для всіх додатків H.323. Ці обмеження допомагають зберегти необхідні ресурси для роботи інших мережних додатків. Кожний термінал H.323 може управляти своєю смугою пропущення в конкретній сесії конференції. Див. рішення VCON для керування смугою пропущення

Міжмережні конференції

Рекомендації H.323 пропонують засіб з'єднання учасників відеоконференції в різнорідних мережах (наприклад, IP і ISDN, IP і PSTN).

Платформна незалежність

H.323 не прив'язаний ні до яких технологічних рішень, пов'язаним з устаткуванням або програмним забезпеченням. Взаємодіючі між собою додатки можуть створюватися на основі різних платформ, з різними операційними системами.

Підтримка багатоточкових конференцій

Рекомендації H.323 дозволяють організовувати конференцію із трьома або більше учасниками. Багатоточкові конференції можуть проводитися як з використанням центрального MCU (пристрою багатоточкової конференції), так і без нього.

Підтримка багатоадресной передачі

H.323 підтримує багатоадресну передачу в багатоточкової конференції, якщо мережа підтримує протокол керування груповою адресацією (такий, як IGMP). При багатоадресній передачі один пакет інформації отримується усіма необхідним адресатама без зайвого дублювання. Багатоадресна передача використовує смугу пропущення набагато більш ефективно, оскільки всім адресатам – учасникам списку розсилання відправляється рівно один потік. Див. VCON Interactive Multicast

Стандарти для кодеків

H323 установлює стандарти для кодування й декодування аудіо- і відеопотоків з метою забезпечення сумісності встаткування різних виробників. Разом з тим стандарт досить гнучкий. Існують вимоги, виконання яких обов'язково, і існують опціональні можливості, у випадку використання яких також необхідно строго додержуватися стандарту. Крім цього, виробник може включати в мультимедійні продукти й додатки додаткові можливості, якщо вони не суперечать обов'язковим і опціональним вимогам стандарту.

Сумісність

Учасники конференції хочуть спілкуватися один з одним, не піклуючись про питання сумісності між собою. Рекомендації H323 підтримують з'ясування загальних можливостей устаткування кінцевих користувачів і встановлюють найкращі із загальних для учасників конференції протоколів кодування, виклику й керування.

Гнучкість

H323 конференція може включати учасників, кінцеве встаткування яких має різні можливості. Наприклад, один з учасників може використовувати термінал як тільки з аудіо-можливостями, у той час як інші учасники конференції можуть мати можливості передачі/прийому також відео й даних.

Таблиця 1 – Зведена таблиця протоколів сімейства H.32x

Стандарт /характе-ристика	H.320	H.321	H.322	H.323	H.324	H.324/C	H.310
Рік прий-няття	1990	1995	1995	1996	1996	1998	1996
Остання редакція	1.3	1.3	1.3	1.3	1.3	—	—
Мережа	Вузько-полосна комуту-єма ISDN	H.320у Ш-ISDN й ATM	Мережа ПК із гаран-тованою пропуск-ною здатністю	Мережа із ПК із негарна-тованої пропуск-ною здатні-стю (Ethernet)	Анало-гова телефон-на система	Мобіль-ний зв'язок	Ш-ISDN, ATM, LAN
Відео	H.261, H.263	H.261, H.263	H.261, H.263	H.261, H.263, H.263+, H.264	H.261, H.263	H.261, H.263	MPEG-2 (H.262), H.261
Аудіо	G.711, G.722, G.728	G.711, G.722, G.728	G.711, G.722, G.728	G.711, G.722, G.723, G.728, G.729	G.723.1	G.723	MPEG-2, G.711, G.722, G.728
Мульти-плексу-вання	H.221	H.221	H.221	H.225.0	H.223	H.223A	H.222.0, H.222.1 (MPEG)
Керу-вання	H.230, H.242	H.242	H.242, H.230	H.245	H.245	H.245	H.245

Конференції	H.231, H.243	H.231, H.243	H.231, H.243	H.332			
Дані	T.120	T.120	T.120	T.120	T.120	T.120	T.120
Комунікаційний інтерфейс	I.400	AAL I.363, ATM I.361, PHY I.400	I.400 і TCP/IP	TCP/IP	Модем V.34	Мобільне радіо	AAI I.363, ATM I.361, PHY I.432

Базова архітектура стандарту H.323

У число "об'єктів" H.323, як вони названі в стандарті, включаються термінали, мультимедіа шлюзи, пристрої керування багатоточковими конференціями й контролери зони (Gatekeeper).

Термінал (Terminal) – прикінцевий мультимедійний (голос, відео, дані) пристрій, призначений для участі в конференції

Мультимедіа шлюз (Gateway) – пристрій, призначений для перетворення мультимедійної й керуючої інформації при сполученні різнорідних мереж.

Пристрій керування багатоточковими конференціями (Multipoint Control Unit – MCU) – призначено для організації конференцій за участю трьох і більше учасників

Контролер зони (Gatekeeper, Воротар, Конференц-менеджер) – що рекомендується, але не обов'язковий пристрій, що забезпечує мережне керування й виконує роль віртуальної телефонної станції.

Термінали H.323

Під терміналом стандарт розуміє встаткування кінцевих точок мережі, що дозволяє користувачам спілкуватися один з одним у реальному часі.

Термінали повинні підтримувати протоколи H.245 – узгодження параметрів з'єднання, Q.931 – для встановлення з'єднання й узгодження параметрів цього з'єднання, канал RAS (Registration/Admission/Status) взаємодії з контролером зони (Gatekeeper), протокол RTP/RTCP для роботи з потоками аудіо й відео пакетів, протокол G.711 для стиску аудіопотоку.

Відповідно до рекомендацій, для термінала H.323 опціональною є підтримка видеокодеків, протоколу T.120, і можливостей MCU.

Відеоможливості терміналів H.323

Незважаючи на те, що стандарт уважає функції відео необов'язковими, всі термінали з відеоможливостями повинні підтримувати кодек H.261, опціонально можлива підтримка H.263.

H.263 є розвитком кодека H.261, відеокартинка, отримана за допомогою кодека H.263 має кращу якість, оскільки використовується полупіксельна технологія пророкування руху. Крім того, використовуване кодування по Хаффману оптимізовано для роботи з більше низькими швидкостями передачі.

Визначено п'ять стандартних форматів кадрів:

Мультимедіа шлюз (Gateway) H.323

Згідно H.323, мультимедіа шлюз – це опціональний елемент у конференції H.323. Він може виконувати багато різних функцій. Типовою його функцією є завдання перетворення форматів протоколів передачі (наприклад, H.225.0 і H.221). Звичайно мультимедіа шлюзи використовуються для підтримки взаємодії між різнорідними мережами. На Рис.3. показано шлюз H.323/PSTN.

Контролер зони (Gatekeeper, Воротар, Конференц-менеджер)

Це рекомендований, але не обов'язковий пристрій, що забезпечує мережне керування й виконує роль віртуальної телефонної станції.

Основними функціями контролера зони є:

– Керування й адресація викликів.

– Забезпечення основними типами обслуговування, такими як телефонний довідник і сервісом, характерним для УАТМ (передача й перенапрямок викликів і т.д.).

– Керування використанням смуги пропущення додатками Н.323 таким чином, щоб забезпечити якість обслуговування (QoS).

– Керування загальним використанням мережних ресурсів.

– Системне адміністрування й забезпечення безпеки.

Незважаючи на те, що Рекомендації Н.323 визначають контролер зони як необов'язковий компонент, без нього неможливо скористатися потужним і різноманітним спектром послуг, передбачених творцями стандарту Н.323 для додатків IP-телефонії й мультимедійних телеконференцій.

Пристрій керування багатоточковою конференцією (Multipoint Control Units (MCU))

Пристрій MCU призначений для підтримки конференції між трьома й більше учасниками. У цьому пристрої повинен бути присутнім контролер Multipoint Controller (MC), і, можливо, процесори Multipoint Processors (MP). Контролер MC підтримує протокол Н.245 і призначений для узгодження параметрів обробки аудіо- і відеопотоків між терміналами. Процесори займаються комутуванням, мікшуванням і обробкою цих потоків.

Конфігурація багатоточкової конференції може бути централізованої, децентралізованої, гібридної й змішаної.

Централізована багатоточкова конференція вимагає наявності пристрою MCU. Кожний термінал обмінюється з MCU потоками аудіо, відео, даними й командами керування за схемою " точка-точка". Контролер MC, використовуючи протокол Н.245, визначає можливості кожного термінала. Процесор MP формує необхідні для кожного термінала мультимедійні потоки й розсилає їх. Крім того, процесор може забезпечувати перетворення потоків від різних кодеків з різними швидкостями даних.

Децентралізована багатоточкова конференція використовує технологію групової адресації. Приймаючі участь в конференції Н.323 термінали здійснюють багатоадресну передачу мультимедіа потоку іншим учасникам без посилки на MCU. Передача контрольної й керуючої інформації здійснюється за схемою "точка-точка" між терміналами й MCU. У цьому випадку контроль багатоточкового розсилання здійснюється контролером MC.

Гібридна схема організації відео-конференц-зв’язку є комбінацією двох попередніх. Приймаючі участь в конференції Н.323 термінали здійснюють багатоадресну передачу тільки аудіо- або тільки відеопотоку іншим учасникам без посилки на MCU. Передача інших потоків здійснюється за схемою " точка-точка" між терміналами й MCU. У цьому випадку задіються як контролер, так і процесор MCU.

У змішаній схемі організації відео-конференц-зв’язку одна група терміналів може працювати за централізованою схемою, а інша група – по децентралізованій.

Тенденції розвитку рекомендацій Н.323

Н.323 v.2

У другій версії Н.323 v.2 рекомендацій були усунуті недоліки попередньої версії. Були вдосконалені існуючі протоколи: Q.931, Н.245 і Н.225, а також уведений ряд нових. Основні переваги нової версії стандарту полягають у додаванні функцій безпеки, установки швидкого виклику, деяких додаткових сервісів і інтеграції протоколів Н.323 і Т.120.

– Функції безпеки (Н.235) містять у собі забезпечення автентифікації (механізм, що підтверджує те, що учасники конференції саме ті, за яких вони себе видають), цілісності (механізм, що підтверджує те, що передані пакети не були перекручені), криптографічний захист переданої інформації від несанкціонованого доступу.

– Функція Fast Call Setup вирішує проблему, що була в першій версії, коли після проходження дзвінка одного абонента іншому могла бути затримка в проходженні аудіо й відеопотоків.

– Протокол Т.120 був інтегрований і в першу версію рекомендацій Н.323, однак сценарії установки дзвінка були досить складні. У другій версії рекомендацій Н.323 ця

проблема вирішується в такий спосіб: стандарт вимагає, щоб устаткування кінцевих користувачів, що підтримує одночасно й T.120, і H.323, управлялося дзвінками по H.323. Більше того, відповідно до другої версії рекомендацій T.120 є опціональною частиною конференції H.323 і можливості дій по T.120 віддаються на розсуд кожного пристрою в H.323 конференції окремо.

H.323 v.3

У третій версії H.323 v.3 рекомендацій було уведено кілька нових можливостей. Насамперед вони стосуються доповнень до основного документа й рекомендацій H.225.0, вносячи вдосконалення в архітектуру стандарту. Серед них можна виділити:

– Більше ефективне використання раніше встановлених сигнальних з'єднань, зокрема, між мультимедіа шлюзом і контролером зони.

– Можливість переадресації виклику при встановленому з'єднанні.

– Підвищено зручність одержання інформації про абонентів (Caller ID).

– Сигнальна інформація містить у собі інформацію про мову абонента, що розширює можливості обробки виклику.

– Запропоновано механізм, що полегшує додавання нових кодеків.

– Механізм сигналізації може тепер використовувати UDP транспорт, замість TCP, що істотно для конференцій з більшим числом учасників.

– Уведено поняття спрощеного термінала (Simple Endpoint Type – SET). Такі термінали можуть підтримувати тільки незначну частину рекомендацій H.323, проте забезпечуючи проведення аудіозв’язку з іншими H.323 терміналами.

– Уведено можливість SNMP – керування встаткуванням відео-конференц-зв’язку.

– Інформаційна база керування (MIB) описується документом H.341.

H.323 v.4

Четверта версія рекомендацій H.323 v.4 прийнята 17 листопада 2000 року. Туди внесено багато змін з метою підвищення надійності, мобільності й гнучкості систем відеоконференцій. Нові можливості, що стосуються мультимедіа шлюзів і пристроїв багатоточкової конференції, спрямовані на підвищення якості організації й проведення конференції з більшим числом учасників. Перелічимо деякі з нововведень.

– Нові механізми підвищення стійкості роботи H.323 конференції.

– Декомпозиція структури мультимедіа шлюзу з метою відділення модуля керування від виконавчих пристроїв.

– Можливість мультиплексування аудіо й відео в одному RTP потоці.

– Модифікація процесу реєстрації на контролері зони з метою полегшити реєстрацію великої кількості учасників конференції.

– Удосконалювання механізмів розподілу навантаження й підвищення стійкості роботи контролерів зони

– Для терміналів H.323 передбачаються способи виділення реально необхідної смуги пропущення як для звичайної, так і для групової адресації.

На даний момент використовується H.323 v.5.

Група стандартів Wi-Fi IEEE 802.11

Розробкою стандартів Wi-Fi 802.11 займається організація IEEE (Institute of Electrical and Electronic Engineers).

IEEE 802.11 – базовий стандарт для мереж Wi-Fi, що визначає набір протоколів для найнижчих швидкостей передачі даних (transfer).

IEEE 802.11b – описує більші швидкості передачі й уводить більше технологічних обмежень. Цей стандарт широко просувався з боку WECA (Wireless Ethernet Compatibility Alliance) і споконвічно називався Wi-Fi.

Використовуються частотні канали в спектрі 2.4GHz.

Ратифікований в 1999 році.

Використовувана радіочастотна технологія: DSSS.

Кодування: Barker 11 і CCK.

Модуляції: DBPSK і DQPSK.

Максимальні швидкості передачі даних (transfer) у каналі: 1, 2, 5.5, 11 Mbps.

IEEE 802.11a – описує значно більше високі швидкості передачі (transfer) чим 802.11b.

Використовуються частотні канали в частотному спектрі 5GHz.

Протокол не сполучимо з 802.11b.

Ратифікований в 1999 році.

Використовувана радіочастотна технологія: OFDM.

Кодування: Convoltion Coding.

Модуляції: BPSK, QPSK, 16-QAM, 64-QAM.

Максимальні швидкості передачі даних у каналі: 6, 9, 12, 18, 24, 36, 48, 54 Mbps.

IEEE 802.11g – описує швидкості передачі даних еквівалентні 802.11a.

Використовуються частотні канали в спектрі 2.4GHz. Протокол сполучимо з 802.11b.

Ратифікований в 2003 році.

Використовувані радіочастотні технології: DSSS і OFDM.

Кодування: Barker 11 і CCK.

Модуляції: DBPSK і DQPSK.

Максимальні швидкості передачі даних (transfer) у каналі:

– 1, 2, 5.5, 11 Mbps на DSSS;

– 6, 9, 12, 18, 24, 36, 48, 54 Mbps на OFDM.

IEEE 802.11n – самий передовий комерційний Wi-Fi-стандарт, на даний момент, офіційно дозволений до ввозу й застосування на території України (802.11ac поки в процесі пророоблення регулятором). В 802.11n використовуються частотні канали в частотних спектрах Wi-Fi 2.4GHz і 5GHz. Сполучимо з 11b/11a/11g. Хоча рекомендується будувати мережі з орієнтацією тільки на 802.11n, тому що потрібне конфігурування спеціальних захисних режимів при необхідності зворотної сумісності із застарілими стандартами. Це веде до великого приросту сигнальної інформації й істотному зниженню доступної корисної продуктивності радіоінтерфейсу. Властиво навіть один клієнт Wi-Fi 802.11g або 802.11b зажадає спеціального налаштування всієї мережі й миттєвої її суттєвої деградації в частині агрегованої продуктивності.

Сам стандарт Wi-Fi 802.11n вийшов 11 вересня 2009 року.

Підтримуються частотні канали Wi-Fi шириною 20MHz і 40MHz (2x20MHz).

Використовувана радіочастотна технологія: OFDM.

Використовується технологія OFDM MIMO (Multiple Input Multiple Output) аж до рівня 4x4 (4x передавача й 4x приймача). При цьому мінімум 2x передавача на Точку Доступу й 1x передавач на користувальницький пристрій.

SGI це захисні інтервали між фреймами.

Spatial Streams ця кількість просторових потоків.

Type це тип модуляції.

Data Rate це максимальна теоретична швидкість передачі даних у радіоканалі в Мбіт/сек.

Важливо підкреслити, що зазначені швидкості відповідають поняттю channel rate і є граничним значенням з використанням даного набору технологій у рамках описуваного стандарту(властиво ці значення, як Ви ймовірно помітили, виробники пишуть і на коробках домашніх Wi-Fi-пристроїв у магазинах). Але в реальному житті ці значення не досяжні в силу специфіки самої технології стандарту Wi-Fi 802.11. Наприклад тут сильно впливає "політкоректність" у частині забезпечення CSMA/CA (пристрої Wi-Fi постійно слухають ефір і не можуть передавати, якщо середовище передачі зайняте), необхідність підтвердження кожного юнікастового фрейму, напівдуплексна природа всіх стандартів Wi-Fi і тільки 802.11ac/ Wave-2 зможе це почати обходити з MU-MIMO і т.інш.. Тому практична ефективність застарілих стандартів 802.11 b/g/a ніколи не перевищує 50% в ідеальних умовах(наприклад для 802.11g максимальна швидкість на абонента звичайно не вище

22Мб/с), а для 802.11n ефективність може бути до 60%. Якщо ж мережа працює в захищеному режимі, що часто й відбувається через змішану присутність різних Wi-Fi-Чипів на різних пристроях у мережі, то навіть зазначена відносна ефективність може впасти в 2-3 рази. Це стосується, наприклад, міксу з Wi-Fi пристроїв із чипами 802.11b, 802.11g у мережі із точками доступу Wi-Fi 802.11g або пристрою Wi-Fi 802.11g/802.11b у мережі із точками доступу Wi-Fi 802.11n і т.п.. Докладніше про MIMO.

Крім основних стандартів Wi-Fi 802.11a, b, g, n, існують і використовуються додаткові стандарти для реалізації різних сервісних функцій:

– **802.11d**. Для адаптації різних пристроїв стандарту Wi-Fi до специфічних умов країни. Усередині регуляторного поля кожної держави діапазони часто розрізняються й можуть бути відмінні навіть у залежно від географічного положення. Стандарт Wi-Fi IEEE 802.11d дозволяє регулювати смуги частот у пристроях різних виробників за допомогою спеціальних опцій, уведених у протоколи керування доступом до середовища передачі.

– **802.11e**. Описує класи якості QoS для передачі різних медіафайлів і, у цілому різного медіаконтенту. Адаптація MAC-рівня для 802.11e, визначає якість, наприклад, одночасної передачі звуку й зображення.

– **802.11f**. Спрямований на уніфікацію параметрів Точок Доступу стандарту Wi-Fi різних виробників. Стандарт дозволяє користувачеві працювати з різними мережами при переміщенні між зонами дії окремих мереж.

– **802.11h**. Використовується для запобігання створення проблем метеорологічному й військовому радарам шляхом динамічного зниження випромінюваної потужності Wi-Fi устаткуванням або динамічний перехід на інший частотний канал при виявленні триггерного сигналу (у більшості європейських країн наземні станції спостереження за метеорологічними супутниками й супутниками зв'язку, а також радари військового призначення працюють у діапазонах, близьких до 5 Мгц). Цей стандарт є необхідною вимогою ETSI, пропонованим до встаткування, допущеному для експлуатації на території країн Європейського Союзу.

– **802.11i**. У перших варіантах стандартів Wi-Fi 802.11 для забезпечення безпеки мереж Wi-Fi використовувався алгоритм WEP. Передбачалося, що цей метод може забезпечити конфіденційність і захист переданих даних авторизованих користувачів бездротової мережі від прослуховування.Тепер цей захист можна зламати всього за кілька хвилин. Тому в стандарті 802.11i були розроблені нові методи захисту мереж Wi-Fi, реалізовані як на фізичному, так і програмному рівнях. У цей час для організації системи безпеки в мережах Wi-Fi 802.11 рекомендується використовувати алгоритми Wi-Fi Protected Access (WPA). Вони також забезпечують сумісність між бездротовими пристроями різних стандартів і різних модифікацій. Протоколи WPA використовують удосконалену схему шифрування RC4 і метод обов'язкової автентифікації з використанням EAP. Стійкість і безпека сучасних мереж Wi-Fi визначається протоколами перевірки конфіденційності й шифрування даних (RSNA, TKIP, CCMP, AES). Найбільш рекомендованим підходом є використання WPA2 із шифруванням AES (і не забувайте про 802.1x із застосуванням, дуже бажано, механізмів туннелювання, наприклад EAP-TLS, TTLS і т.п.).

– **802.11k**. Цей стандарт фактично спрямований на реалізацію балансування навантаження в радіопідсистемі мережі Wi-Fi. Звичайно в бездротовій локальній мережі абонентський пристрій звичайно з'єднується з тією точкою доступу, що забезпечує найбільш сильний сигнал. Нерідко це приводить до перевантаження мережі в одній точці, коли до однієї Точки Доступу підключається відразу багато користувачів. Для контролю подібних ситуацій у стандарті 802.11k запропонований механізм, що обмежує кількість абонентів, що підключаються до однієї Точки Доступу, і даючий можливість створення умов, при яких нові користувачі будуть приєднуватися до інший ТД навіть не дивлячись на більше слабкий сигнал від її. У цьому випадку агрегована пропускна здатність мережі збільшується завдяки більше ефективному використанню ресурсів.

– **802.11m**. Виправлення й виправлення для всієї групи стандартів 802.11 поєднуються підсумуються в окремому документі із загальною назвою 802.11m. Перший випуск 802.11m був в 2007 г, далі в 2011 г и т.інш.

– **802.11p**. Визначає взаємодія Wi-Fi-устаткування, що рухається зі швидкістю до 200 км/год повз нерухливі Точки Доступу Wi-Fi, віддалених на відстань до 1 км. Частина стандарту Wireless Access in Vehicular Environment (WAVE). Стандарти WAVE визначають архітектуру й додатковий набір службових функцій і інтерфейсів, які забезпечують безпечний механізм радіозв'язку між транспортними засобами, що рухаються. Ці стандарти розроблені для таких додатків, як, наприклад, організація дорожнього руху, контроль безпеки руху, автоматизований збір платежів, навігація й маршрутизація транспортних засобів і ін.

– **802.11r**. Визначає швидкий автоматичний роумінг Wi-Fi-пристроїв при переході із зони покриття однієї Точки Доступу Wi-Fi до зони покриття іншої. Цей стандарт орієнтований на реалізацію Мобільності й, насамперед, важливий саме для мобільних/ пристроїв, щоносяться, з Wi-Fi, наприклад, смартфонов, планшетних комп'ютерів, Wi-Fi IP-телефонів і т.п.. До появи цього стандарту при русі користувач часто втрачав зв'язок з однією точкою доступу, був змушений шукати іншу й заново виконувати процедуру підключення. Це займало багато часу. Існували приватні рішення проблеми роумінгу (хендоверів) між пристроями, наприклад від CCKM від Cisco. Пристрої з підтримкою 802.11r можуть зареєструватися заздалегідь із сусідніми Точками Доступу Wi-Fi і виконувати процес перепідключення в автоматичному режимі. У такий спосіб значно зменшується час, коли абонент не доступний у мережах Wi-Fi.

– **802.11s**. Стандарт для реалізації повнозв'язних мереж (Wireless Mesh), де будь-який пристрій може служити як маршрутизатором, так і точкою доступу. Якщо найближча точка доступу перевантажена, дані перенаправляються до найближчого незавантаженого вузла. При цьому пакет даних передається (packet transfer) від одного вузла до іншого, поки не досягне кінцевого місця призначення. У даному стандарті уведені нові протоколи на рівнях MAC і PHY, які підтримують широкомовну й багатоадресну передачу (transfer), а також одноадресну поставку по самоконфігуруючійся системі точок доступу Wi-Fi. С цією метою в стандарті уведений чотирьохадресний формат кадру.

– **802.11t**. Стандарт створений для інституалізації процесу тестування рішень стандарту IEEE 802.11. Описуються методики тестування, способи вимірів і обробки результатів (treatment), вимоги до іспитового встаткування.

– **802.11u**. Визначає процедури взаємодії мереж стандарту Wi-Fi із зовнішніми мережами. Стандарт повинен визначати протоколи доступу, протоколи пріоритету й заборони на роботу із зовнішніми мережами. На даний момент навколо даного стандарту утворився великий рух як у частині розробки рішень – Hotspot 2.0, так і в частині організації міжмережного роумінгу – створена й росте група зацікавлених операторів, які спільно вирішують питання роумінгу для своїх Wi-Fi-мереж у діалозі (Альянс WBA).

– **802.11v**. У стандарті повинні бути розроблені виправлення, спрямовані на вдосконалювання систем керування мережами стандарту IEEE 802.11. Модернізація на MAC- і PHY-рівнях повинна дозволити централізувати й упорядкувати конфігурацію клієнтських пристроїв, з'єднаних з мережею.

– **802.11y**. Додатковий стандарт зв'язку для діапазону частот 3,65-3,70 Ггц. Призначений для пристроїв останнього покоління, що працюють із зовнішніми антенами на швидкостях до 54 Мбіт/с на відстані до 5 км на відкритому просторі. Стандарт повністю не завершений.

802.11w. Визначає методи й процедури поліпшення захисту й безпеки рівня керування доступом до середовища передачі даних (MAC). Протоколи стандарту структурують систему контролю цілісності даних, дійсності їхнього джерела, заборони несанкціонованого відтворення й копіювання, конфіденційності даних і інших засобів захисту. У стандарті уведений захист фрейму керування (MFP: Management Frame Protection), а додаткові заходи

безпеки дозволяють нейтралізувати зовнішні атаки, такі, як, наприклад, DoS. Крім того, ці міри забезпечать безпеку для найбільш уразливої мережної інформації, що буде передаватися по мережах з підтримкою IEEE 802.11r, k, y.

802.11ac. Новий стандарт Wi-Fi, що працює тільки в частотній смузі 5 ГГц і забезпечує значно більші швидкості як на індивідуального клієнта Wi-Fi, так і на Точку Доступу Wi-Fi.

Висновок. У статті розглянуто та проаналізовано програмне забезпечення, яке призначено для відеотехнологій для цифрової трансформації з підтримкою Wi-Fi. В межах України в недостатній мірі представлені вітчизняні розробки в цій області. У роботі наведені теоретичне узагальнення й рішення наукового завдання дослідження методів цифрової трансформації з підтримкою Wi-Fi. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем цифрової трансформації з підтримкою Wi-Fi; Досліджена система цифрової трансформації з підтримкою Wi-Fi.; На основі отриманих результатів досліджень створена програмна реалізація відеотехнологій для цифрової трансформації з підтримкою Wi-Fi. Розроблені під час виконання роботи алгоритми дозволяють успішно вирішувати завдання цифрової трансформації з підтримкою Wi-Fi. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки. Розроблене програмне забезпечення має простий, дружній та зручний інтерфейс користувача, що забезпечує легкість у освоєнні роботи програмного продукту, зручність у використанні, і не потребує особливих спеціальних знань. При створені програмного забезпечення було використано об’єктно-орієнтований підхід, що відповідає сучасним тенденціям у галузі розробки комерційних програмних систем. Програма реалізована на мові високого рівня Embarcadero Delphi 10.2 Tokyo. Дана мова програмування дозволяє найбільш ефективно обробляти дані. Це дозволило мінімізувати строк розробки програмного забезпечення, і, як слід, зменшити витрати на його розробку. Запропоноване програмне забезпечення ділиться на загальне програмне забезпечення, що поставляється із засобами обчислювальної техніки й спеціальне програмне забезпечення, що спеціально розроблене для даної конкретної системи й включає програми, що реалізують її функції. Даються необхідні рекомендації з установки розробленого програмного забезпечення. Для підвищення рівня безпеки запропоновано застосовувати алгоритм SHACAL-1.

Список літератури

1. Дреев А.Н. Использование неравномерного распределения единичных битов для дополнительного сжатия SPIHT кода / А.Н. Дреев, А.А. Смирнов // Информационные системы в управлении, образовании, промышленности: монография. Под редакцией профессора В.С. Пономаренко. – Х.: Вид-во ТОВ «Щедра садиба плюс», 2014. – С. 498.
2. Дрєєв О.М. Дослідження впливу шляху розгортки на ступінь ентропійного стиснення цифрового зображення / О.М. Дрєєв, О.В. Слюсар // Збірник наукових праць Кіровоградського національного технічного університету. Техніка в сільськогосподарському виробництві, галузеве машинобудування, автоматизація. Випуск 21. – Кіровоград: КНТУ. – 2008 – С. 115-118.
3. Дрєєв О.М. Метод розвантаження телекомунікаційного сервера за рахунок кешування зображень / О.М. Дрєєв // Збірник наукових праць Кіровоградського національного технічного університету. Техніка в сільськогосподарському виробництві, галузеве машинобудування, автоматизація. Випуск 25. Ч. І. – Кіровоград: КНТУ. – 2012 – С. 419-424.
4. Дрєєв О.М. Метод прогнозування завантаженості серверу телекомунікаційної мережі / О.М. Дрєєв, О.А. Смірнов, Є.В. Мелешко, О.В. Коваленко // Системи обробки інформації. Випуск 3(101) Том 2. – Х.: ХУПС. – 2012. – С. 181-188.
5. Дрєєв О.М. Оцінка якості стиснення зображень на основі дискретного перетворення Хартлі / О.В. Коваленко, О.П. Доренський, О.М. Дрєєв // Системи озброєння і військова техніка. Науковий журнал 2(34) – Х.: ХУПС – 2013. С. 99-102.

6. Дрєєв О.М. Дослідження впливу ступеня стиснення зображень на оперативність їх доставки у телекомунікаційній системі / О.А. Смірнов, О.М. Дрєєв, О.П. Доренський // Збірник наукових праць "Системи обробки інформації". – Випуск 8(115). – Х.: ХУПС – 2013. – С. 234-239.
7. Дреев А.Н. Сравнение битовых плотностей при использовании различных методов кодирования информации / А.Н. Дреев, А.А. Смирнов // Системи обробки інформації, 2014, випуск 2 (118), том 2 – Харків: ХУПС – 2014. С 64-66.
8. Дрєєв О.М. Моделювання впливу інтенсивності трафіку на оперативність доставляння інформації / О.М. Дрєєв // Науково-виробничій журнал "Зв'язок". – Київ: ДУТ, 2014. – № 2 (108) С. 24-29.
9. Дреев А.Н. Повышение вероятности доставки сообщений в телекоммуникационных системах и сетях для обеспечения информационной безопасности / А.Н. Дреев, А.А. Смирнов //«Безпека інформації» Том 21, №1 2015 р. – Київ: НАУ – 2015. – С. 22-28.
10. Дрєєв О.М. Узагальнення вейвлету Хаара / О.М. Дрєєв, Г.М. Дрєєва // Збірник тез доповідей Комбінаторні конфігурації та їх застосування, 15-16 жовтня 2010 р. – Кіровоград – С. 58

УДК 004

П. Добровольський, магістр гр. КН-18МЗ-1,4
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ ІНФРАСТРУКТУРИ ВІРТУАЛЬНИХ РОБОЧИХ СТОЛІВ

У статті розглянуто розроблене програмне забезпечення, яке призначено для системи інфраструктури віртуальних робочих столів. Метою розробки є дослідження та програмна реалізація системи інфраструктури віртуальних робочих столів. Об'єктом дослідження є процес реалізації системи інфраструктури віртуальних робочих столів. Предметом дослідження є реалізації системи інфраструктури віртуальних робочих столів. Методи дослідження базуються на управлінні віртуальними робочими столами, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи інфраструктури віртуальних робочих столів. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення. Розроблено зручний інтерфейс користувача. Наведені інструкції по роботі з програмними засобами.

комп'ютерні науки, захист інформації, інфраструктура віртуальних робочих столів, віртуалізація

Постановка проблеми. Традиційний підхід до використання IT-сервісів в організації має на увазі їх розміщення на високонадійних і захищених серверах в центрах обробки даних(ЦОД) і доступ до них з ПК користувачів. Найчастіше саме призначений для користувача ПК виявляється найслабшою ланкою. Це призвело до появи термінальних служб, які давали можливість централізувати робоче оточення користувача в ЦОД і надавати доступ до нього за допомогою термінального клієнта з корпоративної мережі, або через інтернет. Однак термінальні служби володіли рядом обмежень, наприклад, неможливість створення повністю ізольованого оточення і технологія інфраструктури віртуальних робочих столів (VDI) стала закономірним розвитком даних рішень, дозволивши зняти більшість обмежень. Якщо говорити простою мовою про VDI – то це віртуалізація робочого місця і розміщення його в ЦОД з наданням гнучкого і централізованого управління. На відміну від служб терміналів, в подібній інфраструктурі кожен користувач отримує доступ до особистого настільного ПК з будь-якого авторизованого пристрою, тим самим підвищуючи гнучкість настільної системи. IT–відділи можуть використовувати весь комплекс переваг централізації, включаючи централізоване управління робочими навантаженнями настільних ПК і забезпечення безперервності ведення бізнесу. На даний момент технологія віртуалізації робочих столів має багато переваг:

– Швидке створення нових робочих місць;

– Зниження витрат на адміністрування і покупку нових ПК або комплектуючих які вийшли з ладу;
– Підвищення мобільності та безпеки;
– Управління всіма даними з однієї точки.

У свою чергу у технології є ряд недоліків:
– Вартість оренди або ж організація власного дата-центру;
– Складнощі в налаштуванні серверного обладнання;
– Залежність від високої пропускної здатності мережі.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини системи інфраструктури віртуальних робочих столів.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи інфраструктури віртуальних робочих столів.

Об'єктом дослідження є процес реалізації системи інфраструктури віртуальних робочих столів.

Предметом дослідження є методи реалізації системи інфраструктури віртуальних робочих столів.

Методи дослідження базуються на управлінні віртуальними робочими столами, методах розробки програмного забезпечення.

Виклад основного матеріалу. В процесі виконання роботи потрібно розробити програмне забезпечення для системи інфраструктури віртуальних робочих столів. Для розробки структури системи, визначення складових, їх взаємозв'язку, побудови функціональної схеми, розробки алгоритмів роботи системи та їх програмного опису, необхідно детально розглянути і означити вимоги та обмеження щодо системи та провести більш детальне визначення функцій.

Параметри, такі як: тип бази даних, IP-адреса, порт серверу, логін та пароль до бази даних повинні зберігатися в налаштуваннях програми і завантажуватись при кожному її запуску.

Програмне забезпечення повинне містити такі функції:
– реєстрація користувача;
– авторизація користувача;
– створення віртуального робочого столу;
– управління вірутальним робочим столом;
– виведення інформації про стан серверу;
– завантаження файлів на сервер.

Опис середовища розробки та відлагодження розроблюваного програмного забезпечення

Laravel прагне зробити весь досвід розробки на PHP приємним, включаючи місцеве середовище розробки. Vagrant пропонує простий, елегантний спосіб надання та управління віртуальних машин.

Laravel Homestead - це офіційна заздалегідь упакована коробка (box) Vagrant, яка забезпечує прекрасне середовище розробки, не вимагаючи встановлення PHP, веб-сервера та будь-якого іншого серверного програмного забезпечення на локальній машині. Якщо щось піде не так, є можливість знищити та знову створити коробку за лічені хвилини.

Homestead працює в будь-якій системі Windows, Mac або Linux і включає Nginx, PHP, MySQL, PostgreSQL, Redis, Memcached, Node та всі інші сервіси, які потрібні, для розробки Laravelзастосунків.

Архітектура серверної частини застосунку

Laravel - безкоштовний, з відкритим кодом PHP-фреймворк, призначений для розробки веб-застосунків відповідно до шаблону model-view-controller (MVC). Деякі з особливостей Laravel є модульна система упакування з виділеним менеджером залежностей

Composer, різні способи для доступу до реляційних баз даних, утиліти, які допомагають в розгортанні застосунків і технічного обслуговування, а також його орієнтація на синтаксичний цукор.

Опис архітектурного шаблону модель-вигляд-контролер

Модель-вигляд-контролер (Model-view-controller, MVC) - архітектурний шаблон, який використовується під час проектування та розробки програмного забезпечення.

Цей шаблон передбачає поділ системи на три взаємопов'язані частини: модель даних, вигляд (інтерфейс користувача) та модуль керування. Застосовується для відокремлення даних (моделі) від інтерфейсу користувача (вигляду) так, щоб зміни інтерфейсу користувача мінімально впливали на роботу з даними, а зміни в моделі даних могли здійснюватися без змін інтерфейсу користувача.

Мета шаблону - гнучкий дизайн програмного забезпечення, який повинен полегшувати подальші зміни чи розширення програм, а також надавати можливість повторного використання окремих компонентів програми. Крім того використання цього шаблону у великих системах сприяє впорядкованості їхньої структури і робить їх більш зрозумілими за рахунок зменшення складності. На рисунку 1 зображена діаграма взаємодії між компонентами шаблону.

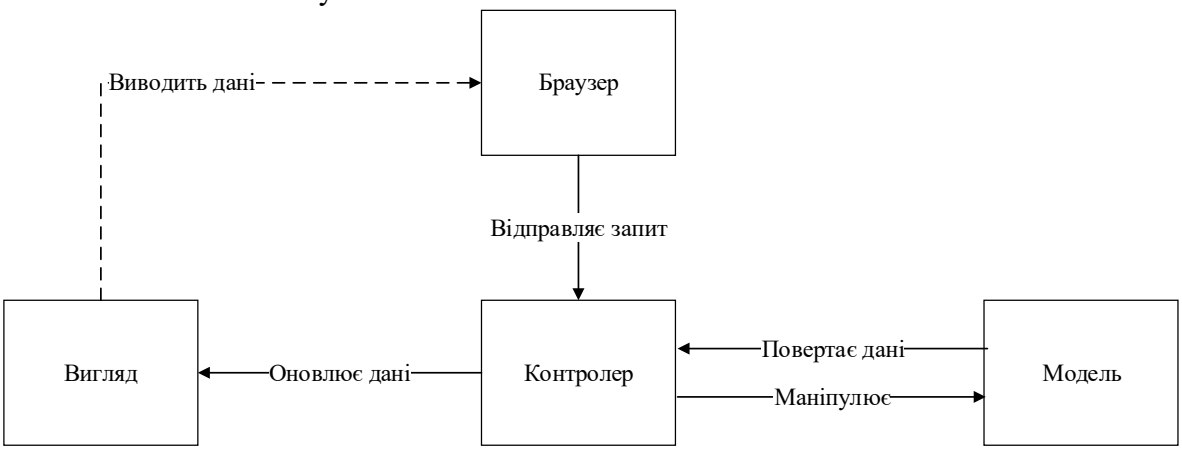


Рисунок 1 – Діаграма взаємодії між компонентами шаблону MVC

У рамках архітектурного шаблону модель–вигляд–контролер (MVC) програма поділяється на три окремі, але взаємопов'язані частини з розподілом функцій між компонентами. Модель (Model) відповідає за зберігання даних та їх структуру. Вигляд (View) відповідальний за представлення цих даних користувачеві, тобто інтерфейс програми. Контролер (Controller) керує компонентами, отримує сигнали у вигляді реакції на дії користувача (зміна положення курсора миші, натискання кнопки, ввід даних в текстове поле) і передає дані у модель.

– Модель є центральним компонентом шаблону MVC і відображає поведінку застосунку, незалежну від інтерфейсу користувача. Модель стосується прямого керування даними, логікою та правилами застосунку;

– Вигляд може являти собою будь-яке представлення інформації, одержуване на виході, наприклад графік чи діаграму. Одночасно можуть співіснувати кілька виглядів (представлень) однієї і тієї ж інформації, наприклад гістограма для керівництва компанії й таблиці для бухгалтерії;

– Контролер одержує вхідні дані й перетворює їх на команди для моделі чи вигляду.

Модель інкапсулює ядро даних і основний функціонал їхньої обробки і не залежить від процесу вводу чи виводу даних.

Вигляд може мати декілька взаємопов'язаних областей, наприклад різні таблиці і поля форм, в яких відображаються дані.

У функції контролера входить відстеження визначених подій, що виникають в результаті дій користувача. Контролер дозволяє структурувати код шляхом групування пов'язаних дій в окремий клас. Наприклад у типовому MVC-проекті може бути користувацький контролер, що містить групу методів, пов'язаних з управлінням обліковим записом користувача, таких як реєстрація, авторизація, редагування профілю та зміна пароля.

Зареєстровані події транслюються в різні запити, що спрямовуються компонентам моделі або об'єктам, відповідальним за відображення даних. Відокремлення моделі від вигляду даних дозволяє незалежно використовувати різні компоненти для відображення інформації. Таким чином, якщо користувач через контролер внесе зміни до моделі даних, то інформація, подана одним або декількома візуальними компонентами, буде автоматично відкоригована відповідно до змін, що відбулися.

Життєвий цикл запиту в Laravel

Точкою входу для всіх запитів до застосунку Laravel є файл public/index.php. Всі запити направляються в цей файл конфігурацією веб-сервера (Apache/Nginx). Файл index.php запускає автозавантажувач, сгенерований програмою Composer, а потім витягує екземпляр застосункуLaravel зі скриптуbootstrap/app.php. Перша дія, яку виконує сам Laravel – створює екземпляр контейнера застосунка/служби.

Далі вхідний запит надсилається або до ядра HTTP, або до ядра консолі, залежно від типу запиту, що надходить до програми. Ці два ядра служать центральним розташуванням, через яке проходять усі запити.

Ядро HTTP розширює клас Illuminate\Foundation\Http\Kernel, який визначає масив завантажувальних пристроїв, які будуть запускатися до виконання запиту. Ці завантажувачі налаштовують обробку помилок, налаштовують ведення журналів, виявляють середовище програми та виконують інші завдання, які необхідно виконати до того, як запит буде фактично оброблений.

Ядро HTTP також визначає список проміжного програмного забезпечення HTTP, через яке повинні пройти всі запити, перш ніж програма обробиться. Ці проміжні програми керують читанням і записом HTTP-сеансу, визначаючи, чи програма перебуває в режимі обслуговування, перевіряє маркер CSRF тощо.

Підпис методу для методу обробки ядра HTTP досить простий: отримати запит та повернути відповідь.

Однією з найважливіших дій завантаження ядра (Kernel) є завантаження постачальників послуг для застосунків. Усі постачальники послуг програми налаштовані в масиві постачальників файлів конфігураційного файлу config/app.php. Спочатку метод реєстрації буде викликаний для всіх провайдерів, потім, як тільки всі провайдери будуть зареєстровані, викличеться метод завантаження.

“Постачальники послуг” (Service providers) несуть відповідальність за завантаження всіх різних компонентів основи, таких як база даних, черга, перевірка та маршрутизація. Оскільки вони завантажують та налаштовують всі функції, пропоновані рамкою, постачальники послуг є найважливішим аспектом усього процесу завантаження Laravel.

Після завантаження програми та реєстрації всіх постачальників послуг, запит буде переданий маршрутизатору (router) для відправки. Маршрутизатор відправить запит на маршрут або контролер, а також запустить будь-яке проміжне програмне забезпечення конкретного маршруту.

Service providers справді є ключем до завантаження програми Laravel. Створюється екземпляр програми, реєструються постачальники послуг, і запит передається завантаженій програмі.

Контейнери служб в Laravel

Контейнер служб (Service Container) Laravel - це потужний інструмент для управління залежностями класу та виконання впровадження залежностей (dependency injection). Dependency Injection - це означає, що клас залежностей "впроваджується" в клас через конструктор або, в деяких випадках, "сеттер" методи.

Майже всі прив’язки service container будуть зареєстровані у service providers.

Постачальник послуг завжди матиме доступ до контейнера через властивість $this->app. Можна зареєструвати прив'язку за допомогою методу bind, передавши ім’я класу або інтерфейсу, яке хочемо зареєструвати, разом із Closure, яке повертає екземпляр класу:

```
$this->app->bind('HelpSpot\API', function ($app) {
   return new HelpSpot\API($app->make('HttpClient'));
});
```

Метод одиночки (singleton) прив'язує клас або інтерфейс до контейнера, який слід вирішити лише один раз. Після того, як прив’язка singleton буде здійснена, той самий єкземпляр об'єкта буде повернутий при наступних викликах у контейнер:

```
$this->app->singleton('HelpSpot\API', function ($app) {
   return new HelpSpot\API($app->make('HttpClient'));
});
```

Фасади в Laravel

Фасади надають "статичний" інтерфейс класам, які доступні в службовому контейнері програми. Фасади Laravel забезпечують доступ майже до всіх можливостей Laravel. Вони служать "статичними провідниками" для базових класів у контейнері служб, забезпечуючи перевагу короткого, виразного синтаксису, зберігаючи при цьому більше гнучкості та можливості для легкого тестування, ніж традиційні статичні методи.

Фасади мають багато переваг. Вони надають стислий синтаксис, що легко запам'ятовується та дозволяє використовувати функції Laravel, не запам'ятовуючи імена довгих класів, які потрібно впроваджувати або налаштовувати вручну. Крім того, завдяки унікальному використанню динамічних методів PHP їх легко протестувати.

Маршрутизація в Laravel

Усі маршрути Laravel визначені у файлах маршрутів, які знаходяться в каталозі routes. Ці файли автоматично завантажуються фреймворком. Файл routes/web.php визначає маршрути, призначені для веб-інтерфейсу. Цим маршрутам присвоюється група проміжного програмного забезпечення (middleware) для web, яка надає такі функції, як стан сесії та захист CSRF. Маршрути в routes/api.php присвоюються групі api middleware.

При проектуванні магістерської роботи потрібно визначити маршрути призначені для інтерфейсу користувача у файлі web.php:

1) Для кожного користувача – гостя. Маршрути без обмеження доступу:

– Виведення головної сторінки, з запитом типу GET та маршрутом “/”;

– Виведення та обробка сторінок та запитів авторизації і реєстрації користувача, з запитами типу GET, POST та маршрутами: “account/login”, “account/create”.

2) Для зареєстрованих користувачів, які є авторизованими (middleware – userAuthenticate):

– Вихід з облікового запису користувача, за маршрутом “account/logout”;

– Виведення сторінки облікового запису користувача зі списком віртуальних робочих столів – “account”;

– Виведення сторінки створення віртуального робочого столу – “account/desktops/create”;

– Виведення сторінки управління віртуальним робочим столом – “account/desktops/virtualDesktopId”.

```
<?php
Auth::routes();
Route::get('/', 'HomepageController@index')->name('homepage');
Route::group(['namespace' => 'Account', 'prefix' => 'account'], function () {
   Route::get('login', 'AuthController@getLogin')->name('account.login.page');
   Route::post('login', 'AuthController@postLogin')->name('account.login.submit');
   Route::get('create', 'AuthController@request')->name('account.request.page');
   Route::post('create', 'AuthController@requestPost')->name('account.request.post');
```

```
Route::group(['middleware' => 'userAuthenticate'], function () {
    Route::get('logout', 'AuthController@getLogout')->name('account.logout');
    Route::get('/', 'AccountController@index')->name('account.homepage');
    Route::get('/desktops/create', 'AccountController@create')-
>name('account.desktop.create');
    Route::get('/desktops/{virtualDesktop}', 'AccountController@index')-
>name('account.desktop.edit');
  });
});
```

Також потрібно визначити маршрути для доступу клієнтського програмного забезпечення яке буде розроблено за допомогою JavaScript фреймворку Angular – API, які доступні тільки авторизованим користувачам та знаходяться в однойменному файлі api.php:

– Створення віртуального робочого столу – “api/desktop/create”, запит типу POST;

– Повернення інформації про віртуальний робочий стіл - “api/desktop/{virtualDesktopId}”, запит типу GET;

– Видалення віртуального робочого столу - “api/desktop/{virtualDesktopId}”, запит типу DELETE;

– Запуск команди, введеної користувачем, на сервері - “api/desktop/{virtualDesktopId}/command”, запит типу POST;

– Повернення інформації про стан оперативної пам'яті - “api/desktop/{virtualDesktopId}/ram”, запит типу GET;

– Повернення інформації про стан навантаження процесору - “api/desktop/{virtualDesktopId}/cpu”, запит типу GET;

– Повернення інформації про файли та директорії на сервері - “api/desktop/{virtualDesktopId}/files”, запит типу GET;

– Завантаження файлів на сервер - “api/desktop/{virtualDesktopId}/files”, запит типу POST;

```
Route::group(['prefix' => 'api/desktop', 'middleware' => 'userAuthenticate'], function () {
  Route::post('create', 'DesktopController@store')->name('api.create.desktop');
  Route::group(['prefix' => '{virtualDesktop}'], function () {
    Route::get('/', 'DesktopController@getInfo')->name('api.get.desktop');
    Route::delete('/', 'DesktopController@delete')->name('api.delete.desktop');
    Route::post('command', 'DesktopController@runCommand')-
>name('api.post.command');
    Route::get('ram', 'DesktopController@runCommand')->name('api.get.ram');
    Route::get('cpu', 'DesktopController@runCommand')->name('api.get.cpu');
    Route::get('files', 'DesktopController@getFiles')->name('api.get.files');
    Route::post('files', 'DesktopController@uploadFiles')->name('api.post.files');
  });
});
```

Посереднє програмне забезпечення в Laravel

Посереднє програмне забезпечення Middleware забезпечує зручний механізм фільтрації HTTP-запитів, що надходять у програму. Наприклад, Laravel включає middleware, яке підтверджує автентичність користувача програми. Якщо користувач не має автентифікації, middleware перенаправить користувача на сторінку авторизації. Однак якщо користувач авторизованний, middleware дозволить запиту продовжувати роботу в застосунку.

Додаткове проміжне програмне забезпечення можна написати для виконання різноманітних завдань, крім автентифікації. Middleware CORS (Cross-Origin Resource Sharing) може бути відповідальним за додавання належних заголовків (headers) до всіх відповідей, що повертаються клієнтському програмному забезпеченню. Middleware також може записувати всі вхідні запити до серверу.

У фреймворку Laravel є кілька проміжних програм, включаючи middleware для автентифікації та захисту CSRF. Усі ці проміжні програми знаходяться в каталозі app/Http/Middleware.

Потрібно розробити індивідуально налаштований Middleware для доступу виключно авторизованих користувачів зі звичайних сторінок та запитів з клієнтського програмного забезпечення написаного за допомогою Angular, тобто для API. Нижче наведений попередній код:

```
<?php namespace App\Http\Middleware;
use App\Contracts\ValueObjects\SessionUserInterface;
use App\Http\Controllers\Website\Account\AuthController as WebsiteAuthController;
use Closure;
class UserAuthenticate
{
   /**
    * Handle an incoming request.
    *
    * @param \Illuminate\Http\Request $request
    * @param \Closure $next
    * @return mixed
    */
   public function handle($request, Closure $next)
   {
      $sessionUser = \app(SessionUserInterface::class);
      if (\is_served_by_angular($request)) {
         return $next($request);
      }
      if ($sessionUser->isGuest()) {
         if ($request->ajax()) {
            return \response(lang('auth.unauthorized'), 401);
         } elseif ($request->wantsJson()) {
            return \json_response(['redirectTo' => route('account.login.page')], 302);
         } else {
            return \App::call(WebsiteAuthController::class . '@getLogin');
         }
      }
      return $next($request);
   }
}
```

Архітектура клієнтської частини застосунку

Клієнтська частини застосунку повинна бути гнучка, динамічна та інтуїтивно зрозуміла. Для вирішення цієї задачі було обрано фреймворк Angular 7 з використанням мови TypeScript для зручності розподілення та представлення типу змінних, який явно не задається у мові JavaScript. Зазначимо, що TypeScript не підтримується браузерами, тому компілюється саме в JavaScript.

Angular – це платформа та фреймворк для побудови клієнтських застосунків на HTML та TypeScript. Angular написаний на TypeScript. Він реалізує основну та додаткову функціональність як набір бібліотек TypeScript, які імпортуються в розроблюване програмне забезпечення.

Фундаментальними блоками Angular застосунку є NgModules, які забезпечують контекст компіляції компонентів. NgModules збирають відповідний код у функціональні набори; Angular застосунок визначається набором NgModules. У застосунку завжди є

кореневий модуль, який дозволяє завантажуватися, і, як правило, має ще багато функціональних модулів.

– Компоненти визначають представлення даних, що є набором елементів браузеру, які можна вибирати та змінювати відповідно до логіки та даних розроблюваного програмного забезпечення.

– Компоненти використовують сервіси, які надають певні функціональні можливості, не пов'язані безпосередньо з представленнями. Постачальники послуг можуть бути впроваджені в компоненти як залежності, що робить код модульним, багато-використовуваним та ефективним.

І компоненти, і сервіси – це просто класи, в яких є декоратори, які позначають їх тип та надають метадані, які вказують Angular як ними користуватися.

– Метадані класу компонентів асоціюють його з шаблоном, який визначає представлення. Шаблон поєднує звичайний HTML з Angular директивами та прив'язкою даних, що дозволяє Angular змінювати HTML, перш ніж відтворити його для користувача.

– Метадані для класу сервісу надають інформацію, яку Angular потребує, щоб зробити її доступною для компонентів через введення залежності (Dependency Injection).

Компоненти застосунку зазвичай визначають багато представлень, розташованих ієрархічно. Angular надає послугу маршрутизатора, щоб допомогти визначити шляхи навігації серед представлень. Маршрутизатор забезпечує складні навігаційні можливості в браузері.

Опис модулів Angular

Angular NgModules відрізняються від модулів JavaScript та доповнюють їх. NgModule оголошує контекст компіляції для набору компонентів, присвячених домену програми, робочому процесу або тісно пов'язаному набору можливостей. NgModule може асоціювати свої компоненти з відповідним кодом, таким як служби, для формування функціональних одиниць.

Кожен застосунок Angular має кореневий модуль, умовно названий AppModule, який забезпечує механізм завантаження. Застосунок, як правило, містить багато функціональних модулів.

Як і модулі JavaScript, NgModules можуть імпортувати функціональність з інших NgModules і дозволяти експортувати та використовувати їх власні функціональні можливості іншими NgModules. Наприклад, щоб скористатися послугою маршрутизатора потрібно імпортувати Router.

Організація коду у різні функціональні модулі допомагає в управлінні складними застосунками та розробці для повторного використання. Крім того, ця методика дозволяє скористатись “ледачим завантаженням” (lazy-loading), тобто завантаженням модулів на вимогу, щоб мінімізувати кількість коду, який потрібно завантажити при запуску.

Компоненти Angular застосунків

Кожний Angular застосунок має щонайменше один компонент, кореневий компонент, який з'єднує ієрархію компонентів із моделлю об'єкта сторінки документа (DOM). Кожен компонент визначає клас, який містить дані програми та логіку, і асоціюється з HTML-шаблоном, який визначає подання для відображення в цільовому середовищі.

Опис шаблонів, директив та прив'язки даних в Angular

Шаблон поєднує HTML з розміткою Angular, яка може змінювати елементи HTML до їх відображення. Директиви щодо шаблонів надають логіку програми, а розмітка прив'язки (*binding markup)* з'єднує дані програми та DOM. Існує два типи прив'язки даних:

– Прив'язка подій (*Event binding)* дозволяє застосунку реагувати на введення даних або дії користувачів, оновлюючи дані;

– Прив'язка властивостей (*Property binding)* дозволяє інтерполювати значення, які обчислюються з даних програми, в HTML.

Перед відображенням представлення,Angular визначає директиви та синтаксис прив'язки в шаблоні для зміни елементів HTML та DOM відповідно до даних програми та

логіки. Angular підтримує двосторонню прив'язку даних, тобто зміни в DOM, такі як вибір користувача, також впливають на дані програми.

Шаблони можуть використовувати канали (pipes) для поліпшення роботи користувача, перетворюючи значення для відображення. Наприклад, використовуються канали для відображення дат і значень валюти, які відповідають місцезнаходження користувача. Angular забезпечує заздалегідь задані канали для загальних перетворень, і також можна створити власні.

Сервіси та впровадження залежностей в Angular

Для даних або логіки, які не пов'язані з певним представленням даних, і які потрібно поширити серед компонентів, потрібно створити клас сервісу. Визначенню класу сервісу безпосередньо передує декоратор @Injectable(). Декоратор надає метадані, які дозволяють іншим постачальникам впровадити як залежність у клас.

Впровадження залежності дозволяє підтримувати класи компонентів компактними та ефективними. Вони не отримують дані з сервера, не перевіряють введенні дані користувачів або виводять безпосередньо до консолі браузера; вони делегують такі завдання сервісам.

Маршрутизація в Angular

Angular модуль Router надає можливість, яка дозволяє визначати шлях навігації серед різних станів програми та переглядати ієрархії у застосунку. Він моделюється за звичними умовами навігації в браузері:

– Введіть URL-адресу в адресний рядок, і браузер перейде на відповідну сторінку;
– Натисніть на посилання на сторінці, і браузер перейде на нову сторінку;
– Натисніть кнопки назад і вперед браузера, і браузер переміщається назад і вперед по всій історії, яку бачили.

Маршрутизатор відображає URL-подібні шляхи до представлень, замість сторінок. Коли користувач виконує дію, таку як натискання на посилання, яка завантажує нову сторінку у браузер, маршрутизатор перехоплює поведінку браузера та показує або приховує ієрархії перегляду.

Якщо маршрутизатор визначить, що поточний стан програми вимагає певної функціональності, а модуль, який визначає, що він не завантажений, маршрутизатор може ліниво завантажувати модуль на вимогу.

Маршрутизатор інтерпретує URL-адресу посилання відповідно до правил навігації у розроблюваному застосунку та стану даних. Можна перейти до нових представлень, коли користувач натискає кнопку або вибирає з випадаючого вікна. Маршрутизатор записує активність в історію веб-браузера, тому кнопки назад і вперед також працюють.

Щоб визначити правила навігації, потрібно зв’язати шляхи навігаціїзі створеними компонентами. Шлях використовує URL-подібний синтаксис, який інтегрує дані програми. Потім можна застосувати логіку програми, щоб вибрати, які елементи відображати чи ховати, у відповідь на введенні користувачем дані та власні правила.

Як для серверної частини застосунку, так і для клієнтської, потрібно розробити маршрутизацію для відображення сторінок у браузері. Нижче наведений вищесказані маршрути:

```
const routes: Routes = [
  {
        path: 'account', component: AccountComponent, data: {type: 'dashboard', title:
'Virtual Desktops'}
  },
  {
    path: 'account/desktops/create',
    component: AccountComponent,
    data: {type: 'desktops-create', title: 'Create a Virtual Desktop'},
  },
  {
```

```
    path: 'account/desktops/:id',
    children: [
      {
        path: '',
        component: DesktopInfoComponent,
        data: {type: 'desktop-edit', title: 'Desktop Info'},
      },
    ],
  },
];
```

Опис бази даних

Для створення таблиць баз даних в Laravel використовують міграції. З їх допомогою можна легко проаналізувати історію зміни структури таблиці, повернути все назад до запуску SQL команди та безпосередньо зручно проектувати таблиці.

Для розробки програмного забезпечення системи інфраструктури віртуальних робочих столів потрібні такі таблиці бази даних:

1) Таблиця користувачів users:

– id - ідентифікатор;
– name - ім'я користувача;
– email - електронна адреса;
– email_verified_at - дата та час підтвердження автентичності адреси;
– password - зашифрований пароль;
– last_appeared_at - дата та час останньої дії користувача;
– plan_code - код обраного тарифного плану;
– remember_token - токен для підтвердження входу користувача;
– created_at - дата та час створення запису;
– updated_at - дата та час останнього редагування;
– deleted_at - дата та час псевдо-видалення.

Міграція таблиціusers виглядає так:

```
Schema::create('users', function (Blueprint $table) {
    $table->bigIncrements('id');
    $table->string('name');
    $table->string('email')->unique();
    $table->timestamp('email_verified_at')->nullable();
    $table->string('password');
    $table->dateTime('last_appeared_at')->nullable();
    $table->string('plan_code')->default('');
    $table->rememberToken();
    $table->timestamps();
    $table->softDeletes();
});
```

2) Таблиця адміністраторівadmin_users:

– id - ідентифікатор;
– name - ім'я користувача;
– email - електронна адреса;
– password - зашифрований пароль;
– remember_token - токен для підтвердження входу користувача;
– reset_token - токен для скидання паролю;
– created_at - дата та час створення запису;
– updated_at - дата та час останнього редагування;
– deleted_at - дата та час псевдо-видалення.

Міграція таблиці admin_users:

```
Schema::create('admin_users', function (Blueprint $table) {
    $table->increments('id');
    $table->string('name');
    $table->string('email')->unique();
    $table->string('password', 60);
    $table->string('reset_token')->nullable();
    $table->string('remember_token', 100)->nullable();
    $table->timestamps();
    $table->softDeletes();
});
```

3) Таблиця для зберігання токенів скидання паролів користувачів:

– email - електронна адреса;
– token - токен для скидання паролю;
– created_at - дата та час створення запису.

Міграція таблиці password_resets:

```
Schema::create('password_resets', function (Blueprint $table) {
    $table->string('email')->index();
    $table->string('token');
    $table->timestamp('created_at')->nullable();
});
```

4) Таблиця для зберігання записів віртуальних робочих столів користувачів:

– id - ідентифікатор;
– user_id - ідентифікатор користувача для зв'язку з записом користувача;
– name - назва віртуальної машини.

Міграція таблиці virtual_desktop:

```
Schema::create('virtual_desktops', function (Blueprint $table) {
    $table->increments('id');
    $table->unsignedBigInteger('user_id')->index();
    $table->string('name')->default('');
    $table->timestamps();
    $table->foreign('user_id')
        ->references('id')
        ->on('users')
        ->onUpdate('CASCADE')
        ->onDelete('CASCADE');
});
```

На рисунку 2 зображено діаграму зв’язків між таблицями бази даних:

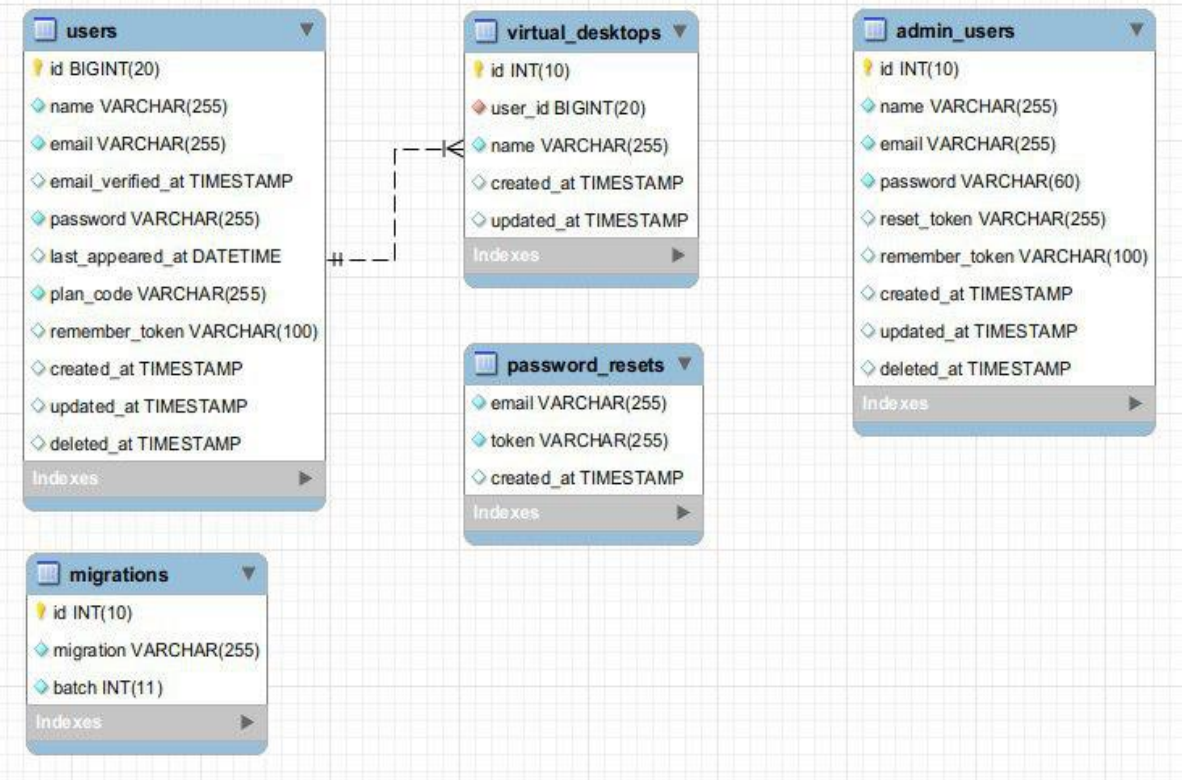


Рисунок 2 – Діаграма зв’язків таблиць бази даних за стосунку

Розробка структурної схеми

На рисунку 3 зображена структурна схема розробленого програмного забезпечення системи інфраструктури віртуальних робочих столів.

Розглянемо структурну схему клієнтськогопрограмного забезпечення. Вона складається з наступних блоків:

– Браузер;
– Головна сторінка застосунку;
– Сторінка авторизації;
– Сторінка авторизації;
– Блок швидкої авторизації;
– Блок вибору тарифного плану;
– Сторінка довідки застосунку.

Сторінка списку віртуальних робочих столів:

– Сторінка створення віртуального робочого стола;
– Сторінка управління віртуальним робочим столом.

Сторінка управління віртуальним робочим столом:

– Блок управління сервером через консоль;
– Блок перегляду інформації про стан сервера;
– Блок перегляду і завантаження файлів на сервер.

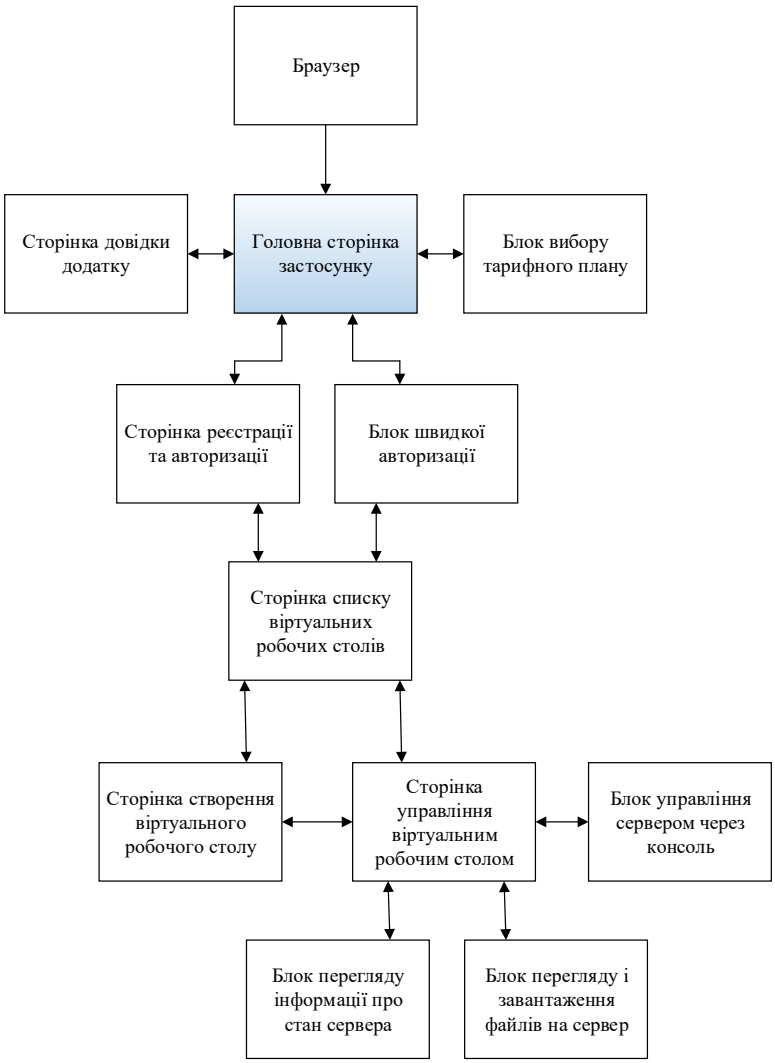


Рисунок 3 – Структурна схема клієнтського програмного забезпечення

Висновок. У статті розглянуто та проаналізовано програмне забезпечення, призначено для системи IDS яка базується на частотно-часовому аналізі. В процесі виконання роботи згідно ТЗ та постановки задачі був виконаний наступний обсяг роботи по розробці програмного забезпечення системи інфраструктури віртуальних робочих столів, а саме: Визначене призначення системи: створення, налаштування та використання віртуальних робочих столів. Проведене обґрунтування актуальності виконаної розробки. Визначена область застосування системи: у підприємстві.; Визначені концепція, основні принципи розробки та методологія побудови системи, розроблена постановка задачі щодо реалізації технічного завдання. Визначені та обґрунтовані засоби для побудови системи та мова програмування; Проведено опис і обґрунтування проектних рішень системи з ціллю визначення шляхів їх реалізації. Проведено опис функціонування системи. Розроблені: функціональна та структурна схеми системи, визначена взаємодія функцій та підфункцій програмного забезпечення, що підлягає розробці, і база даних. Окрім цього, визначена взаємодія процесів в системі, побудована діаграма взаємодії процесів в системі та надається її опис; Спроектоване технічне завдання на розробку програмного забезпечення системи.; Програма реалізована на мові PHP та JS. Дана мова програмування дозволяє найбільш ефективно реалізувати поставлену задачу щодо з'єднання програмного забезпечення з базою даних, що знаходиться на сервері. В цілому створене програмне забезпечення підтверджує правильність використаних проектних рішень та повністю відповідає вимогам технічного завдання. Створене програмне забезпечення має потенційну можливість для подальшого вдосконалення і застосування у різних галузях.

Список літератури

1. Майк МакГрат. PHP 7 для начинающих с пошаговыми инструкциями. 2018. –258 с.
2. Дэвид Скляр. Изучаем PHP 7. 2019. – 464с.
3. К. Дж. Дейт. SQL и реляционная теория. Как грамотно писать код на SQL. 2010. – 480 с.
4. Ржеуцкая С.Ю.Базы данных. Язык SQL. 2010. – 159 с.Ржеуцкая С.Ю.Базы данных. Язык SQL. 2010. – 159 с.
5. Денис Колисниченко. PHP и MySQL. Разработка Web-приложений. 2017. – 640с.
6. Дуглас Крокфорд. JavaScript. Сильные стороны. 2012. – 176с.
7. ЯковФайн. Angular и TypeScript. Сайтостроение для профессионалов. 2016. – 464с
8. Angular Docs [Електронний ресурс]. – Режим доступу до ресурсу: https://angular.io/docs
9. Laravel Documentation [Електронний ресурс]. – Режим доступу до ресурсу: https://laravel.com/docs/6.x
10. Владимир Дронов. Laravel. Быстрая разработка современных динамических Web-сайтов на PHP, MySQL, HTML и CSS. 2018. – 768с.

УДК 004

В. Доля, магістр гр. КН-18МЗ-1,4
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ КОМУНІКАЦІЙНОЇ ПЛАТФОРМИ ЯК СЕРВІСУ НА БАЗІ ALE RAINBOW

У статті розроблено програмне забезпечення, яке призначено для системи комунікаційної платформи як сервісу на базі ALE Rainbow. Метою розробки є дослідження та програмна реалізація системи комунікаційної платформи як сервісу на базі ALE Rainbow. Об'єктом дослідження є процес комунікаційної платформи як сервісу на базі ALE Rainbow. Предметом дослідження є методи комунікаційної платформи як сервісу на базі ALE Rainbow. Методи дослідження базуються на методах побудови хмарних платформ як сервісу, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи комунікаційної платформи як сервісу на базі ALE Rainbow. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення. Розроблено зручний інтерфейс користувача. Наведені інструкції по роботі з програмними засобами.

комп'ютерні науки, комунікаційна платформа як сервіс, ALE Rainbow

Постановка проблеми. При високому рівні конкуренції на ринку корпоративних комунікацій компанія Alcatel Lucent Enterprise (ALE) сподівається підсилити свої позиції завдяки пропозиції рішень для вертикальних ринків, у яких крім комунікаційних компонентів включена підтримка IoT. П'ять галузей, на які компанія робить ставку – державні установи, транспорт, утворення, охорона здоров'я й готельний бізнес. Для цих галузей будуть випускатися адаптовані рішення як, наприклад, комунікаційну платформу Alcatel-Lucent OpenTouch Hospitality Cloud для готельного бізнесу.

Основу стратегії Alcatel Lucent Enterprise становить Rainbow, «хмарна платформа керування взаєминами, що зв'язує людей, речі й системи». Інакше кажучи, це хмарна комунікаційна платформа, на якій розвиваються дві основних хмарних пропозиції компанії – уніфіковані комунікації як сервіс (as-a-Service, UCaaS) і комунікаційна платформа як сервіс (as-a-Service, CPaaS). Якщо не вдаватися в подробиці, Rainbow дозволяє реалізувати гібридні комунікації, наприклад, підключити наявні автоматичні телефонні мережі установи (УАТМ) до хмарних сервісів, причому це можуть телефонні станції й інших вендорів. На базі Rainbow також надається різна аналітика.

CPaaS позиціонується як платформа для керування комунікаційними потоками й інтеграції сторонніх застосунків. Вона пропонує відкриті API, за допомогою яких можна зокрема підключити УАТМ інших виробників. Це дозволяє, наприклад, вирішити таку застарілу проблему як відсутність видимості контактів: якщо контакти перебувають на одній УАТМ, а користувач підключений до іншої, то йому буде непросто з ними зв'язатися. При підключенні УАТМ до хмари він може їх переглянути.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи реалізація системи комунікаційної платформи як сервісу на базі ALE Rainbow.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи комунікаційної платформи як сервісу на базі ALE Rainbow.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем комунікаційної платформи як сервісу на базі ALE Rainbow.

– Дослідження системи комунікаційної платформи як сервісу на базі ALE Rainbow.

– Програмна реалізація системи комунікаційної платформи як сервісу на базі ALE Rainbow.

Об'єктом дослідження є процес комунікаційної платформи як сервісу на базі ALE Rainbow.

Предметом дослідження є методи комунікаційної платформи як сервісу на базі ALE Rainbow.

Методи дослідження базуються на методах побудови хмарних платформ як сервісу, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Компанія ALE (ця абревіатура утворена від Alcatel-Lucent Enterprise) 30 листопада випустила у світ нову віртуалізовану платформу керування комунікаціями, що забезпечує з'єднання бізнес-користувачів, бізнес-контактів і систем.

За інформацією компанії, платформа ALE Rainbow надає набір хмарних комунікаційних сервісів (веб, офісна телефонія, чат і ін.) з високорівневими функціями й можливостями спільної роботи, зручний для розгортання й експлуатації компанією-замовником і її бізнес-партнерами незалежно від уже існуючих у них комунікаційних систем.

Перший реліз платформи, названий Rainbow Essential, уже доступний у формі безкоштовної UCaaS-пропозиції (Unified Communications as a Service – уніфіковані комунікації як сервіс). У нього включені такі функції, як керування контактами, повідомлення про присутність, обмін миттєвими повідомленнями, аудіо- і відеовиклики, демонстрація екрана й загальне використання файлів.

Платформа працює через застосунок, установлюваний на настільних ПК і смартфонах з iOS і Android, доступне після попередньої реєстрації.

Із другого кварталу 2020 р. Rainbow Essential поповниться гібридною опцією для спільного використання з комунікаційними платформами Alcatel-Lucent Enterprise і інших виробників, що працюють на локальних системах. Повідомляється, що інтеграція Rainbow з іншими комунікаційними системами надасть користувачам додаткові можливості, такі як повідомлення про присутність у телефону, одночасне з'єднання з територіально-розподіленими філіями й контроль викликів.

Випуск premium-версії Rainbow запланований на 2020 р. Цей варіант платформи, що будуть поставлятися через мережу бізнес-партнерів ALE, надасть можливості багатобічних конференцій, додаткові сервіси для адміністраторів (наприклад, керування користувачами, резервне копіювання, інтеграція каталогів) і додаткові сервіси інтеграції з офісними АТМ (наприклад, розширений контроль викликів).

ALE працює над створенням відкритих API-інтерфейсів, які дозволять розроблювачам створювати для нової платформи замовлені додатки й додаткові функції. Наприклад, Rainbow дозволить підсилити мобільні банківські додатки функціями чата. Державні

установи або місцеві влади зможуть установлювати миттєві контакти із громадянами, а аеропорти й авіаперевізники зможуть використовувати Rainbow для інформування пасажирів.

На сьогоднішній момент немає чіткого стандарту який вказує роботу протоколів IP-телефонії. Умовно протоколи IP телефонії можна розділити на дві групи: сигнальні й передачі даних. Постараємося розглянути найпоширеніші з них і використовувані, у сьогоднішній час, із практичної сторони питання.

Сигнальні протоколи

SIP (Session Initiation Protocol)

Протокол установлення сеансу зв'язку, перша версія протоколу SIP 1.0 вийшла в 1999 році й була описана в рекомендаціях RFC 2543 організацією IETF. В 2002 році вийшла остаточна рекомендація протоколу SIP 2.0 описана в рекомендації IETF RFC 3261. З тих пор SIP обростав безліччю доповненні й розширень. SIP, будучи клієнт-серверним протоколом, подібно HTTP і SMTP працює на основі послідовних запитів-відповідей. Як і HTTP, SIP реалізований за допомогою текстових тегів – всі SIP-заголовки передаються у вигляді ASCII-тексту, що спрощує його використання в додатках. На даний момент SIP протокол став основним в устаткуванні IP-телефонії, у першу чергу за його лаконічність і простоту.

Додатково існують різновиди даного протоколу для використання його в традиційних мережах загального користування SIP-T (Session Initiation Protocol for Telephones) описаного в RFC3372 і SIP-I (Session Initiation Protocol Internetworking), основне завдання яких є прозора передача ОКС7 (ISUP) повідомлень по IP-мережі.

Протокол H.323

Історично найперший протокол для IP телефонії, розроблений Міжнародним союзом електрозв'язку (ITU) в 1996 році. У свою чергу H.323 охоплює питання передачі голосу, відеоданих через IP-мережі. На сьогоднішній день даний протокол використовується усе рідше й рідше, в основному в старих аналогових АТМ. Недоліком даного протоколу послужила його складність і прихильність до медіа даних у відмінності від SIP.

Skinny (SCCP)

Пропрієтарний протокол для IP телефонії використовуваний компанією Cisco у своєму телекомунікаційному устаткуванні. У якомусь ступені стороннє устаткування Symbol Technologies, IPBlue, SocketIP і Asterisk уміє працювати з даним протоколом.

H.248(MEGACO)

Даний протокол використовуваний між елементами телекомунікаційних мереж: шлюзом (Media Gateway) і контролером шлюзів (Media Gateway Controller). Підтримує різні системи сигналізації мереж з комутацією каналів, включаючи тонову сигналізацію, ISDN, ISUP, QSIG і GSM. Закріплений як стандартний протокол IMS, поряд з SIP і Diameter. Є спадкоємцем протоколу MGCP і використовується в основному мережах провайдеру IMS платформ.

IAX2 (Inter-Asterisk eXchange protocol)

Протокол розроблені для роботи IP-ATM Asterisk. Особливістю даного протоколу є пристосованість до трансляції мережних адрес і подолання NAT голосових пакетів. На відміну від SIP і H.323 використовує тільки один порт 4569 протоколу UDP для сигналізації й медіаданих. Протокол використовується в мережах зі слабкою пропускною здатністю й більше практично не розвивається.

Протоколи передачі даних

RTP (Real-time Transport Protocol)

Протокол, призначений для передачі аудіо й відеопотоків через мережу Інтернет. Описаний в RFC3550 (до це в RFC 1889). Цим же стандартом описується протокол RTCP (Real-time Control Protocol), що призначений для узгодження параметрів Qo між учасниками обміну.

SRTP (Secure Real-time Transport Protocol)

Розширення до протоколу RTP, що забезпечує шифрування, автентифікацію, цілісність і захист від повторів. Опублікований як RFC 3711і використовує порт 5004.

H.323 довгий час утримував лідируючі позиції в сфері відеоконференцзв'язку (ВКЗ). Але останнім часом по статистиці все більшу популярність на ринку набирає протокол **SIP**, що уже підтриманий багатьма великими виробниками, включаючи рішення Polycom і Cisco.

У даному огляді пропонуємо розглянути особливості протоколу SIP і його відмінності від H.323 при реалізації програмного забезпечення для ВКЗ. Постараємося відповістити на головне запитання – якої ж із протоколів більше перспективний для організації відеотрансляцій через Інтернет.

H.323 рекомендований Міжнародним союзом електрозв'язку (ITU-T), що визначає набір стандартів для передачі мультимедіа-даних по мережах з пакетною передачею. Набори рекомендації визначають порядок функціонування абонентських терміналів у мережах з поділюваним ресурсом.

Стандарт H.323 не вимагає обов'язкового використання протоколу IP, однак, більшість реалізацій заснована на цьому протоколі.

SIP (Session Initiation Protocol) – протокол передачі даних, що описує спосіб установлення й завершення користувальницького інтернет-сеансу, що передбачає обмін мультимедійним умістом (відео- і аудіоконференція, миттєві повідомлення, онлайн-ігри). Цей протокол розроблений і стандартизований Internet Engineering Task Force (IETF), силами IETF MMUSIC Working Group в RFC 3261.

Поряд з H.323, SIP відноситься до VoIP. Останнім часом H.323 в IP-телефонії все частіше заміняється протоколом SIP.

За даними звіту www.infonetics.com, ринок глобальних VoIP-послуг для домашнього використання й у бізнесі склав $63 млрд. в 2018 році, що на 9% вище, ніж в 2017 році.

За прогнозом Infonetics, VoIP-ринок у цілому виросте до $82.7 млн. в 2020 році:

Порівняння протоколів SIP і H.323

Обидва протоколи вже досить старі – і той і інший «побачили світло» наприкінці 90-х. H.323 працює на рівні бітових полів, що в ідеальних умовах реалізації (не в Інтернеті) дозволяє заощаджувати мережний трафік у порівнянні з SIP. Однак у сучасних умовах швидкого поширення широкополосного Інтернету ця перевага вже не виглядає настільки значимою. SIP – протокол прикладного рівня, що працює по мережній моделі OSI.

Принципи, закладені в основу протоколу SIP:

– Простота: містить у собі тільки шість методів.

– Незалежність від транспортного рівня: може використовувати UDP, TCP, ATM і т.д.

– Персональна мобільність користувачів. Користувачі можуть переміщатися в межах мережі без обмежень завдяки присвоєнню користувачеві унікального ідентифікатора.

– Масштабованість мережі. Структура мережі на базі протоколу SIP дозволяє легко її розширювати й збільшувати число елементів.

– Розширюваність протоколу. Протокол характеризується можливістю доповнювати його новими функціями з появою нових послуг.

– Інтеграція в стек існуючих протоколів Інтернет. Протокол SIP є частиною глобальної архітектури мультимедіа, розробленої IETF. Ця архітектура також містить у собі протоколи RSVP, RTP, RTSP, SDP.

– Взаємодія з іншими протоколами сигналізації. Протокол SIP може бути використаний разом з іншими протоколами IP-телефонії, протоколами ТфОП і для зв'язку з інтелектуальними мережами.

SIP – протокол, максимально зрозумілий людині, тому розробка й підтримка програмного забезпечення для SIP простіше, ніж H.323. Дані про згадування в Google Trends також підтверджують популярність цього протоколу:

Протокол SIP

SIP розшифровується як Session Initiation Protocol – протокол ініціювання сеансу, це протокол, розроблений IETF для VoIP і для інших сеансів передачі тексту або мультимедіа даних, наприклад, таких як, системи обміну миттєвими повідомленнями, відео, гри в реальному часі й інші сервіси.

Витримка з SIP RFC 3261

Цей документ описує Session Initiation Protocol (SIP), протокол контролю й сигналізації рівня додатка для створення, модифікації, і завершення сеансів з одним або декількома учасниками. Ці сеанси містять у собі: телефонні виклики через Інтернет, презентація мультимедійних даних, і мультимедійні конференції.

При створенні сеансів, використовується SIP запрошення з описом сесії, що дозволяє учасникам підтвердити сумісність використовуваних налаштувань для передачі медіаданих. SIP дає можливість використання таких елементів, як проксі сервер, у функції якого входить допомога в доставці запитів до кінцевого користувача, установка дійсності й розмежування доступу користувачів до різних сервісів, підтримує правила маршрутизацію викликів, що задаються провайдерами, а також підтримує різні можливості, орієнтовані на кінцевих користувачів. Так само в протоколі SIP є механізм реєстрації, що дає можливість користувачам підключатися зі свого поточного місця розташування до сервісів, через проксі сервер. Протокол SIP може використовувати кілька основних протоколів різного транспортного рівня.

SIP дуже схожий на протокол HTTP, використовуваний для Web застосунків, або на SMTP (обмін поштовими повідомленнями). Повідомлення складаються із заголовків і тіла повідомлення. Зміст тіла SIP повідомлення для телефонних викликів описується в SDP: session description protocol – протокол опису сеансу.

SIP – це протокол, що використовує текстові повідомлення, у яких використовується кодування UTF-8.

SIP використовує номер порту 5060, як для комунікації по протоколі UDP, так і для TCP. Для SIP можуть використовуватися інші способи передачі даних.

Протокол SIP пропонує всі, потенційно затребувані можливості, використовувані в Інтернет технологіях, такі як:

- передача викликів або мультимедійних даних;
- конференцзв’язок;
- утримання викликів.

Внаслідок того, що SIP – це досить гнучкий протокол, є можливість розширення його можливостей зі збереженням зворотної сумісності.

Також, протокол SIP може переборювати обмеження, пов'язані з використанням NAT або файрволів. (Зверніть увагу на розділ: NAT and VoIP).

Протокол SDP (протокол опису сеансу)

Протокол SDP описує параметри мультимедіа сеансу зв'язку й використовується для оголошення типу й параметрів сесії, у запрошенні до початку сеансу зв'язку, і в інших мультимедійних сеансах, при установки зв'язку й узгодженні параметрів. SDP використовується в таких протоколах сигналізації VoIP, як SIP, H.323 і в інші, менш відомих протоколах VoIP, для передачі інформації про налаштування потоку передачі мультимедіа даних від клієнта A до клієнта B.

Протокол SDP використовується в SAP – Протокол анонса сервісів (Service Announcement Protocol).

Протокол SDP використовується в SIP.

IETF RFC:

- RFC2327: Протокол Опису Сеансу (SDP).
- RFC3264: Модель обробки Запиту/Відповіді для Протокол Опису Сеансу (SDP).
- RFC3388: Групування рядків з описом медіаданих у протоколі опису сеансу (SDP).

– RFC3266: Підтримка IPv6 у Протоколі Опису Сеансу (SDP)
– Параметри SDP IANA: http://www.iana.org/assignments/ sdp-parameters

Поля, використовувані в протоколі

Необов'язкові елементи відзначені символом '*'.

Опис сеансу

v= (версія протоколу)
o= (ідентифікатори творця/власника й сесії)
s= (ім'я сесії)
i=* (інформація про сесію)
u=* (URI опису)
e=* (email адреса)
p=* (номер телефону)
c=* (інформація для з'єднання – не потрібно, якщо є в описі всіх медіаданих)
b=* (інформація про займану смугу пропущення каналу зв'язку)
Одна й більше рядків з описом параметрів часу (Дивися нижче)
z=* (установка для тимчасової зони)
k=* (ключ шифрування)
a=* (одна або кілька рядків з описом атрибутів сесії)
Від нуля й більше описів, даних передачі мультимедіа

Опис параметрів часу

t= (час активності сеансу)
r=* (число спроб повторів, від нуля й більше)

Опис дані передачі мультимедіа

m= (назва медіаданих і адреса їхньої передачі)
i=* (заголовок медіаданих)
c=* (інформація для з'єднання – не обов'язково, якщо описано в параметрах сеансу)
b=* (інформація про займану смугу пропущення каналу зв'язку)
k=* (ключ шифрування)
a=* (від нуля й більше рядків з описом атрибутів медіаданих)

Принципи протоколу SIP

Протокол ініціювання сеансів – Session Initiation Protocol (SIP) є протоколом прикладного рівня й призначається для організації, модифікації й завершення сеансів зв'язку: мультимедійних конференцій, телефонних з'єднань і розподілу мультимедійної інформації. Користувачі можуть брати участь в існуючих сеансах зв'язку, запрошувати інших користувачів і бути запрошеними ними до нового сеансу зв'язку. Запрошення можуть бути адресовані певному користувачеві, групі користувачів або всіх користувачів.

Протокол SIP розроблений групою MMUSIC (Multiparty Multimedia Session Control) комітету IETF (Internet Engineering Task Force), а специфікації протоколу представлені в документі RFC 2543]. В основу протоколу робоча група MMUSIC заклала наступні принципи:

– Персональна мобільність користувачів. Користувачі можуть переміщатися без обмежень у межах мережі, тому послуги зв'язки повинні надаватися їм у будь-якому місці цієї мережі. Користувачеві привласнюється унікальний ідентифікатор, а мережа надає йому послуги зв'язку поза залежністю від того, де він перебуває. Для цього користувач за допомогою спеціального повідомлення – **REGISTER** – інформує про свої переміщення сервер визначення місця розташування/сервер реєстрацій.

– Масштабованість мережі. Вона характеризується, у першу чергу, можливістю збільшення кількості елементів мережі при її розширенні. Серверна структура мережі, побудованої на базі протоколу SIP, повною мірою відповідає цій вимозі.

– Розширюваність протоколу. Вона характеризується можливістю доповнення протоколу новими функціями при введенні нових послуг і його адаптації до роботи з різними додатками.

Як приклад можна привести ситуацію, коли протокол SIP використовується для встановлення з'єднання між шлюзами, взаємодіючими із ТфОП за допомогою сигналізації ОКС7 або DSS1.

У цей час SIP не підтримує прозору передачу сигнальної інформації телефонних систем сигналізації. Внаслідок цього додаткові послуги ISDN виявляються недоступними для користувачів IP-мереж.

Розширення функцій протоколу SIP може бути зроблене за рахунок введення нових заголовків повідомлень, які повинні бути зареєстровані у вже згадуваній раніше організації IANA. При цьому, якщо SIP, сервер приймає повідомлення з невідомими йому полями, то він просто ігнорує їх і обробляє лише ті поля, які він знає.

Для розширення можливостей протоколу SIP можуть бути також додані й нові типи повідомлень.

Інтеграція в стек існуючих протоколів Інтернет, розроблених IETF. Протокол SIP є частиною глобальної архітектури мультимедіа, розробленої комітетом Internet Engineering Task Force IETF. Ця архітектура містить у собі також протокол резервування ресурсів (Resource Reservation Protocol – RSVP, RFC 2205), транспортний протокол реального часу (Real,Time Transport Pro,tocol – RTP, RFC 1889), протокол передачі потокової інформації в реальному часі (Real,Time Streaming Protocol – RTSP, RFC 2326), протокол опису параметрів зв'язку (Session Description Protocol – SDP, RFC 2327). Однак функції протоколу SIP не залежать від жодного із цих протоколів.

Взаємодія з іншими протоколами сигналізації. Протокол SIP може бути використаний разом із протоколом H.323. Можливо також взаємодія протоколу SIP із системами сигналізації ТфОП – DSS1 і ОКС7. Для спрощення такої взаємодії сигнальні повідомлення протоколу SIP можуть переносити не тільки специфічна SIP адреса, але й телефонний номер формату E.164 або будь-якого іншого формату. Крім того, протокол SIP, нарівні із протоколами H.323 і ISUP/IP, може застосовуватися для синхронізації роботи пристроїв керування шлюзами; у цьому випадку він повинен взаємодіяти із протоколом MGCP. Іншою важливою особливістю протоколу SIP є те, що він пристосований до організації доступу користувачів мереж IP телефонії до послуг інтелектуальних мереж, і існує думка, що саме цей протокол стане основним при організації зв'язку між зазначеними мережами.

Методи SIP протоколу, певні в SIP RFC

У протоколі SIP визначено кілька методів, використовуваних при комунікації.

- метод SIP: invite : Запрошення іншого UA (учасника) почати сеанс;
- метод SIP: re-invite: Зміна параметрів запущеного сеансу;
- метод SIP: register: Зареєструвати своє місце розташування в мережі, використовуючи SIP сервер реєстрації;
- метод SIP: ack: Використовується для підтвердження прийому повідомлень INVITE при їхньому обміні;
- метод SIP: cancel: Скасування запрошення про початок сеансу;
- метод SIP: bye: Завершення сеансу зв'язку;
- метод SIP: options.

Розширені методи SIP протоколу з інших RFC:

- SIP method info: Розширення протоколу, описане в RFC 2976.
- SIP method notify: Розширення протоколу, описане в RFC 2848 PINT.
- SIP method subscribe: Розширення протоколу, описане в RFC 2848 PINT.
- SIP method unsubscribe: Розширення протоколу, описане в RFC 2848 PINT.
- SIP method update: Розширення протоколу, описане в RFC 3311.
- SIP method message: Розширення протоколу, описане в RFC 3428.
- SIP method refer: Розширення протоколу, описане в RFC 3515.
- SIP method prack: Розширення протоколу, описане в RFC 3262.
- SIP Specific Event Notification: Розширення протоколу, описане в RFC 3265.

– SIP Message Waiting Indication: Розширення протоколу, описане в RFC 3842.
– SIP method PUBLISH: Розширення протоколу, описане в RFC 3903.

Відповіді на SIP повідомлення

Після прийому й інтерпретації запиту, адресат (проксі сервер) передає відповідь на цей запит. Зміст відповідей буває різним:

підтвердження встановлення з'єднання, передача запитаної інформації, відомості про несправності й т.д.

Структуру відповідей і їхні види протокол SIP успадкував від протоколу HTTP.

Визначено шість типів відповідей, що несуть різне функціональне навантаження. Тип відповіді кодується тризначним числом. Найважливішої є перша цифра, що визначає клас відповіді, інші дві цифри лише доповнюють першу. У деяких випадках устаткування навіть може не знати все коди відповідей, але воно обов'язково повинне інтерпретувати першу цифру відповіді.

Терміни й визначення, специфічні для SIP

– Користувальницькі термінали/агенти.
– SIP outbound proxy.
– SIP proxy: SIP проксі сервер.
– SIP redirect server: SIP сервер переадресації.
– SIP registrar server SIP сервер визначення місця розташування користувачів/сервер обробки реєстрацій.
– SIP URI – як визначити з'єднання SIP, в URL.
– SIP Compression: Компресія в SIP протоколі.
– SIP DMTF Signalling: Передача DTMF сигналів, використовуючи SIP протокол.
– SIP Authentication: Авторизація в SIP протоколі.

Чи можна за допомогою SIP повністю замінити H.323?

Так, і навіть більш ніж! На кожне розширення H.323 є розширення SIP. Session Initiation Protocol більше гнучкий у цьому плані (наприклад, при додаванні нового поля, якщо хтось його не розуміє, воно просто ігнорується). Серйозні апаратні рішення підтримують і те, і інше.

По великому рахунку H.323 і SIP функціонально рівнозначні для розробки ВКЗ рішень.

Але перехід до SIP не є панацеєю від проблем несумісності між рішеннями декількох виробників (при функціональних доробках). Ця проблема властива будь-якому протоколу на ринку ВКЗ, включаючи й H.323.

Виробники не особливо зацікавлені в сумісності пропрієтарних розширень. Вони не можуть дозволити собі бути повністю несумісними, але намагаються обмежити сумісність по максимуму – гарним прикладом є Microsoft Lync – SIP з'єднання обмежені до CIF при набагато більших теоретичних можливостях.

Також одним з найважливіших моментів є забезпечення безпеки переданих даних. Питанням безпеки використання протоколу SIP присвячений один з розділів RFC 3261. Шифрування сигнального трафіку можливо на транспортному рівні через TLS. Крім того, розроблений стандарт SIPS, що накладає додаткові угоди по безпечній передачі даних за допомогою SIP. Для шифрування мультимедійного контенту застосовується протокол SRTP.

За рахунок більше простої реалізації, у порівнянні з H.323, SIP-зв'язок став популярною VoIP-послугою, надаваною багатьма постачальниками послуг Інтернет-телефонії, що підключає УАТМ до телефонної мережі загального користування (ТфОП) через Інтернет.

Розробка структурної схеми

Хмарна АТМ на базі ALE Rainbow – це рішення для оптимізації й розширення можливостей офісної телефонної мережі.

Хмарна АТМ на базі ALE Rainbow працює на базі устаткування оператора зв'язку, і не має на увазі придбання Клієнтом дорогої офісної АТМ на базі ALE Rainbow.

Хмарна АТМ на базі ALE Rainbow– це послуга для компаній, що заміняє офісну міні АТМ на базі ALE Rainbow і навіть колл-центр. Віртуальна IP АТМ на базі ALE Rainbow надає такі можливості, як багатоканальний номер, запис розмов, голосові вітання, переклад виклику – все це й багато чого іншого доступно через Інтернет без придбання офісної АТМ на базі ALE Rainbow.

Суть послуги в тому, що автоматична телефонна станція фізично розміщається в провайдеру, а клієнт одержує доступ через VoIP і засобу вилученого керування. Власники одержують можливість використовувати всю функціональність сучасної IP-АТМ на базі ALE Rainbow без витрат на інфраструктуру.

Перше, із чого починається віртуальна IP АТМ на базі ALE Rainbow – багатоканальний телефонний номер. Це може бути номер. При дзвінку на нього абонент почує голосове вітання компанії клієнта. Голосове вітання краще записати за допомогою професійного диктора – це створить правильне відчуття солідності компанії.

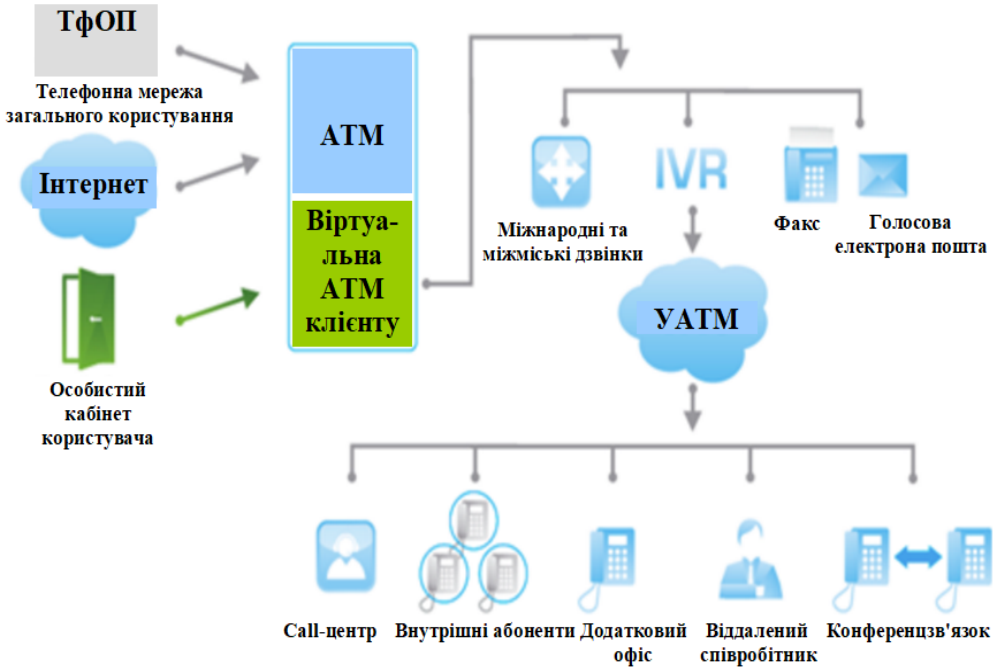


Рисунок 1 – Структурна схема системи

Потім у справу вступає сценарій IVR. Це та сама система, що пропонує нам «набрати внутрішній номер абонента, цифру один для з'єднання з технічною підтримкою..» Для чого це потрібно? Справа в тому, що при великому потоці дзвінків від клієнтів IVR меню вивільняє значну частину часу співробітників, що раніше йшло на переключення дзвінків вручну. Крім того, IVR-сценарій може надати стандартну інформацію в автоматичному режимі (наприклад, адресу й годинники роботи).

Якщо співробітникові прийшов вхідний виклик, а його немає на робочому місці – відбувається переадресація на мобільний. Можна задати кілька номерів телефону, по яких хмарна АТМ на базі ALE Rainbow намагається додзвонитися співробітникові.

Телефонія через Інтернет протокол (IP), також відома як VoIP телефонія, являє собою технологію, що дозволяє використовувати Інтернет для телефонного зв'язку. Сьогодні популярність IP-телефонії у світі бурхливо росте, оскільки переваги нових технологій дають компаніям важливі нові можливості.

Так само доступні послуги: Голосова пошта, запис розмов, телефонна конференція.

Основні переваги послуги:

– Висока швидкість організації телефонії для підприємства.

– Відсутність капітальних витрат в інфраструктуру.

– Відсутність витрат на зміст устаткування й обслуговуючий персонал.

– Гнучкість системи (можливий перенос телефонних номерів, для цього досить підключити устаткування до УАТМ або змінити переналаштування в особистому кабінеті).

– Керування послугою через Особистий кабінет (включення й вимикання додаткових функцій відбувається через особистий кабінет, для керування послугою немає необхідності приходити в офіс оператора, всі налаштування застосовуються автоматично після активації додаткової функції в особистому кабінеті).

Цільові аудиторії

Start UP

Кількість співробітників до 15 чоловік.

Вигоди:

– підвищення «доступності» компанії для клієнта;

– можливість аналізу ефективності реклами;

– можливість аналізу ефективності відділу продажів;

– підвищення «сприйманого» статусу компанії;

– можливість для значного підвищення ефективності бізнесу за рахунок високої керованості.

SMB (Малий і середній бізнес)

Кількість співробітників від 15 чоловік до 250 чоловік.

Вигоди:

– підвищення «доступності» компанії для клієнта;

– можливість аналізу ефективності реклами;

– можливість аналізу ефективності відділу продажів;

– підвищення «сприйманого» статусу компанії;

– зниження щомісячних витрат на місцевий телефонний зв'язок;

– зниження щомісячних витрат на міжміський і міжнародний зв'язок;

– можливість для значного підвищення ефективності бізнесу за рахунок високої керованості.

Територіально розподілені компанії

Кількість співробітників від 50 чоловік.

Вигоди:

– підвищення «доступності» компанії для клієнта;

– можливість аналізу ефективності реклами;

– можливість аналізу ефективності відділу продажів;

– підвищення «сприйманого» статусу компанії;

– зниження щомісячних витрат на місцевий телефонний зв'язок;

– зниження щомісячних витрат на міжміський і міжнародний зв'язок;

– можливість об'єднання в одну інфраструктуру териториально-розподілених офісів;

– можливість гнучкого керування викликами;

– можливість для значного підвищення ефективності бізнесу за рахунок високої керованості.

Сучасний світ розвивається стрімкими темпами. Усе більше комп'ютерних технологій входять у наше життя й міцно там обґрунтовуються. Не є виключенням і бізнес середовище.

Хмарні сховища, хмарна CRM, мобільні додатки, які полегшують нам життя. А тепер ще й хмарна телефонія або хмарна АТМ на базі ALE Rainbow. Якщо раніше при слові офісна телефонія ми уявляли собі такі величезні телефонні апарати з безліччю кнопок і функцій, то тепер таке слово усе більше асоціюється із графічним інтерфейсом програми, що управляє

всіма вашими дзвінками в офісі. А звичний телефонний апарат усе більше заміняє гарнітура, підключена до офісного комп'ютера.

Чим же гарна така система, і які перевазі ви одержуєте, використовуючи її?

Показник надійної й великої інтернаціональної компанії

Ви більша компанія, у вас багато співробітників по усьому світі, і багато філій? Тоді вам просто необхідна хмарна АТМ на базі ALE Rainbow. Ви зможете придбати й завести на неї телефонні міські номери із усього світу, а також розподілити ці номери по філіях. Наявність міжнародних телефонних номерів буде викликати довіру у ваших потенційних клієнтів і партнерів. Партнери будуть дзвонити вам по тим номерам, які будуть зручні їм. Й вони завжди будуть знати, що з вами легко зв'язатися по-місцевому.

Ефективна корпоративна телефонна мережа

Хмарна АТМ на базі ALE Rainbow дозволяє створювати єдину корпоративну телефонну мережу для великої компанії з філіями в різних країнах. Ви зможете організувати ефективну зовнішню й внутрішню нумерацію для зручності ваших працівників. Всі дзвінки будуть записуватися в загальну базу, і ви зможете аналізувати їх виходячи з необхідних вам параметрів.

Хмарна АТМ на базі ALE Rainbow разом із системою керування клієнтами (CRM) дозволить вам створювати картки клієнтів, які будуть спливати при дзвінках. Це дуже ефективний інструмент, що дозволяє вашим менеджерам відразу бачити, хто вам дзвонить, і далі визначати як працювати з таким клієнтом.

Економія на телефонному устаткуванні

Усе, що вам потрібно для функціонування вашої корпоративної телефонної мережі – це стійкий Інтернет. Вам не потрібно тягти дорогі телефонні лінії зв'язку, вам не потрібно ставити в себе в офісі дороге устаткування для організації АТМ на базі ALE Rainbow, вам навіть не потрібні телефонні апарати як такі або покупка безлічі корпоративних сім-карт: для прийому й здійснення вихідних дзвінків вам буде досить комп'ютера й гарнітури.

Вам взагалі не потрібно платити за установку й налагодження хмарної АТМ на базі ALE Rainbow. Так само як і за фізичні сервера й ліцензії. Всі ці можливості ви одержуєте разом з орендою віртуального телефонного номера й хмарної АТМ на базі ALE Rainbow. Ви платите тільки за використання цієї системи, а фахівці компанії-провайдери роблять за вас всі необхідні налаштування.

Незалежність від географічного місця розташування

Один раз підключившись до віртуального АТМ на базі ALE Rainbow ви назавжди звільняєтеся від необхідності зміни налаштувань, номера й так далі при переїзді або географічному розширенні вашої компанії. Ваша компанія, всі ваші філії й співробітники можуть перебувати в різних куточках планети – ваші клієнти й партнери навіть не помітять цього.

Хмарна АТМ на базі ALE Rainbow з віртуальними міськими телефонними номерами – ваш простий і швидкий старт у великий міжнародний бізнес. Це набагато дешевше й ефективніше, ніж участь у міжнародних галузевих виставках.

Купите віртуальний телефонний номер прямо сьогодні й використовуйте всю перевагу сучасної телефонії й віртуальної АТМ на базі ALE Rainbow.

Можливості віртуальних АТМ на базі ALE Rainbow

До хмарних сервісів можна підключати зовсім будь-яких операторів зв'язку з будь-яких міст. Також віртуальне рішення дозволяє одночасно працювати з декількома операторами й декількома номерами.

Якщо в офісі або компанії є які-небудь філії, де встановлені фізичні телефонні станції, то вони можуть бути легко підключені до хмарного сервісу зв'язку. Це дозволить об'єднати філії й головний офіс у єдину номерну ємність. Результат – безкоштовні корпоративні дзвінки для всіх.

За допомогою хмарної віртуальної системи зв'язку можна повністю безкоштовно здійснювати дзвінки користувачам Skype або Microsoft Office365. Це відмінна можливість заощадити засоби.

Сучасне рішення для зв'язку на базі хмарних технологій не дасть пропустити важливих дзвінків. Часто трапляється так, що немає можливості прийняти терміновий дзвінок на комп'ютері. Система Microsoft Lync без праці виконати переадресацію дзвінка на смартфон або ж на сервіс голосової пошти. Це дуже зручно – тепер можна не хвилюватися через пропущені дзвінки.

Для тих, хто часто їздить у відрядження хмарна АТМ також пропонує широкі можливості. Перебуваючи в іншому місті, країні, навіть на іншому континенті досить запустити застосунок на смартфоні й безкоштовно робити дзвінки по міським або ж мобільних номерах. При цьому буде використаний міський номер, до якого підключена телефонна станція.

Можливість використання IP-ТЕЛЕФОНІВ

Для тих, хто звик використовувати традиційні класичні телефонні апарати, пропонуємо різноманітні асортименти самих різних IP-апаратів. Серед брендів – самі передові й відомі виробники, такі як Polycom, Snom, HP, AudioCodes і інші.

Для того, щоб можна було здійснювати дзвінки за допомогою IP-телефонів, досить тільки доступу до інтернету.

Мобільні пристрої

Поза офісом, щоб залишатися завжди на зв'язку, можна використовувати мобільні пристрої. Смартфони, планшети будь-яких виробників і марок відмінно підійдуть для прийому й здійснення дзвінків.

Мобільний пристрій, що обслуговує віртуальна АТМ, має всі ті можливості й функції, що й клієнт на комп'ютері. Можна використовувати функції дзвінків, відеоконференцій, відправляти повідомлення, синхронізувати контакти.

Якщо довелося вийти за межі офісу, але незабаром важливий дзвінок, то хмарний сервіс для зв'язку дозволяє завгодно налаштовувати параметри переадресації вхідних дзвінків. Також з мобільного можна прослухати голосову пошту.

Якщо поруч немає надійного й швидкого інтернету, то можна скористатися функцією Call Back. Досить набрати потрібний номер і хмарний сервіс передзвонить і з'єднає з потрібним абонентом.

Комунікації для комп'ютерів і ноутбуків

При участі в різного роду конференціях може знадобитися демонстрація робочого стола аудиторії. Ці функції також доступні в хмарному сервісі. Можна демонструвати весь простір робочого стола, окремі додатки. Також є можливість передачі керування іншим учасникам.

Для того, щоб почати використовувати сервіс, досить тільки гарнітури або веб-камери. Із цими простими інструментами можна відразу ж почати робити або приймати будь-які виклики від різних абонентів на будь-які пристрої й всілякі телефонні номери в будь-якій крапці земної кулі.

Відеоконференції

Відеоконференцзв’язок також використовується бізнесом. Наша компанія пропонує широкі можливості й самий різноманітний асортименти устаткування для організації комфортних і зручних у використанні переговірних кімнат. Можна придбати камери 360°, спікерфони й багато чого іншого. Все устаткування найвідоміших торговельних марок.

Хмарна віртуальна АТМ дозволяє приєднати до конференції до 255 учасників. При цьому якість зв'язку буде на висоті. Співробітники можуть приєднатися до конференції прямо з робочого стола комп'ютера або зі смартфону або планшета.

Зовнішні абоненти, які не підключені до цього хмарного сервісу, можуть підключатися до конференції безкоштовно. Для підключення необхідний браузер на ПК, звичайний телефон або смартфон.

Переваги рішень на базі хмарних технологій

Крім зручного й надійного сервісу для комунікацій клієнти одержують масу додаткових послуг:

– Інтеграція й підключення будь-яких АТМ на базі ALE Rainbow і ТфОП – будь-який оператор буде підключений або інтегрований з АТМ на базі ALE Rainbow.

– Адміністрування – немає ніякої необхідності вивчати систему й принцип дії, по якому працює IP-телефонія. Кваліфіковані фахівці будуть самостійно виконувати адміністрування.

– Можливість безкоштовної інтеграції хмарних сервісів зі службою каталогів – це спрощує підключення користувачів до сервісу.

Це віртуальне рішення для зв'язку підійде для будь-яких компаній. Так, це може бути малий, середній або великий бізнес. Ми надаємо якісні послуги поза залежністю від кількості абонентів – це може бути 10 співробітників у невеликому офісі або ж кілька тисяч чоловік.

Висновок. У статті розглянуто та проаналізовано програмне забезпечення, призначено для системи комунікаційної платформи як сервісу на базі ALE Rainbow. В межах України в недостатній мірі представлені вітчизняні розробки в цій області. У роботі наведені теоретичне узагальнення й рішення наукового завдання дослідження методів комунікаційної платформи як сервісу на базі ALE Rainbow. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем комунікаційної платформи як сервісу на базі ALE Rainbow; Досліджена система комунікаційної платформи як сервісу на базі ALE Rainbow; На основі отриманих результатів досліджень створена програмна реалізація системи комунікаційної платформи як сервісу на базі ALE Rainbow. Розроблені під час виконання роботи алгоритми дозволяють успішно вирішувати завдання комунікаційної платформи як сервісу на базі ALE Rainbow. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки. Розроблене програмне забезпечення має простий, дружній та зручний інтерфейс користувача, що забезпечує легкість у освоєнні роботи програмного продукту, зручність у використанні, і не потребує особливих спеціальних знань. При створені програмного забезпечення було використано об’єктно-орієнтований підхід, що відповідає сучасним тенденціям у галузі розробки комерційних програмних систем. Програма реалізована на мові високого рівня Delphi 10.2. Дана мова програмування дозволяє найбільш ефективно обробляти дані. Це дозволило мінімізувати строк розробки програмного забезпечення, і, як слід, зменшити витрати на його розробку. Запропоноване програмне забезпечення ділиться на загальне програмне забезпечення, що поставляється із засобами обчислювальної техніки й спеціальне програмне забезпечення, що спеціально розроблене для даної конкретної системи й включає програми, що реалізують її функції. Для підвищення рівня безпеки запропоновано застосовувати алгоритм Lucifer. В цілому створене програмне забезпечення підтверджує правильність використаних проектних рішень та повністю відповідає вимогам технічного завдання. Створене програмне забезпечення має потенційну можливість для подальшого вдосконалення і застосування у різних галузях.

Список літератури

1. Босько В.В. Анализ и сравнительное исследование перспективных направлений развития цифровых телекоммуникационных систем и сетей / Смирнов А.А., Босько В.В., Мелешко Е.В. // Системи обробки інформації. – Х.: ХУ ПС, 2008. – Вип.7(74). – С.120-123.
2. Босько В.В. Разработка методики оценки среднего времени обслуживания информационных пакетов в телекоммуникационной сети / Смирнов А.А., Босько В.В., Мелешко Е.В. // Системи управління, навігації та зв’язку. – Київ: ДП «Центральний науково-дослідний інститут навігації і управління», 2009. – Вип. 2(10). – С.162-165.
3. Босько В.В. Разработка математической модели процесса динамического управления маршрутизацией данных в телекоммуникационной сети / Смирнов А.А., Босько В.В. // Системи управління, навігації та зв’язку. – К.: ДП «ЦНДІ навігації і управління», 2009. – Вип. 3(11). – С.208-210.

4. Босько В.В. Разработка метода определения оптимального множества путей передачи информации в телекоммуникационной сети / Смирнов А.А., Босько В.В. // Збірник наукових праць. – Х.: ХУПС, 2009. – Вип. 3(21). – С.102-108.
5. В.В. Босько. Разработка метода прогнозирования поведения информационного потока в телекоммуникационной сети // Збірник наукових праць. Харківського університету Повітряних Сил: – Х.:ХУ ПС, – 2010.-Вип. 3 (25) .- С.126-130.
6. Босько В.В. Исследование особенностей построения современных телекоммуникационных систем и сетей / Смирнов А.А., Босько В.В. // Проблемы информатики и моделирования. Материалы восьмой международной научно-технической конференции 26-28 ноября. – Х.: НТУ "ХПИ", 2008. – С.54.
7. Босько В.В. Исследование влияния времени мониторинга телекоммуникационной сети на точность прогнозирования поведения трафика / Смирнов А.А., Босько В.В. // Перша міжнародна науково-практична конференція "Проблеми й перспективи розвитку IT-індустрії" м. Харків , 18-19 листопада 2009р. – С.198-200.
8. Босько В.В. Анализ математических моделей телекоммуникационной сети / Смирнов А.А., Босько В.В. // Проблемы информатики и моделирования. Материалы девятой международной научно-технической конференции 26-28 ноября. – Х.: НТУ "ХПИ", 2009. – С.52-53.
9. Босько В.В. Метод повышения оперативности передачи данных в телекоммуникационной сети / Смирнов А.А., Босько В.В. // Збірник тез доповідей науково-практичної конференції "Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку" 24-25 березня. – Х.: АВВ МВС України, 2010. – С.54.
10. Босько В.В. Динамическое управление процессом маршрутизации данных в телекоммуникационной сети / Смирнов А.А., Босько В.В. // Тези доповідей Міжнародної науково-практичної конференції м. Вінниця, Україна 19-21 травня 2010 року. – Вінниця: ВНТУ, 2010. – С.231-232.

УДК 004

Д. Друмашко, магістр гр. КН-18МЗ-1,4
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ РОЗРОБКИ ІНДИВІДУАЛЬНОГО ПРОЕКТУ ЦЕНТРІВ ОБРОБКИ ДАНИХ З ЗАСТОСУВАННЯМ ТЕХНОЛОГІЙ КАСТОМІЗАЦІЇ

У статті розроблено програмне забезпечення, яке призначено для системи розробки індивідуального проекту центрів обробки даних з застосуванням технологій кастомізації. Метою розробки є дослідження та програмна реалізація системи розробки індивідуального проекту центрів обробки даних з застосуванням технологій кастомізації. Об'єктом дослідження є процес розробки індивідуального проекту центрів обробки даних з застосуванням технологій кастомізації. Предметом дослідження є методи розробки індивідуального проекту центрів обробки даних з застосуванням технологій кастомізації. Методи дослідження базуються на методах теорії побудови телекомунікаційних мереж, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи розробки індивідуального проекту центрів обробки даних з застосуванням технологій кастомізації. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення. Розроблено зручний інтерфейс користувача. Наведені інструкції по роботі з програмними засобами.

комп'ютерні науки, центр обробки даних, кастомізація

Постановка проблеми. Поняття «кастомізація» має безліч різних визначень. От одне з них, на мій погляд, найбільш точне: «Кастомізація – це індивідуалізація продукції під замовлення конкретних споживачів шляхом внесення конструктивних або дизайнерських змін».

Важливе завдання кастомізації – створити в споживача впевненість у тому, що робота робиться саме для нього й націлена на задоволення його конкретних потреб. Ряд експертів

уважають кастомізацію чи не ідеалом взаємодії постачальника й споживача. Вона залучає не тільки своєю етичною спрямованістю, але й можливістю одержувати фінансову вигоду, адже завдяки більше високій цінності кастомізованого рішення клієнт одержує конкурентну перевагу.

Найчастіше кастомізацію сприймають як досить дорогу процедуру. До того ж існує думка, що індивідуалізацію продукції можуть дозволити собі далеко не всі, оскільки її вартість виявляється занадто високою. Хтось також уважає, що сама по собі дана «послуга» покликана лише створювати видимість додання більшої цінності для замовника, у той час як її першочергова функція – одержання максимального прибутку виробником. Але чи не так це насправді?

В умовах твердої конкуренції ринок насичений схожими продуктами, але в той же самий час кожний з них має унікальні характеристики. При виборі того або іншого рішення замовник намагається знайти оптимальне, максимально відповідним його потребам. Серед критеріїв вибору часто зустрічаються такі, як технологічність, якість, строки поставок і, безсумнівно, вартість. Крім цього, ураховуються також прихильність певній торговельній марці, її популярність, вдалий досвід впровадження й інші фактори. Часто в результаті доводиться робити вибір між пошуком оптимального рішення серед, умовно, стандартизованих продуктів і створенням унікального, зробленого для рішення конкретного завдання й маючого максимальний ККД.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи розробки індивідуального проекту центрів обробки даних з застосуванням технологій кастомізації.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи розробки індивідуального проекту центрів обробки даних з застосуванням технологій кастомізації.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем розробки індивідуального проекту центрів обробки даних з застосуванням технологій кастомізації.

– Дослідження системи розробки індивідуального проекту центрів обробки даних з застосуванням технологій кастомізації.

– Програмна реалізація системи розробки індивідуального проекту центрів обробки даних з застосуванням технологій кастомізації.

Об'єктом дослідження є процес розробки індивідуального проекту центрів обробки даних з застосуванням технологій кастомізації.

Предметом дослідження є методи розробки індивідуального проекту центрів обробки даних з застосуванням технологій кастомізації.

Методи дослідження базуються на методах теорії побудови телекомунікаційних мереж, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Етапи кастомізації

По своїй суті модель життєвого циклу процесу кастомізації є каскадною з можливістю ітеративного повторення деяких етапів.

На першому етапі формується загальне подання про продукт, його основних функціях і розв'язуваних з його допомогою завданнях, складається технічне завдання, що, за суттю, є якимось сигналом про завершення одного етапу й переході до наступного. Дуже важливо одержати максимум інформації й зафіксувати її у вихідних документах.

Варто враховувати, що далеко не всі побажання зацікавлених осіб у формуванні завдання можуть бути відображені у фінальній версії ТЗ, особливо при комплексному підході. Деякі пропозиції можуть суперечити один одному, а інші й зовсім виявитися неспроможними. Однак не варто відразу ж відмітати ідеї, які, на перший погляд, можуть здаватися марними.

На другому етапі здійснюється проектування продукту. Залежно від його типу це можуть бути креслення, ескізи, технічні карти, алгоритми роботи, програмний код і інші дані й документи, необхідні для виробництва прототипу продукції, його приймання й запуску в досвідчену експлуатацію.

Стадія прототипування є ключовою в життєвому циклі кастомізованого продукту: під час даного етапу виготовляється досвідчений зразок для проведення попередніх і експлуатаційних випробувань. При цьому допускається відсутність у прототипі деяких вузлів, частин і елементів, які відповідно до рішення відповідальних осіб є другорядними. Як приклад можна привести ситуацію, коли на момент випробувань несучої здатності рами шафи конструктив не піддається фарбуванню. Як правило, на даному етапі калькулюється остаточна вартість виробництва одиниці продукції. Отримані дані дають можливість оцінити не тільки технічні, але й цінові характеристики продукту й ухвалити рішення щодо доцільності його подальшої розробки.

Якщо на основі сукупних даних приймається рішення про продовження процесу кастомізації, розробка продукції переходить на наступний етап – внесення змін і виправлень. Всі конструктивні й технологічні моменти, що не відповідають вимогам ТЗ, повинні бути виправлені. При виявленні службою експлуатації якихось недоробок теж доводиться вносити зміни в даний продукт.

Етапи проектування, прототипування й внесення змін можуть повторюватися кілька разів, поки не буде досягнутий результат, що задовольняє всі вимоги замовника. Виходячи з досвіду реалізації подібних проектів, можна сказати, що число циклів звичайно становить один або два й практично ніколи не перевищує трьох.

Остання стадія життєвого циклу кастомізованого продукту – його виготовлення. Причому однієї з основних завдань є аж ніяк не складання плану-графіка й вибудовування логістики поставок готової продукції, а забезпечення можливості виробництва погодженого обсягу в позначений термін. Найчастіше індивідуальним продуктам, зробленим по приватних вимогах, можуть вимагатися спеціальні аксесуари або навіть технологічні вузли, які необхідно вивчити, вписати в конструкцію й забезпечити їхню наявність на момент складання кінцевого продукту.

Ринок кастомізованих рішень перестає бути привілеєм великих компаній і поступово здобуває масовий характер. Безсумнівно, амбіційні й зухвалі розробки, а також високотехнологічні рішення, як і колись, будуть превалювати в масштабних проектах, однак згодом всі вони можуть тією чи іншою мірою стати загальнодоступними. Не слід забувати, що багато стандартизованих рішень, перш ніж стати такими, пройшли через стадію кастомізованого продукту.

Ріст хмарних обчислень, високошвидкісний широкополосний доступ і поштовх до цифрових перетворень популяризували використання програмного забезпечення як сервісу (Software as a Service; SaaS). Ця зростаюча централізована модель поширення й ліцензування ПЗ викликає усе більше тривоги в IT-менеджерів, стурбованих безпекою й доступністю своїх дата-центрів.

Як правило, двадцять років – це не так багато, але у світі технологій – це ціла епоха. Так само було й два десятиліття назад, коли підприємства спілкувалися за допомогою ручки й паперу, оплата відбувалася за допомогою банківських чеків, і якщо треба було організувати особисту зустріч із клієнтом, приходилось чекати тиждень.

З тих пор світ бізнесу й технологій пройшов довгий шлях. Електронна пошта стала стандартом спілкування, системи керування взаєминами із клієнтами (Customer Relationship Management; CRM) стали нормою, і тепер, за допомогою могутніших інструментів, таких як чат, автоматизація бізнесу й створення бази потенційних клієнтів, ми можемо зробити більше, ніж коли-або колись.

От три аспекти, на які необхідно звернути увагу при виборі нового дата-центру.

Довіра своєму провайдеру дата-центру в критичній ситуації

З перших днів розвитку ЦОДів, компаніям, які вибирають віддалене зберігання даних, доводиться фізично відвідувати місця розташування серверів, набудовувати кожний сервер, установлювати їх у стійку й одержувати дозвіл від клієнта перш, ніж запускати систему.

Це був трудомісткий і тривалий процес, що приводив до повної зупинки, якщо щось ішло не так. Була мінімальна надмірність, низька доступність, і користувач часто відповідав за періодичне обслуговування, установку патчей і відновлень. Так чи інакше, це як і раніше дешевше, ніж самостійна покупка й керування мережею фізичних серверів.

Зрештою, усе полегшало, коли провайдери ЦОДів почали працювати в хмарі. Комерційно доступні й готові до продажу рішення, такі як Citrix XenServer, були використані для створення хмарної платформи віртуалізації. Система працює досить добре, але для користувачів, які мають потребу у високому рівні кастомізації, система може почати викликати проблеми із простоєм і розв'язною здатністю за часом, а також стати нездійсненно дорогою.

У таких ситуаціях підійде тільки рішення на замовлення. Тут варто очікувати, що ваш провайдер допоможе з міграцією, установкою нових серверів і користувальницькою конфігурацією. Якщо він може запропонувати гнучке рішення, наприклад, використання кластерів, це означає, що система буде функціонувати навіть у тому випадку, коли сервер вийде з ладу й ви зможете без праці перемістити дані на резервний сервер.

Можливість реагувати на ріст бізнесу також є ключовим моментом. Якщо ви знаєте, що в наступному році 70 серверів, які ви тільки що встановили, потрібно буде розширити до більш ніж 100, необхідна впевненість, що ваш провайдер зможе із цим упоратися.

Довіра провайдеру з питань безпеки й дотримання нормативних вимог

З появою масивів даних, інтернету речей і настанням четвертої промислової революції найважливішу роль стали грати безпека й контроль. Після того, як зберігання даних перемістилося за межі офісу, стало усе сутужніше стежити за їхнім розташуванням – дані можуть розміщатися не там, де ви думаєте або навіть не в тій країні. Для забезпечення безпеки буде цілком достатньо закону Великобританії про захист даних або аналогічних строгих правил, за умови, що дані перебувають у межах Європи, однак за межами Європи цих правил може бути недостатньо.

Ця проблема збільшується, якщо ви розробляєте ПЗ для регульованих галузей, таких як фінансові послуги, охорона здоров'я, медицина й оборона. Тут лідери бізнесу повинні відповідати вимогам індустрії платіжних карт (Payment Card Industry; PCI) і стандарту безпеки даних (Data Security Standards; DSS), а також закону Великобританії про захист даних (the UK Data Protection Act; DPA), стандарту ISO 27000, закону Сарбейнса-Оксли (Sarbanes-Oxley Act; SOX), закону про відповідальність і перенесення даних про страхування здоров'я громадян (the Health Insurance Portability and Accountability Act; HIPAAS) – і це тільки деякі з них.

Вирішальним фактором тут є те, що не всі провайдери ЦОДів будуть відповідати всіма правилам. Це відповідальність бізнесу й лідерів IT, щоб забезпечити відповідність цим правилам і стандартам.

Краща рада при виборі дата-центра, – переконатися, що ваш провайдер використовує сумісні ПЗ й устаткування з розширеними мірами безпеки, з довгим ключем шифрування й новітніх сертифікатів безпеки, і які також оснащені цілодобовими відео й аудіо-моніторингом.

Незважаючи на це, блискучі плани часто складаються невдало. У часи, коли сервіс випробовував проблеми – наприклад, під час DDoS-атаки по фінансовому секторі – клієнти одержували персонального менеджера й виділену телефонну лінію. Це було необхідно, коли надходив нестримний потік вхідних дзвінків від розгніваних клієнтів, що вимагають негайно повернути сервіс до роботи. Це були ті часи, коли можливість сказати своїм клієнтам, що все під контролем і проблема буде незабаром вирішена, була просто безцінна.

Еволюція дата-центрів, безумовно, додала бізнесу більшу гнучкість і вдосконалену ефективність в експлуатації, але це не виходить, що можна залишити дата-центр без уваги.

Більшість угод про рівень обслуговування (Service Level Agreement; SLA) зобов'язують провайдерів SaaS відповідати за подальше обслуговування й відновлення ПЗ, а це означає, що вони є останньою інстанцією.

У результаті, провайдеру надто важливо встановлювати регулярні відновлення, патчи й виправлення в міру їхньої появи. Дуже важливо мати в штаті експертів по безпеці для коректного виконання регулярних перевірок на уразливості й рішення проблем з ними. Наприклад, недавні зміни в правилах PCI говорять, що TLS1.0 і TLS1.1 – заміни для шифрування SSL V3.0 (Secure Socket Layer) – більше не застосовуються як приклад надійної криптографії в правилах PCI і DSS і починаючи з 30 червня 2016 року не можуть використовуватися як контроль безпеки.

Ретельно проаналізувавши рівень гнучкості провайдеру, те, як він дотримує стандартів, а також власні обов'язки, підприємства можуть продовжувати розвивати успішні платформи SaaS. Хоча створення стійких і вигідних довгострокових відносин усе ще може зажадати повернення до вікової традиції – зустрічі з постачальником послуг віч-на-віч.

Розробка структурної схеми

Розроблювальний у даній роботі програмний продукт Кастомізатор ЦОД Manager – це програмний продукт, що автоматизує керування різнорідної IT інфраструктурою центра обробки даних з метою кастомізації під конкретні вимоги клієнта. У цьому розділі я коротко опишу, для чого цей продукт призначений і які завдання вирішує.

Кастомізатор ЦОД – це серверна платформа, що базується на лінійках Rack і Blade.

Особливість серверної платформи програмний продукт Кастомізатор ЦОД у тому, що в конфігурації є одна блейд-кошик і деякий набір серверів. При цьому немає градації рішень і є внутрішній комутатор – модель 62 серії, Fabric Interconnect.

Традиційний підхід побудови інфраструктури полягає в тому, що в кожну блейд-кошик містяться комутатори типу LAN, SAN або Management. З такого підходу ми одержуємо безліч крапок керування й складне кабелювання. Далі все це виноситься в комутатор Top of Rack і в результаті виходить зайве накопичення.

Програмний продукт Кастомізатор ЦОД Manager дозволяє вирішити проблему настільки складної організації інфраструктури.

Серверне рішення програмний продукт Кастомізатор ЦОД відрізняється від традиційної схеми побудови інфраструктури тим, що на Fabric Interconnected будується єдиний внутрішній комутатор, що має винесені порти в кожну блейд-корзину. Завдяки цьому ми зменшуємо кількість сполучних ліній між центральними комутаторами й самими лезами. Ми одержуємо більшу масштабованість і легко нарощуємо ресурси.

Пари інтерконнектів може підтримувати до 20 шасі лез. На таких інтерконнектах відноситься System Manager, що саме й взаємодіє із програмний продукт Кастомізатор ЦОД Manager, завдяки чому ми можемо управляти пулами серверів і нав'язувати на них політики.

Керування фізичною інфраструктурою й віртуальними середовищами

Як відомо, сучасні вимоги до IT ростуть, потрібно постійно збільшувати оперативність розгортання тої або іншої інфраструктури. Традиційно у великих компаніях є розподіл системних адміністраторів по різних напрямках: адміністрування віртуальної інфраструктури, серверне адміністрування, адміністрування систем зберігання даних або мережної частини.

Ми одержуємо безліч учасників, який необхідно об'єднати між собою й налагодити ефективна їхня взаємодія. Також необхідно організувати ефективне виконання рутинних операцій, таких як прописування vLAN, фізична комутація чого-небудь і т.п. Із усього цього випливає загальна проблема – відсутність ефективного контролю. Через непогодженість у роботі різних фахівців строки впровадження часом виростають від декількох годин до декількох тижнів, а те й місяців. У результаті чого простоюють проекти бізнесу.

У продукті програмний продукт Кастомізатор ЦОД Manager усе зводиться до єдиної крапки керування. Він дозволяє нам з єдиної крапки управляти всіма чотирма рівнями: віртуалізація, обчислення, системи зберігання даних, мережа.

Структура програмного продукту Кастомізатор ЦОД Manager

Почнемо з фізичного середовища:

– Сервера: Cisco, HP, IBM, Dell. Від них потрібне наявність менеджменту керування сервером.

– Системи зберігання даних: EMC, VNX, VNX2, NetApp, вся лінійка FAS.

– Мережна частина: комутатори Cisco Nexus v1000, залізні Nexus, ASA і Brocade.

Віртуальне середовище: підтримується Hyper-V, VMware. Також є інтеграція з публічними хмарами.

Все керування базується на ролях. Є три основні ролі:

– Кінцевий користувач, того хто користується панеллю самообслуговування.

– IT адміністратор.

– Оператор, що займається моніторингом і базовими операціями з інфраструктурою

Система є модульною, отже є можливість інтеграції у віртуальну інфраструктуру без вимоги додаткових обчислювальних потужностей.

За допомогою програмного продукту Кастомізатор ЦОД Manager ми одержуємо глобальний моніторинг всіх чотирьох складових:

– Віртуалізація.

– Сервера.

– Мережа.

– Системи зберігання.

Рисунок 1 – Структурна схема системи

Все це здійснюється через користувальницький портал. Користувальницький портал надає деякий набір шаблонів, які вже зконфігуровані, і можливість відстеження виконання запитів. Через користувальницький портал можна сформувати запит на створення віртуальної віртуальної машини. Запити можуть вимагати попереднього твердження, а можуть виконуватися повністю автоматично. Їсти можливість створити віртуальну машину максимально швидко, не чекаючи дій з боку технічного фахівця.

Необхідність твердження запиту залежить від пула, у якому запитувана машина буде розташована. Є обчислювальні пули, які контролюються адміністратором, а є пули, з якими

користувач взаємодіє прямо, і повідомлення приходить адміністраторові тільки по факті виконання.

Програмний продукт Кастомізатор ЦОД Manager це продукт, що управляє всіма чотирма напрямками адміністрування інфраструктури й зводить їх у єдину крапку. При цьому відсутня необхідність перемикання між різними системами керування й використання консолі. програмний продукт Кастомізатор ЦОД Manager є готовим коробковим продуктом, його налаштування займає порядку години або двох залежно від глибини налаштування. Базова функціональність стає доступна буквально за 1 годину розгортання.

Висновок. У статті розглянуто та проаналізовано програмне забезпечення, призначено для системи розробки індивідуального проекту центрів обробки даних з застосуванням технологій кастомізації. В межах України в недостатній мірі представлені вітчизняні розробки в цій області. У роботі наведені теоретичне узагальнення й рішення наукового завдання дослідження методів розробки індивідуального проекту центрів обробки даних з застосуванням технологій кастомізації. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем розробки індивідуального проекту центрів обробки даних з застосуванням технологій кастомізації; Досліджена система розробки індивідуального проекту центрів обробки даних з застосуванням технологій кастомізації; На основі отриманих результатів досліджень створена програмна реалізація системи розробки індивідуального проекту центрів обробки даних з застосуванням технологій кастомізації. Розроблені під час виконання роботи алгоритми дозволяють успішно вирішувати завдання розробки індивідуального проекту центрів обробки даних з застосуванням технологій кастомізації. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки. Розроблене програмне забезпечення має простий, дружній та зручний інтерфейс користувача, що забезпечує легкість у освоєнні роботи програмного продукту, зручність у використанні, і не потребує особливих спеціальних знань. При створені програмного забезпечення було використано об'єктно-орієнтований підхід, що відповідає сучасним тенденціям у галузі розробки комерційних програмних систем. Програма реалізована на мові високого рівня Visual C#. Дана мова програмування дозволяє найбільш ефективно обробляти дані. Це дозволило мінімізувати строк розробки програмного забезпечення, і, як слід, зменшити витрати на його розробку. Запропоноване програмне забезпечення ділиться на загальне програмне забезпечення, що поставляється із засобами обчислювальної техніки й спеціальне програмне забезпечення, що спеціально розроблене для даної конкретної системи й включає програми, що реалізують її функції. Даються необхідні рекомендації з установки розробленого програмного забезпечення. Для підвищення рівня безпеки запропоновано застосовувати алгоритм DES. В цілому створене програмне забезпечення підтверджує правильність використаних проектних рішень та повністю відповідає вимогам технічного завдання. Створене програмне забезпечення має потенційну можливість для подальшого вдосконалення і застосування у різних галузях.

Список літератури

1. Мохамад Гани Абу Таам Разработка математической gert-модели технологии распространения компьютерных вирусов в информационно-телекоммуникационных сетях / А.А.Смирнов, Мохамад Гани Абу Таам // Информационные системы в управлении, образовании, промышленности: монография / Под редакцией профессора В.С. Пономаренко. – Х.: Вид-во ТОВ «Щедра садиба плюс», 2014. – 498 с.
2. Мохамад Гани Абу Таам метод управления доступом в интеллектуальных узлах коммутации / Мохамад Гани Абу Таам, А.А.Смирнов // Информационные технологии и защита информации в информационно-коммуникационных системах: монография / Под редакцией профессора В.С. Пономаренко. – Х.: Вид-во ТОВ «Щедра садиба плюс», 2015. – 486 с.

3. Мохамад Гани Абу Таам Математическая gert-модель технологии передачи метаданных в облачные антивирусные системы / В.В.Босько, А.А.Смирнов, И.А.Березюк, Мохамад Гани Абу Таам // Збірник наукових праць "Системи обробки інформації". – Випуск 1(117). – Х.: ХУПС – 2014. – С. 137-141.
4. Мохамад Гани Абу Таам структурно-логическая GERT-модель технологии распространения компьютерных вирусов / А.А.Смирнов, И.А.Березюк, Мохамад Гани Абу Таам // Системи управління, навігації та зв'язку. – Випуск 1(29). – П.: ПНТУ. – 2014. – С. 120-125.
5. Мохамад Гани Абу Таам Сравнительные исследования математических моделей технологии распространения компьютерных вирусов в информационно-телекоммуникационных сетях / Мохамад Гани Абу Таам, А.А. Смирнов, А.В. Коваленко, С.А. Смирнов // Збірник наукових праць "Системи обробки інформації". – Випуск 9(125). – Х.: ХУПС – 2014. – С. 105-110.
6. Мохамад Гани Абу Таам Математическая модель интеллектуального узла коммутации с обслуживанием информационных пакетов различного приоритета / Мохамад Гани Абу Таам, А.А. Смирнов, Н.С. Якименко, С.А. Смирнов // Збірник наукових праць Харківського університету Повітряних Сил. Випуск 4 (41). – Харків: ХУПС. – 2014. – С. 48-52.
7. Мохамад Гани Абу Таам Исследование показателей качества функционирования интеллектуальных узлов коммутации в телекоммуникационных системах и сетях / Мохамад Гани Абу Таам, А.А. Смирнов, Н.С. Якименко, С.А. Смирнов // Наука і техніка Повітряних Сил Збройних Сил України. – Випуск 4(17). – Харків: ХУПС. – 2014. – С.90-95.
8. Мохамад Гани Абу Таам Усовершенствованный алгоритм управления доступом к «облачным» телекоммуникационным ресурсам / Мохамад Гани Абу Таам, А.А. Смирнов, Н.С. Якименко, С.А. Смирнов // Збірник наукових праць "Системи обробки інформації". – Випуск 1(126). – Х.: ХУПС – 2015. – С. 150-153.
9. Мохамад Гани Абу Таам Анализ и исследование методов управления сетевыми ресурсами для обеспечения антивирусной защиты данных / Мохамад Гани Абу Таам, А.А. Смирнов, С.А. Смирнов // Системи озброєння і військова техніка. – Випуск 3(43) – Х.: ХУПС – 2015. – С. 100-107.
10. Мохамад Гани Абу Таам Исследование эффективности метода управления доступом к облачным антивирусным телекоммуникационным ресурсам / Мохамад Гани Абу Таам, А.А. Смирнов, С.А. Смирнов // Наука і техніка Повітряних Сил Збройних Сил України. – Випуск 3(19). – Х.: ХУПС. – 2015. – С. 134-141.
11. Mohamad Abou Taam Method of controlling access to intellectual switching nodes of telecommunication networks and systems / A.A. Smirnov, Mohamad Abou Taam, S.A. Smirnov // International Journal of Computational Engineering Research (IJCER). – **Volume 5, Issue 5. –** India. Delhi. – 2015. – P. 1-7.

УДК 004

А. Золотков, магістр гр. КІ-18-1,4
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ ЗАБЕЗПЕЧЕННЯ ШИРОКОМОВНОГО HD-ВІДЕО З ЗАСТОСУВАННЯМ ТЕХНОЛОГІЇ MBMS

У статті розроблено програмне забезпечення, яке призначено для системи забезпечення широкомовного HD-відео з застосуванням технології MBMS. Метою розробки є дослідження та програмна реалізація системи забезпечення широкомовного HD-відео з застосуванням технології MBMS. Об'єктом дослідження є процес забезпечення широкомовного HD-відео з застосуванням технології MBMS. Предметом дослідження є методи забезпечення широкомовного HD-відео з застосуванням технології MBMS. Методи дослідження базуються на методах теорії кодування інформації, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи забезпечення широкомовного HD-відео з застосуванням технології MBMS. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення. Розроблено зручний інтерфейс користувача. Наведені інструкції по роботі з програмними засобами.

комп'ютерна інженерія, HD-відео, MBMS

Постановка проблеми. Ринок мобільного зв'язку й послуг широкополосного доступу перетерпів значні зміни. Однак ARPU стагнує, незважаючи на можливості мережі, що постійно розширюються, при цьому значну частку доходів від Інтернету одержують OTT-гравці, а за телеком-операторами залишається тільки вкрай вузька ніша «труби із трафіком» без можливості збільшення прибутку. У цих умовах особливу важливість здобувають додаткові джерела доходу, які оператори мобільного зв'язку можу витягти шляхом надання послуг поверх своїх існуючих каналів.

Одним з потенційних джерел підвищення доходу є трансляція високоякісного HD-відео за допомогою технології Multimedia Broadcast Multicast Service (MBMS). Мова йде про виділення певного зарезервованого обсягу радіоресурсів для трансляції відеоконтенту в режимі багатоадресної передачі (multicast), тобто той самий контент транслюється всім споживачам у соті, де активована MBMS.

Подібна трансляція поверх стільникової мережі має наступні особливості. По-перше, окремий користувач не може вибрати довільне відео «для себе». По-друге, нікому не надаються окремий радіоресурс – всі користувачі приймають той самий загальний відеопотік, так що переглядати відео може практично нескінченне число абонентів у соті. По-третє, MBMS має на увазі виділення каналу для кожного відеопотоку, чим гарантується певна якість відео без деградації якості (за умови достатнього рівня сигнал/шум у точці прийому).

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні програмної реалізації системи забезпечення широкомовного HD-відео з застосуванням технології MBMS.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи забезпечення широкомовного HD-відео з застосуванням технології MBMS.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем забезпечення широкомовного HD-відео з застосуванням технології MBMS.

– Дослідження системи забезпечення широкомовного HD-відео з застосуванням технології MBMS.

– Програмна реалізація системи забезпечення широкомовного HD-відео з застосуванням технології MBMS.

Об'єктом дослідження є процес забезпечення широкомовного HD-відео з застосуванням технології MBMS.

Предметом дослідження є методи забезпечення широкомовного HD-відео з застосуванням технології MBMS.

Методи дослідження базуються на методах теорії кодування інформації, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. У цей час спостерігається значний ріст обсягів переданого трафіку в мережах LTE. Більше того, такі компанії, як Ericsson і Cisco прогнозують, що обсяг переданих у мобільних мережах даних за місяць збільшиться в 10 разів до 2020 року в порівнянні з 2014 роком.

Відповідно, перед операторами мобільного зв'язку буде стояти завдання забезпечення передачі таких обсягів даних. Одним з рішень цього завдання є використання технології **eMBMS (evolved Multicast/Broadcast Multimedia Services)**. Яку ми й розглянемо в даному розділі. Далі приводяться опис основних варіантів використання цієї технології й стан справ у світі по її впровадженню, пілотуванню.

Якщо говорити про технологію eMBMS коротко, то це передача тих самих даних практично необмеженій кількості користувачів. При цьому, на радіоканалі використовується той самий частотно-часовий ресурс. Тобто, всі базові станції, які ставляться до зони віщання eMBMS сервісу, у те саме час на тих самих частотних ресурсах з абсолютно однаковими параметрами передачі транслюють ті самі дані. Таким чином, технологія eMBMS дозволяє

вирішити завдання доставки популярних даних абонентам, передаючи їхній один раз відразу всім одержувачам, а не кожному окремо, як це відбувається у випадку з unicast трафіком. Такими популярними даними можуть бути відео, аудіо, ПЗ, новини й т.д.

Для запуску технології eMBMS потрібне розширення пакетної мережі (Core Network) оператора й відновлення ПЗ на радіомережі. Крім цього, для прийому eMBMS сервісу необхідно, щоб мобільний термінал підтримував дану технологію. Список таких мобільних терміналів приводиться нижче. Технічні деталі eMBMS будуть розглянуті в окремій замітці трохи пізніше. Зараз же зупинимося на варіантах її використання.

1. Трансляції на масових подіях

eMBMS може використовуватися для надання додаткового сервісу на масових заходах, включаючи концерти, спортивні заходи, виставки, конференції й т.д. Як правило, на таких заходах мобільні мережі випробовують істотне навантаження. Через цього значним образом страждає якість обслуговування абонентів, аж до повної відсутності сервісів. Використання технології eMBMS дозволяє надавати сервіси з гарантованою якістю обслуговування практично для необмеженої кількості абонентів (залежить від використовуваного рішення й обраної бізнес моделі). Як такі сервіси можуть виступати відео трансляції для глядачів на стадіоні, повтори небезпечних моментів, додаткова статистика, результати й відео небезпечних/цікавих моментів інших матчів/змагань, які йдуть у цей же час.

У цьому випадку існує кілька варіантів монетизації таких сервісів. Найпростіший, коли сервіс надається безкоштовно й/або включається в пакет послуг і служить додатковим фактором для збільшення лояльності абонентів. Інший варіант – це підписка. Абонент підписується на сервіс, платить абонентську плату за місяць і протягом місяця ним користується. Також є варіант включення плати за сервіс у вартість квитків на захід. Ще один варіант, коли організатор заходу замовляє надання такого сервісу в оператора мобільного зв'язку. Ну й, звичайно, є варіант монетизації таких сервісів через розміщення в них реклами.

2. Мобільне ТБ і радіо

eMBMS може використовуватися для передачі мобільного ТБ і/або радіо в реальному часі. У такий спосіб абоненти будуть мати можливість дивитися свої улюблені канали й передачі в будь-якому місці, де є покриття стільникової мережі, з гарантованою якістю. Такий сервіс може входити в пакет послуг, може бути оформлений як додатковий сервіс по підписці. Може надаватися безкоштовно за рахунок продажів реклами або за рахунок надходжень від телеканалів за доступ до аудиторії.

З технічної точки зору eMBMS технологія вже зараз готова до такого використання, однак є ряд подальших поліпшень, які дозволять підвищити ефективність використання цієї технології. Частина із цих поліпшень ще не включена в специфікації 3GPP.

3. Доставка популярних відео, музики, газет і журналів

eMBMS може використовуватися для передачі популярних даних таких, як відео, музика, газети й журнали. Більше того, ця передача може здійснюватися в годинники найменшого навантаження на мережу (наприклад, уночі). Абоненти підписуються на серіали, ТБ програми, музичних виконавців, газети, журнали й т.д. Як тільки з'являється нова серія, випуск програми, пісня й т.д. це відразу передається всім передплатникам за один сеанс, а не кожному окремо.

4. Відновлення ПЗ

eMBMS може використовуватися для передачі даних під час відновлення програмного забезпечення (ПЗ). Це може бути кожне ПЗ (ОС на телефоні, додатка, ПЗ WiFi роутерів і т.д.). Наприклад, після виходу чергової версії iOS у мережі одного з європейських операторів передача нового ПЗ займала кілька десятків відсотків від загальної передачі даних. При використанні eMBMS передача цього відновлення могла бути здійснена вночі після виходу нової версії один раз на всі пристрої, що дозволило б розвантажити мережа оператора.

5. Рекламні акції

eMBMS може використовуватися для поширення реклами. Це може бути як щось масштабне в межах країни, регіону, міста. Так і локальні рішення. Наприклад, молли, де передається інформація про акції, знижки, нових надходженнях, розважальних програмах і т.д.

6. Локальні сервіси

Один із прикладів локальних сервісів – це інформація про розклад і поточне місце розташування транспортних засобів на зупинках суспільного транспорту. Ще варіант трансляція аудіо екскурсій для туристів у найбільш популярних місцях.

7. Суспільна безпека

У цей час 3GPP активно проробляється використання eMBMS для рішень суспільної безпеки. eMBMS може використовуватися для організації Push-to-Talk сервісу. А також для передачі якихось даних, сигналів одночасно всім співробітникам.

Тестування й запуски eMBMS у світі

У цей час eMBMS запущений у комерційну експлуатацію корейським оператором KT у січні 2014 року. Нижче в таблиці приводиться список пілотних запусків eMBMS, які були здійснені операторами по усьому світі.

Таблиця 1 – Тестування й запуски eMBMS у світі

	Хто запускав	**Країна**	**Опис**
1	Telstra	Австралія	Перший у світі запуск на стадіоні 31 січня 2014 під час матчу по крикету на Melbourne Cricket Ground (MCG)
2	China Mobile	Китай	Публічна демонстрація на мережі LTE TDD в 2013. Плани запуску комерційного eMBMS в 2015
3	China Telecom	Китай	Тріал у червні 2014 у місті Nanjing. Прекомерційний запуск у рамках 2014 Summer Youth Olympic Games (Август 16-28)
4	Orange	Франція	Тріал у рамках French Tennis Open 2014 at Roland Garros
5	Vodafone	Германія	Перший у Європі запуск на стадіоні під час футбольного матчу "Боруссії" Мьонхенгладбах. Тріал під час вітрильної регати в Кілі (Kieler Woche).
6	RJIL	Індію	Тріал у місті Мумбай.
7	KPN	Голландія	Тріал на стадіоні під час футбольного матчу "Аякса" 3-го травня 2014
8	Globe	Філіппіни	Демонстрація під час Globe Innovation Forum
9	Smart	Філіппіни	Тріал в 2013 році на частотах 2.1 ГГц.
10	Polkomtel	Польща	Тріал під час першої гри чемпіонату світу з волейболу з використанням 300 терміналів на національному стадіоні
11	Meo	Португалія	Тріал
12	SingTel	Сінгапур	Тріал у другій половині 2014
13	Etisalat	ОАЕ	Тріал
14	EE & BBC	Британія	Демонстрація під час Commonwealth Games 2014 у Глазго. Демонстрація на фіналі Кубка Англії по футболі 2015 на стадіоні Уемблі.
15	3UK	Британія	Тріал на комерційній мережі в Maidenhead
16	AT&T	США	Плани запуску комерційного eMBMS сервісу в 2015
17	Verizon	США	Тріал під час SuperBowl 2014 і гонок Indy 500. Плани запуску комерційного eMBMS в 2015.
18	Telecom Italia	Італія	Тріал eMBMS на стадіоні Сан-сиро під час гри "Милана". Сервіс включав трансляцію трьох футбольних матчів, що проводилися в той же час.
19	IRT	Германія	Тріал у Мюнхені на частотах 700 МГц разом з Nokia.
20	Vodafone	Іспанія	Тріал під час футбольного матчу на стадіоні Mestalla у Валенсії 17-го травня 2015. Сервіс містив у собі 5 відео каналів у форматі HD.

Як видно з наведеного вище списку, основна маса пробних запусків здійснюється в рамках спортивних заходів. Однак, спільний тріал німецького інституту IRT і Nokia у Мюнхені служить мети вивчити використання eMBMS для передачі ТБ каналів і зрівняти eMBMS з існуючими стандартами DVB-T.

Підтримка eMBMS з боку мобільних пристроїв

Лідер виробництва чипсетів для мобільних пристроїв Qualcomm має у своїй лінійці рішення з підтримкою eMBMS, починаючи з MSM8974. Австралійський оператор Telstra говорить про те, що в його мережі присутні наступні моделі мобільних терміналів з підтримкою eMBMS: Sony Experia Z1, Z2; Samsung Galaxy S5, S4 mini; LG G2, G3. І до кінця 2015 року очікує появи ще 5 моделей з підтримкою eMBMS. Крім зазначених вище моделей, підтримку eMBMS мають наступні термінали: Samsung Galaxy Note 3, Huawei C8817, TCL P688L.

Розробка структурної схеми

Передумови впровадження MBMS

Оператори мобільного зв'язку вже доставляють величезні обсяги відео своїм абонентам: цей контент затребуваний, і на нього вже доводиться основна частка мобільного трафіку (в основному із сайту YouTube). За останні роки із впровадженням HSDPA/HSDPA+ і розгортанням мереж 4G/4G+ користувачі звикли до високих швидкостей передачі даних, і перегляд відео на смартфонах уже не є екзотикою. Навпаки, у міру все більшого розширення аудиторії зростає споживання мобільного відеоконтенту. У результаті оператори зв'язку одержують можливість утримувати наявних користувачів і залучати нових шляхом надання такої послуги/сервісу, як трансляція високоякісного відео, що напевно зацікавить споживачів.

Бізнес-драйверами для впровадження MBMS є, таким чином, необхідність задоволення зростаючого попиту на відеоконтент в умовах обмеженого спектра й зацікавленість у нових джерелах доходу, які стають доступні з появою технології MBMS.

Надання сервісу MBMS групі абонентів, зацікавлених у тому самому відеоконтенті, дозволяє не тільки значно поліпшити якість відео, призначеної для цієї групи, але й у деяких випадках підвищити швидкість і якість мобільного Інтернету для інших користувачів, тому що всі споживачі «важкого» відеоконтенту будуть переведені на радіоресурс MBMS, звільнивши «звичайні» LTE-радіоресурси конкретної стільники для інших абонентів.

В 3GPP Rel.12 визначений режим MBMS на вимогу (MBMS Operation On Demand, MOOD), що дозволяє динамічно включати/виключати MBMS залежно від установлених порогів спрацьовування. Інакше кажучи, MBMS можна буде активувати тільки після перевищення якогось порога X для числа зацікавлених в MBMS користувачів і відключати після скорочення кількості активних MBMS-користувачів нижче встановленого порога Y, вивільняючи ресурси під «звичайний LTE».

Технічні основи MBMS

У звичайній мобільній мережі, якщо той самий відеоконтент проглядається, допустимо, п'ятьома користувачами в соті, для нього необхідно виділити пропорційний обсяг радіоресурсу, тобто в п'ять разів більше, ніж при одиничному перегляді. Ситуація погіршується в X раз, якщо той самий відеоконтент переглядають X користувачів.

MBMS, з іншого боку, забезпечує гарантоване й високоякісне відео для будь-якої кількості абонентів у соті без нарощування обсягу виділених радіоресурсів у випадку збільшення числа користувачів, тому що трансляція ведеться в режимі «точка – безліч точок». Інакше кажучи, багатоадресна передача MBMS активується на рівні стільники, що дає певну волю у виділенні й призначенні ресурсів для MBMS-відео залежно від переваги абонентів у тій або іншій зоні, а підтримка декількох відеоканалів MBMS на кожної соті дозволяє пропонувати різні варіанти відеоконтенту.

Технологія MBMS має на увазі виділення спектра для відеовіщання усередині наявної несучої LTE. З одного боку, це плюс, тому що MBMS може бути розгорнута на існуючих мережах без додавання частот, але з іншого боку – мінус, оскільки ємність стільники

(несучої) знижується на величину, виділену для MBMS. Технологія MBMS може бути реалізована в мережах як FDD, так і TDD LTE, вона не прив'язана до спектра й може бути розгорнута на будь-яких частотах LTE, доступних операторові. Усередині несучої LTE під MBMS може бути виділене від 0,3 до 60% ширини, причому ширина виділеної смуги є компромісом між якістю й кількістю відеоканалів, з одного боку, і шириною спектра, якому потрібно залишити «звичайним» абонентам LTE для доступу в Інтернет, з іншої сторони.

Технологія MBMS має на увазі надання того самого відеоконтенту на виділеному кластері, що складається з декількох базових станцій, віщання здійснюється синхронно у всіх секторах у ті самі виділені моменти часу. Як наслідок, для MBMS потрібна точна (фазова) синхронізація GPS. Висока якість відео досягається за рахунок двох основних аспектів цієї технології: по-перше, це гарантований виділений обсяг радіоресурсу, що ні за яких умов не може бути ні зменшений, ні зайнятий абонентами LTE, і по-друге – синхронна трансляція того самого відеоконтенту у всіх секторах і на всіх БС у кластері, завдяки чому в будь-якій точці прийому сигнали від сусідніх секторів (або сусідніх БС) є не перешкодою, а, навпаки, представляють собою корисний сигнал. Сигнали від сусідніх стільник складаються, у результаті збільшується відношення сигнал/шум у точці прийому й, у порівнянні з «звичайним» цілеспрямованим віщанням, «картинка» поліпшується.

По своїй суті MBMS має на увазі синхронну передачу відеоконтенту для масової аудиторії й не припускає ніякого зворотного зв'язка по висхідному каналі (channel feedback). Як наслідок, модуляція в радіоінтерфейсі для каналу MBMS фіксується – вона однакова для всіх користувачів у соті й кластері без можливості динамічної зміни схеми кодування для окремого абонента. При реалізації MBMS із трьох основних типів модуляції фізичного рівня QPSK/16QAM/64QAM, як правило, установлюється одна «середня» модуляція 16QAM.

Для LTE FDD на ширині несучої 20 Мгц максимальна пікова швидкість передачі даних при використанні 64QAM і MIMO2x2 становить близько 150 Мбіт/с, при виділенні під MBMS половини несучої одержуємо швидкість близько 75 Мбіт/с, однак в MBMS не використовується MIMO, що автоматично приводить до зниження пікової швидкості у два рази. Інакше кажучи, на несучої 20 Мгц при виділенні 50% спектра під MBMS пікова швидкість передачі даних при модуляції 64QAM дорівнює приблизно 37 Мбіт/с. Однак для забезпечення нормального покриття стільники доречно використовувати менш швидкісну й краще захищену від перешкод схему модуляції 16QAM, що приводить до зниження пікової швидкості ще приблизно на третину. Таким чином, реалістична швидкість, який можна досягти при несучої 20 Мгц і виділенні під MBMS половини несучої, становить близько 20-25 Мбіт/с. При несучої 10 Мгц швидкість знижується до 10 Мбіт/с.

Для доставки HD-відео на смартфон або планшет, залежно від відеокодека, необхідна швидкість передачі даних близько 2 Мбіт/с на один відеопотік. Таким чином, на несучої 20 МГц при виділенні під MBMS половини несучої ми одержуємо 10–12 відеоканалів з якістю HD, а на несучої 10 МГц при виділенні під MBMS половини несучої – близько 5 HD-відеоканалів. При виділенні 30% несучої під MBMS для несучої 20 МГц буде близько 7–8 HD-відеоканалів, а у випадку 10 МГц за тих самих умов одержуємо 3–4 HD-відеоканали. При використанні низькошвідкістних кодеків з'являється можливість дворазового зниження швидкості відеопотоку при збереженні прийнятної якості картинки, що дозволяє вдвічі збільшити кількість відеоканалів.

Крім радіоподсистеми, для реалізації MBMS необхідно впровадити два додаткових мережних елементи: BM-SC (Broadcast Multicast Service Center) і MBMS-GW (MBMS Gateway). Перший є вхідною точкою для подачі відеопотоку (-ів) і керування їм (ними) контент-провайдером, а другий доставляє відеопотік до базової станції й управляє сигнальними повідомленнями сеансу MBMS.

Практичне застосування MBMS

В Україні найбільше поширення одержали мережі FDD LTE ‹band › у діапазоні 2600 МГц, у якому в кожного із трьох національних операторів є смуга шириною 10 Мгц. При виділенні під MBMS третини смуги спектра можна транслювати 3-4 HD-відеоканали зі

швидкістю відеопотоку близько 2 Мбіт/с кожний. Важливо розуміти, що при виділенні під MBMS, наприклад, 30% несучої, ми, відповідно, на 30% знижуємо смугу частот, доступну «звичайним» LTE-Абонентам, що приводить до пропорційного зменшення ємності стільники й максимальної швидкості передачі Інтернету в соті. Таким чином, включення MBMS – це досить «дороге задоволення», при якому надання всього лише 3–4 відеоканалів у якості HD знижує на 30% максимальну швидкість Інтернету для всіх абонентів.

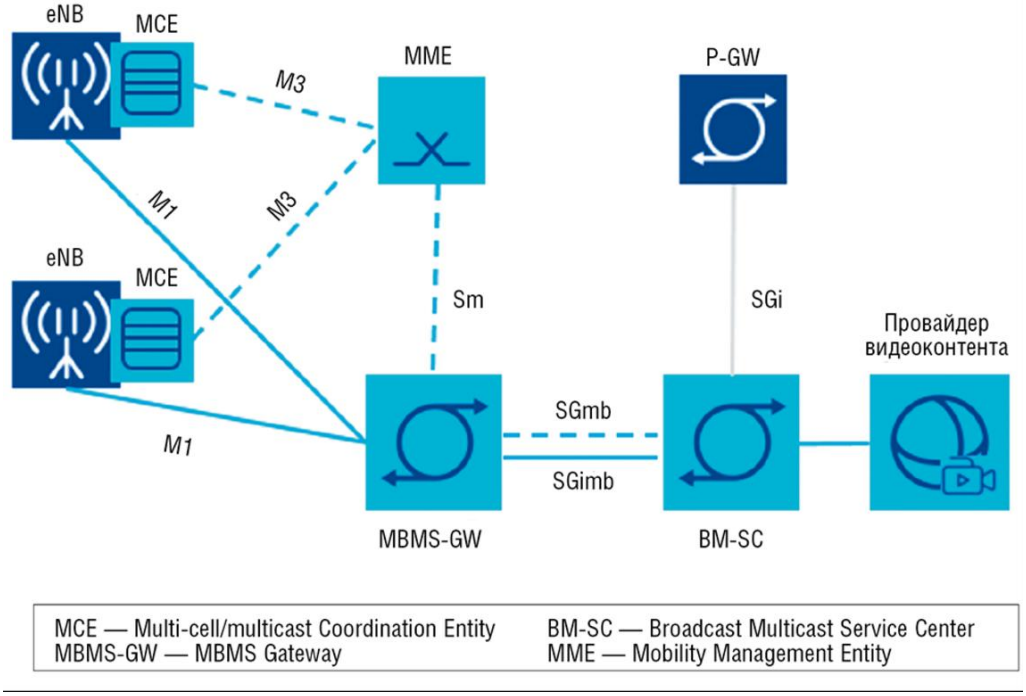


Рисунок 1 – Структурна схема системи

MBMS підтримується тільки найсучаснішими й дорогими смартфонами, а із цієї незначної кількості власників сумісних терміналів далеко не всі зацікавлені в MBMS. У середньому частка зацікавлених користувачів, у яких є технічна можливість використання MBMS (підтримується терміналом абонента), становить одиниці відсотків. Разом з тим при виділенні під MBMS, допустимо, 30% спектра несучої, ми знижуємо і ємність стільники, і максимальну швидкість передачі для абсолютно всіх абонентів. Очевидно, що обмежувати ємність стільники й швидкість Інтернету заради задоволення настільки невеликого попиту невигідно з економічної точки зору. Відповідно, включення MBMS на всій мережі навряд чи коли-або відбудеться.

Однак уже відомі окремі випадки застосування MBMS, коли її включення на певному кластері й у певних умовах може бути економічно вигідно. Нагадаємо, що по якості відео MBMS має значні переваги перед «звичайним» LTE, коли той самий відеоконтент дивляться багато користувачів, оскільки кожному з них не виділяється окремий радіоресурс, але всі приймають один загальний канал, що віщає у виділеній гарантованій смузі.

Даним умовам відповідають такі події, як масові заходи, коли в ході відеотрансляції ті або інші епізоди проглядаються з різних ракурсів безліччю абонентів. Як приклади можна назвати хокейні й футбольні матчі з їхніми повторами гольових ситуацій, а також автогонки, де глядачам цікаво бачити не тільки близько розташована ділянка траси, але й вилучені ділянки.

Проведені опитування показують, що успішний запуск MBMS можливий у наступних областях:

– ексклюзивне відео в місцях значної концентрації абонентів, що прийшли на масовий захід (концерт, шоу, спортивне захід);

– трансляція суспільно значимих подій, а також заходів, що цікавлять більшість абонентів (футбольних/хокейних матчів збірні Україні по всій країні, матчів команди «А» для регіону «А» або команди «Б» для регіону «Б»);

– мобільне HD-ТБ.

Крім перерахованих, можна назвати ще кілька приватних випадків, коли має сенс використовувати MBMS: тимчасове виділення каналу MBMS для накачування в смартфони «важких» і однакових для всіх відновлень програмного забезпечення (наприклад, відновлення версій iOS або Android протягом декількох днів після виходу нової версії ОС); виділення каналу для відновлення ПЗ великими організаціями з розгалуженою розподіленою інфраструктурою (датчики, M2M); передача відеоінструкцій екстреними службами (наприклад, в випадку стихійних лих).

Найбільш реалістичним випадком комерційного застосування MBMS є трансляція HD-відео спортивного заходу з різних ракурсів для вболівальників, що прийшли на стадіон. Наявність декількох відеоканалів дозволяє диференціювати відеоконтент для різних користувачів, у той час як загальні екрани на стадіоні не дозволяють це робити. У такому випадку під MBMS можна виділити максимально широку смугу. При цьому наявність 5-10 HD-каналів дозволить глядачам насолоджуватися переглядом гри з різних ракурсів і різних точок і вибирати найцікавіші додаткові ракурси перегляду.

У випадку віщання MBMS для групи відвідувачів якого-небудь заходу витрати оператора зв'язку на запуск MBMS можуть бути «упаковані» у вартість вхідного квитка, так що користувачам не буде потрібно додатково оплачувати сервіс MBMS. Надання сервісу MBMS для певної групи користувачів може позиціонуватися як «преміальна» послуга з ексклюзивним відеоконтентом, недоступним іншим абонентам.

Можливими перешкодами на шляху впровадження MBMS можуть стати недолік абонентських терміналів з підтримкою MBMS і відсутність економічно привабливого бізнесу-кейса.

Абонентські пристрої з підтримкою MBMS

Недостатня підтримка технології MBMS на терміналах абонентів є одним із ключових факторів, що стримують комерційне застосування даної технології. У даний момент на українському ринку лише мала частина терміналів оснащена такою опцією. Разом з тим MBMS підтримується більшістю сучасних мікросхем преміального рівня й деяких чипів середнього цінового діапазону. Оскільки вартість мікросхем знижується, очікується, що в найближчі роки майже всі нові смартфони будуть випускатися з убудованою підтримкою MBMS. Як показують опитування, для комерційно успішного запуску послуг на базі MBMS частка таких смартфонів повинна становити не менш 30%. Відновлення цих пристроїв відбувається в середньому один раз у півтора-два роки. Тому очікується, що протягом декількох років кількість смартфонів з підтримкою MBMS досягне «критичної маси», при якій запуск послуг на основі MBMS стане економічно доцільним.

Висновок. У статті розглянуто та проаналізовано програмне забезпечення, яке призначено для забезпечення широкомовного HD-відео з застосуванням технології MBMS. В межах України в недостатній мірі представлені вітчизняні розробки в цій області. У роботі наведені теоретичне узагальнення й рішення наукового завдання дослідження методів забезпечення широкомовного HD-відео з застосуванням технології MBMS. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем забезпечення широкомовного HD-відео з застосуванням технології MBMS; Досліджена система забезпечення широкомовного HD-відео з застосуванням технології MBMS; На основі отриманих результатів досліджень створена програмна реалізація системи забезпечення широкомовного HD-відео з застосуванням технології MBMS. Розроблені під час виконання роботи алгоритми дозволяють успішно вирішувати завдання забезпечення широкомовного HD-відео з застосуванням технології MBMS. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована

алгоритм і вибраний середовище розробки. Розроблене програмне забезпечення має простий, дружній та зручний інтерфейс користувача, що забезпечує легкість у освоєнні роботи програмного продукту, зручність у використанні, і не потребує особливих спеціальних знань. При створені програмного забезпечення було використано об'єктно-орієнтований підхід, що відповідає сучасним тенденціям у галузі розробки комерційних програмних систем. Програма реалізована на мові високого рівня Embarcadero Delphi 10. Дана мова програмування дозволяє найбільш ефективно обробляти дані. Це дозволило мінімізувати строк розробки програмного забезпечення, і, як слід, зменшити витрати на його розробку. Запропоноване програмне забезпечення ділиться на загальне програмне забезпечення, що поставляється із засобами обчислювальної техніки й спеціальне програмне забезпечення, що спеціально розроблене для даної конкретної системи й включає програми, що реалізують її функції. Даються необхідні рекомендації з установки розробленого програмного забезпечення. Для підвищення рівня безпеки запропоновано застосовувати алгоритм Blowfish.

Список літератури

1. Дреев А.Н. Использование неравномерного распределения единичных битов для дополнительного сжатия SPIHT кода / А.Н. Дреев, А.А. Смирнов // Информационные системы в управлении, образовании, промышленности: монография. Под редакцией профессора В.С. Пономаренко. – Х.: Вид-во ТОВ «Щедра садиба плюс», 2014. – С. 498.
2. Дрєєв О.М. Дослідження впливу шляху розгортки на ступінь ентропійного стиснення цифрового зображення / О.М. Дрєєв, О.В. Слюсар // Збірник наукових праць Кіровоградського національного технічного університету. Техніка в сільськогосподарському виробництві, галузеве машинобудування, автоматизація. Випуск 21. – Кіровоград: КНТУ. – 2008 – С. 115-118.
3. Дрєєв О.М. Метод розвантаження телекомунікаційного сервера за рахунок кешування зображень / О.М. Дрєєв // Збірник наукових праць Кіровоградського національного технічного університету. Техніка в сільськогосподарському виробництві, галузеве машинобудування, автоматизація. Випуск 25. Ч. І. – Кіровоград: КНТУ. – 2012 – С. 419-424.
4. Дрєєв О.М. Метод прогнозування завантаженості серверу телекомунікаційної мережі / О.М. Дрєєв, О.А. Смірнов, Є.В. Мелешко, О.В. Коваленко // Системи обробки інформації. Випуск 3(101) Том 2. – Х.: ХУПС. – 2012. – С. 181-188.
5. Дрєєв О.М. Оцінка якості стиснення зображень на основі дискретного перетворення Хартлі / О.В. Коваленко, О.П. Доренський, О.М. Дрєєв // Системи озброєння і військова техніка. Науковий журнал 2(34) – Х.: ХУПС – 2013. С. 99-102.
6. Дрєєв О.М. Дослідження впливу ступеня стиснення зображень на оперативність їх доставки у телекомунікаційній системі / О.А. Смірнов, О.М. Дрєєв, О.П. Доренський // Збірник наукових праць "Системи обробки інформації". – Випуск 8(115). – Х.: ХУПС – 2013. – С. 234-239.
7. Дреев А.Н. Сравнение битовых плотностей при использовании различных методов кодирования информации / А.Н. Дреев, А.А. Смирнов // Системи обробки інформації, 2014, випуск 2 (118), том 2 – Харків: ХУПС – 2014. С 64-66.
8. Дрєєв О.М. Моделювання впливу інтенсивності трафіку на оперативність доставляння інформації / О.М. Дрєєв // Науково-виробничій журнал "Зв'язок". – Київ: ДУТ, 2014. – № 2 (108) С. 24-29.
9. Дреев А.Н. Повышение вероятности доставки сообщений в телекоммуникационных системах и сетях для обеспечения информационной безопасности / А.Н. Дреев, А.А. Смирнов //«Безпека інформації» Том 21, №1 2015 р. – Київ: НАУ – 2015. – С. 22-28.
10. Дрєєв О.М. Узагальнення вейвлету Хаара / О.М. Дрєєв, Г.М. Дрєєва // Збірник тез доповідей Комбінаторні конфігурації та їх застосування, 15-16 жовтня 2010 р. – Кіровоград – С. 58

УДК 004

К. Ібатуліна, магістр гр. КН-18М3
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ УПРАВЛІННЯ ВЕБ-САЙТОМ ОНЛАЙН-КУРСІВ

У статті розроблено програмне забезпечення, яке призначено для системи управління веб-сайтом онлайн-курсів. Метою розробки є дослідження та програмна реалізація системи управління веб-сайтом онлайн-курсів. Об’єктом дослідження є процес дистанційного навчання та тестування знань студентів. Предметом дослідження є алгоритми та методи дистанційного навчання та оцінювання знань студентів. Методи дослідження базуються теорії інформації, аналізу статистичних даних, теорії обчислювальної складності алгоритмів, а також технології відкритих систем. При створенні програмного забезпечення використовувалися методи об'єктно-орієнтованого програмування. Результат роботи – програмна реалізація системи управління веб-сайтом онлайн-курсів для вивчення різних предметів та циклів предметів. В процесі роботи над програмною моделлю виконано аналіз існуючих алгоритмів та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення. Розроблено зручний інтерфейс користувача. Наведені інструкції по роботі з програмними засобами.Програму розроблено на мові програмування PHP.
комп’ютерні науки, онлайн курси, дистанційне навчання, онлайн тестування, веб-сайти

Постановка проблеми. Актуальність теми обумовлена тим, що на сьогодняшій день комп’ютери відіграють досить значну, якщо не сказати вирішальну, роль у житті як окремих особистостей, так і людства в цілому. Різноманітні інформаційні технології фігурують практично у всіх сферах людського життя та побуту. Глобальна мережа Internet є яскравим тому прикладом. За допомогою інтернету можна задовольнити майже будь-які людські потреби, починаючи від банального спілкування (соціальні мережі, skype, e-mail) і закінчуючи потребою в заробітку коштів (інтернет-торгівля, фріланс, інтернет-лотереї).

Не обійшли інформаційні технології й освітню сферу. На даний момент існує безліч освітніх порталів, за допомогою яких віддалено можна отримати знання досить високої якості. Одним з аспектів навчального процесу є перевірка знань. Таку перевірку зручно проводити у форматі тестування. Тестування є одним з найбільш ефективних способів перевірки отриманих знань і зараз набуло великої популярності.

Дистанційне навчання та тестування знань є оптимальним варіантом для багатьох людей, які прагнуть здобути знання, але мають обмаль часу, або географічні обмеження.

Зважаючи на вищезазначені переваги можна зробити висновок, що система управління веб-сайтом онлайн-курсів є актуальною науково-практичною задачею.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи управління веб-сайтом онлайн-курсів**.**

Мета й завдання дослідження. Метою роботи є розробка системи управління веб-сайтом онлайн-курсів.

Для досягнення поставленої мети вирішувалися наступні завдання:

1. Формальна постановка завдання та розробка загальної схеми процесу проектування.
2. Розробка методики побудови комплексу алгоритмів, за якими будуть надаватися курси та оцінюватися знання студентів.
3. Експериментальна перевірка запропонованої методики.

Об’єктом дослідження є процес дистанційного навчання та тестування знань студентів.

Предметом дослідження є алгоритми та методи дистанційного навчання та оцінювання знань студентів.

Виклад основного матеріалу. Метою даної роботи є розробка програмного забезпечення для дистанційного навчання та тестування знань студентів. Реалізацією поставленої задачі буде веб-сайт, який матиме всі потрібні для перевірки знань функції.

Розроблене програмне забезпечення створено згідно з парадигмою MVC. MVC (Model-View-Controller) – схема використання декількох шаблонів проектування, за допомогою яких модель, користувацький інтерфейс і взаємодія з користувачем розділені на три окремих компоненти таким чином, щоб модифікація одного з компонентів надавала мінімальний вплив на інші. Дана схема проектування часто використовується для побудови архітектурного каркаса, коли переходять від теорії до реалізації в конкретної предметної області. Схема MVC зображена на рисунку 1.

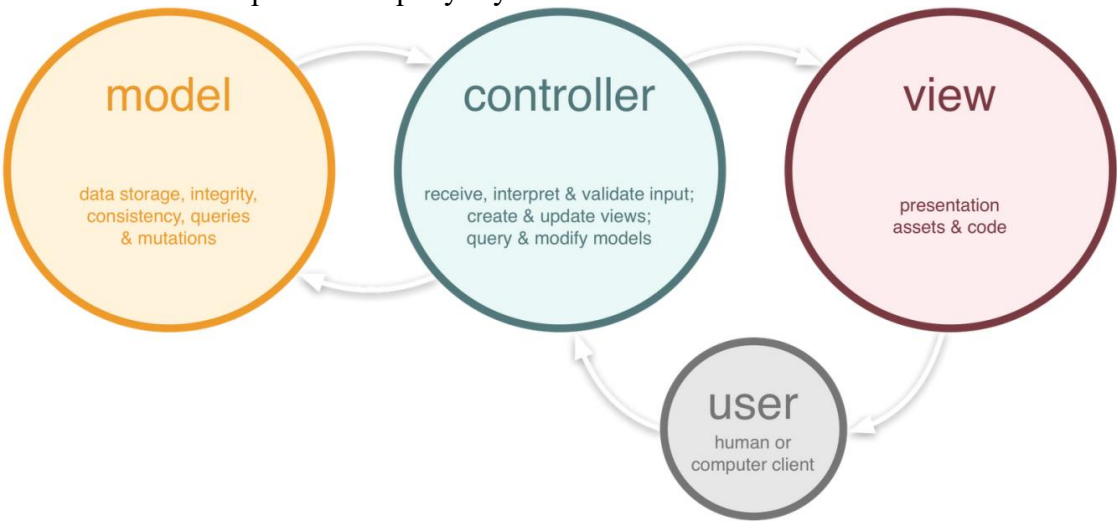


Рисунок 1 – Структура MVC

Концепція MVC дозволяє розділити дані, подання та обробку дій користувача на три окремих компоненти:

− Модель. Модель надає знання: дані і методи роботи з цими даними, реагує на запити, змінюючи свій стан. Не містить інформації, як ці знання можна візуалізувати.

− Подання, вид. Відповідає за відображення інформації (візуалізацію). Часто як подання виступає форма (вікно) з графічними елементами.

− Контролер. Забезпечує зв'язок між користувачем і системою: контролює введення даних користувачем і використовує модель та подання для реалізації необхідної реакції.

Важливо відзначити, що як подання, так і контролер залежать від моделі. Однак модель не залежить ні від уявлення, ні від контролера. Тим самим досягається призначення такого поділу: воно дозволяє будувати модель незалежно від візуального представлення, а також створювати кілька різних подань для однієї моделі.

Для реалізації схеми модель-подання-контролер використовується досить велике число шаблонів проектування (залежно від складності архітектурного рішення), основні з яких «спостерігач», «стратегія», «компонувальник».

Найбільш типова реалізація відокремлює подання від моделі шляхом встановлення між ними протоколу взаємодії, використовуючи апарат подій (підписка/сповіщення). При кожній зміні внутрішніх даних в моделі вона оповіщає всі залежні від неї подання, і подання оновлюється. Для цього використовується шаблон «спостерігач». При обробці реакції користувача подання вибирає, залежно від потрібної реакції, потрібний контролер, який забезпечить той чи інший зв'язок з моделлю. Для цього використовується шаблон «стратегія», або замість цього може бути модифікація з використанням шаблону «команда». А для можливості однотипного поводження з підоб'єктами складно-складеного ієрархічного

виду може використовуватися шаблон «компонувальник». Крім того, можуть використовуватися й інші шаблони проектування, наприклад, «фабричний метод», який дозволить задати за замовчуванням тип контролера для відповідного виду.

Розроблена система має простий та інтуїтивно зрозумілий інтерфейс користувача. Інтерфейс має приємний зовнішній вигляд, і в той же час включає елементи користувацького інтерфейсу, які відповідають семантиці HTML5 та є функціональними. Інтерфейс є адаптивним, тобто він розрахований як на комп'ютери, так і на мобільні пристрої. Це значно збільшує «юзабіліті» системи, адже на даному етапі розвитку інформаційних технологій та технологій загалом мобільні пристрої займають значний відсоток ринку. Мобільна версія сайту має повний функціонал і приємний зовнішній вигляд. Також слід зазначити, що дизайн сайту розроблений згідно зі стандартами Material Design.

Розроблена система розрахована на досить широку аудиторію, тому система реєстрації\входу вкрай необхідна. Розглянемо структуру таблиці, яка відповідає за користувачів. Набір полів для даної таблиці є досить стандартним:

- id – поле автоінкременту;
- name – ім'я користувача (логін);
- email – електронна пошта, яка буде використуватись для ідентифікації користувача, поле є первинним ключем;
- password – пароль користувача;
- rememberToker – запам'ятати користувача при вході, чи ні;
- timestamps – час створення та редагування інформації про користувача.

Процес тестування відбувається в декілька етапів. Спочатку необхідно додати тест в базу. Таку можливість надає адмін-панель, доступ до якої мають лише користувачі, що мають роль «Admin». Для того, шоб додати тест, необхідно вказати наступну інформацію: назва тесту, дата початку та закінчення та короткі відомості про тест. Після того, як тест було додано, необхідно додати питання, котрі входять до даного тесту. Адмін-панель має зручний та функціональний інтерфейс для цієї задачі. Після того, як питання до тесту було складено та додано, необхідно зберегти тест. Далі необхідно зберегти тест, і він буде записаний в базу даних.

Для контролю прав користувачів використовується інструмент Middleware, який надається фреймворком Laravel «з коробки». Наприклад, для доступу до адмін-панелі використовується наступний middleware:

```
public function handle($request, Closure $next)
   {
      if(!Auth::user()->hasRole('admin'))
         return redirect('/');
      return $next($request);
   }
```

Тут відбувається перевірка ролі авторизованого користувача – якщо користувач, який намагається отримати доступ до адмін-панелі, не є адміністратором сервісу, тобто не має ролі 'admin', то він перенаправляється на головну сторінку сервісу. Для цих цілей було створено дві допоміжні таблиці в базі даних, а саме таблиці 'roles', 'permissions', 'role_permission' та 'role_user'. Таблиця 'roles' має наступну структуру:

- id – поле автоінкременту;
- name – ім'я ролі, яке використовується у middleware;
- display_name – ім'я ролі для відображення;
- description – коротка характеристика ролі;
- timestamps – час створення та редагування ролі.

Дана таблиця містить в собі всі ролі, передбачені системою.

Наступна таблиця – role_user, являється зв'язуючою таблицею (pivot table)

для таблиць 'roles' та 'users'. Вона має наступну структуру:

- user_id – ідентифікатор користувача;

- role_id – ідентифікатор ролі.

Дана таблиця відповідає за призначення ролей користувачам.

Наступна таблиця – таблиця ‘permissions’, містить в собі дозволи для користувачів. Вона має таку структуру:

- id – поле автоінкременту;
- name – ім’я дозволу;
- display_name – ім’я дозволу для відображення;
- description – коротка характеристика дозволу;
- timestamps – час створення та редагування.

Таблиця ‘permission_role’ має наступну структуру:

- user_id – ідентифікатор користувача;
- role_id – ідентифікатор ролі.

Дана таблиця відповідає за призначення дозволів певним ролям.

Зі сторони користувача, для проходження навчання та тестування необхідно спочатку пройти процес реєстрації, так як незареєстровані користувачі не мають доступу до онлайн-навчання. Процес реєстрації є стандартним: користувачеві пропонується ввести і’мя, електронну адресу, та пароль з підтвердженням. Після перевірки введених даних на коректність (процес валідації даних) відбувається реєстрація користувача. Також користувач має можливість відновити пароль, у випадку його втрати.

Можливість проходити навчання та тестування мають лише авторизовані користувачі. Авторизований користувач має доступ до відкритих на даний момент курсів та тестів. Контент має статус «відкритого», якщо він є доступним в даний час, тобто дата початку курсу/тесту менша, від теперішньої, і дата закінчення більша, від теперішньої. Також при виведенні доступних курсів/тестів відбувається перевірка, чи було вже пройдено вказаним користувачем даний курс/тест, відповідно до чого і відбувається виведення доступних до проходження курсів/тестів. Загалом, умова, яка відбирає доступні курси/тести має наступний вигляд:

```
$tests = DB::table('test_user')->where('user_id', 1)->lists('test_id');
  $now = Carbon::now();
  $query->where('ends_at', '>=', $now)
      ->where('starts_at', '<=', $now)
      ->whereNotIn('id', $tests);
```

Таблиця, в якій містяця результати проведених тестувань має структуру:

- user_id – ідентифікатор користувача;
- test_id – ідентифікатор тесту;
- mark – кількість правильних відповідей;
- timestamps – дата проходження тесту.

Таблиця, яка містить в собі всі тести має наступну структуру:

- id – поле автоінкременту;
- name – ім’я тесту;
- description – текстове поле, в якому міститься коротка характеристика;
- starts_at – дата початку тесту;
- ends_at – дата закінчення тесту.

Два останні поля в таблиці призначені для визначення доступності тесту станом на конкретний момент у часі.

Питання, які входять до тесту містяться в таблиці ‘questions’. Таблиця має наступну структуру:

- id – поле автоінкременту;
- test_id – зовнішній ключ для зв’язку питання з відповідним тестом;
- question – текстове поле, в якому міститься текст запитання;
- answers – варіанти відповідей;
- answer – вірна відповідь на запитання.

Варіанти відповідей зберігаються у форматі serialized масиву. Перевагою такого підходу є те, що він не потребує додаткових полів у базі даних. Це зберігає місце на дисковому просторі серверу та зменшує навантаження на сам сервер. Рядок, який містить варіанти відповідей має наступний формат:

a:4:{i:0;s:2:"aa";i:1;s:2:"bb";i:2;s:6:"aabbss";i:3;s:2:"ss";}

Після того, як користувачем було обрано тест зі списку доступних, розпочинається безпосередньо процес тестування. Процес тестування підпорядковується наступній логіці: після початку тестування користувачеві виводиться запитання, варіанти відповіді на нього та таймер. Кількість варіантів може змінюватись від запитання до запитання – це залежить від структури питань. В таймері вказано час, який відведено на дане запитання. Користувач повинен відповісти на поставлене запитання за відповідний час. Якщо відповіді не було отримано, вважається, що відповідь була хибною. Таймер має візуальне графічне відображення відведеного часу та веде зворотній відлік в секундах. Якщо ж користувач встиг дати відповідь на поставлене запитання за відведений час, він має можливість дізнатись, чи правильною була його відповідь за допомогою можливостей інтерфейсу – якщо відповідь була правильною – вона набуває зеленого кольору, якщо відповідь була хибною – червного. Також, якщо користувач дав неправильну відповідь він має змогу дізнатись, яка відповідь була вірною.

Після того, як користувач відповів на всі запитання, йому виводиться результат у форматі «кількість вірних відповідей \ кількість запитань». Результат має індикацію кольором, а саме: якщо користувач дав менше 30% правильних відповідей – результат виводиться червоним кольором, якщо користувач здобув від 30% до 60% правильних відповідей – результат виводиться помаранчевим кольором, якщо більше 60% – зеленим. Таким чином, користувач має змогу дізнатись, якого результату він досягнув при проходженні даного тесту.

Також система включає в себе модуль збору статистики. Статистична інформація формується на основі проведених тестів. Після того, як певний тест було пройдено групою користувачів здійснюється вибірка даних, на основі яких буде сформовано статистичний звіт. Сформований звіт буде включати в себе загальну інформацію, а саме: відсоток успішності, середній бал, середній час проходження тесту, відсоток явки і т.і. Загальна статистична інформація буде відображатись в адмін-панелі. Користувач також матиме доступ до статистики, але дещо іншого формату. Статистика для користуввача буде представляти собою наступне: перелік пройдених тестів, кількість набраних балів з кожного тесту та дата проходження.

При створенні нового тесту передбачено механізм підрахунку часу, який необхідний для відповіді на запитання. Далі будуть описані основні принципи вищезазначеного алгоритму. Базовий час, який встановлюється при створенні запитаня складає 9 секунд. Кожен варіант відповіді на запитання додає 4 секунди до базового часу. Також на час впливає характер запитання, а саме кількість слів у питанні, наявність формул та\або зображень.

Для реалізації програмного забезпечення було обрано PHP-фреймворк Laravel версії 5.1. Вибір пав саме на цей фреймворк з декількох причин:

- відкритий код, що знаходиться в репозиторії на github;
- велике мультинаціональне ком’юніті, до якого можна звернутись за допомогою з будь-якого питання;
- відповідність всім шаблонам проектування (MVC, ActiveRecord, Facade, Repository і т.д);
- зручність розробки.

Laravel підтримує наступний функціонал:

- Пакети (англ. Packages) – дозволяють створювати і підключати модулі в форматі Composer до додатка на Laravel.
- Eloquent ORM – реалізація шаблону проектування ActiveRecord на PHP.

Дозволяє строго визначити відносини між об'єктами бази даних. Стандартний для Laravel інструмент для побудови запитів Fluent підтримується ядром Eloquent.

- Логіка додатку – частина розроблюваного додатку, оголошена або за допомогою контролерів, або маршрутів (функцій-замикань). Синтаксис оголошень схожий на синтаксис, використовуваний в каркасі Sinatra.
- Зворотня маршрутизація – пов'язує між собою посилання і маршрути, що генеруються додатком, дозволяючи змінювати останні з автоматичним оновленням пов'язаних посилань. При створенні посилань за допомогою іменованих маршрутів Laravel автоматично генерує кінцеві URL.
- REST-контролери – додатковий шар для розділення логіки обробки GET і POST-запитів HTTP.
- Автозавантаження класів – механізм автоматичного завантаження класів PHP без необхідності підключати файли їх визначень в include. Завантаження на вимогу запобігає завантаження непотрібних компонентів; завантажуються тільки ті з них, які дійсно використовуються.
- Укладачі уявлень (англ. View composers) – блоки коду, які виконуються при генерації подання (шаблону).
- Інверсія управління (англ. Inversion of Control) – дозволяє отримувати екземпляри об'єктів за принципом зворотного управління. Також може використовуватися для створення та отримання об'єктів-одинаків (англ. Singleton).
- Міграції – система управління версіями для баз даних. Дозволяє зв'язувати зміни в коді програми зі змінами, які потрібно внести в структуру БД, що спрощує розгортання і оновлення програми.
- Модульне тестування (юніт-тести) – відіграє дуже велику роль в Laravel, який сам по собі містить велике число тестів для запобігання регресій (помилок внаслідок поновлення коду або виправлення інших помилок).
- Сторінкове виведення (англ. Pagination) – спрощує генерацію сторінок, замінюючи різні способи вирішення цієї задачі єдиним механізмом, вбудованим в Laravel.

Laravel відповідає за back-end, тобто за логіку програмного забезпечення. Front-end частина виконана за допомогою комбінації наступних інструментів: Javascript, включаючи бібліотеку jQuery та UI-фреймворк Bootstrap 3.

Bootstrap – вільний набір інструментів для створення сайтів і веб-додатків. Включає в себе HTML і CSS шаблони оформлення для типографіки, веб-форм, кнопок, міток, блоків навігації і інших компонентів веб-інтерфейсів, включаючи JavaScript розширення. Bootstrap використовує найсучасніші напрацювання в галузі CSS і HTML.

Даний фреймворк було обрано з ряду причин, а саме:

- Економія часу – Bootstrap дозволяє заощадити час і зусилля, використовуючи шаблони дизайну і класи, і сконцентруватися на інших розробках;
- Висока швидкість – динамічні макети Bootstrap масштабуються на різні пристрої і розширення екрану без будь-яких змін в розмітці;
- Гармонійний дизайн – всі компоненти платформи Bootstrap використовують єдиний стиль і шаблони за допомогою центральної бібліотеки. Дизайн і макети веб-сторінок узгоджуються один з одним;
- Простота у використанні – платформа проста у використанні, користувач з базовими знаннями HTML і CSS може почати розробку з Bootstrap;
- Сумісність з браузерами – Bootstrap сумісний з Mozilla Firefox, Google Chrome, Safari, Internet Explorer і Opera;
- Відкрите програмне забезпечення – особливість Bootstrap, яка передбачає зручність використання, за допомогою відкритості вихідних кодів і безкоштовного завантаження.

Bootstrap надає наступний інструментарій для розробника:

- Сітки – заздалегідь задані розміри колонок, які можна відразу ж

використовувати, наприклад ширина колонки 140px відноситься до класу .span2 (.col-md-2 в третій версії фреймворку), який можна використовувати в CSS описі документа;

- Шаблони – фіксований або гумовий шаблон документа;
- Типографіка – описи шрифтів, визначення деяких класів для шрифтів, таких як код, цитати і т.і;
- Медіа – надає інструментарій для управління зображеннями і відео;
- Таблиці – засоби оформлення таблиць;
- Форми – класи для оформлення форм і деяких подій, що відбуваються з ними;
- Навігація – класи оформлення для табів, вкладок, меню і тулбару;

Алерт – оформлення діалогових вікон, підказок і спливаючих вікон.

Розробка структурної схеми

Структурна схема сайту – це сукупність об'єктів, частин сайту та взаємозв'язки між ними. Вона призначена для відображення загальної структури сайту, тобто його основних блоків, вузлів, частин та головних звя'зків між ними.

Структурну схему розроблюваного сайту зображено на рисунку 2.

Рисунок 2 – Структурна схема розроблюваного сайту

Зі схеми можна побачити, що сайт має головну сторінку з якої користувач може перейти до сторінки реєстрації/авторизації, відновлення паролю, сторінки "Про нас", сторінки контактів, сторінки списку курсів та тестів, профілю користувача та до сторінки адміністративної панелі. Також на головній сторінці користувач може авторизуватись або вийти зі свого акаунта.

Адмінпанель надає необхідний функціонал для перегляду та редагування інформації про існуючі курси, тести та зареєстрованих користувачів. Також адмінпанель надає можливості для видалення та створення нових курсів та тестів. Адмінпанель містить функціонал для роботи з користувачами системи, зокрема, редагування прав доступу користувачів, перегляд їх статистики та перегляд результатів пройдених тестів. Також безпосередньо з адмінпанелі можна запустити нові курси та тести.

Висновок. У статті розглянуто та проаналізовано програмне забезпечення, яке призначено для реалізації системи управління веб-сайтом онлайн-курсів. Виходячи з поставленої в даній роботі мети було досягнуто: розглянуто та проаналізовано існуючі на даний момент рішення в області дистанційного навчання та дистанційного тестування; реалізовано задачу розробки системи управління веб-сайтом онлайн-курсів; реалізовано задачу визначення прогресу користувача системи; створено простий інтуїтивно зрозумілий

інтерфейс вітчизняної програми для системи управління веб-сайтом онлайн-курсів. При створені програмного забезпечення було використано об'єктно-орієнтований підхід, що відповідає сучасним тенденціям у галузі розробки комерційних програмних систем. Програмне забезпечення реалізоване на мові програмування PHP. Дана мова програмування дозволяє найбільш ефективно обробляти дані, що використовуються у розробленому програмному забезпеченні. Це дозволило мінімізувати строк розробки програмного забезпечення, і, як наслідок, зменшити витрати на його розробку. Розроблена програма призначена для виконання під управлінням багатозадачної операційної системи Windows 7/8/10. Даються необхідні рекомендації з роботи з системою. Для підвищення рівня безпеки запропоновано застосовувати алгоритм MD5.

Список літератури

1. Приемы объектно-ориентированного проектирования, из-во "ДМК", 376 стр., 2011р.
2. Регулярные выражения. 3-е издание, из-во "Символ-Плюс", 608 стр., 2008р.
3. Разгони свой сайт. Методы клиентской оптимизации веб-страниц. Николай Мациевский, 264 стр., 2009р.
4. JavaScript. Подробное руководство, 5-е издание, из-во "Символ-Плюс", 992 стр., 2009р.
5. jQuery. Подробное руководство по продвинутому JavaScript, 2-е издание, из-во "Символ-Плюс", 624 стр., 2011р.
6. PHP 5, из-во "BHV-СПб", 1104 стр., 2008р.
7. HTML и XHTML. Подробное руководство, из-во "Символ-Плюс", 752 стр., 2012р.
8. CSS – каскадные таблицы стилей. Подробное руководство, 2-е издание, из-во "Символ-Плюс", 576 стр., 2005р.
9. "Алан Купер об интерфейсе. Основы проектирования взаимодействия", из-во "Символ-Плюс", 688 стр.
10. Атаманюк В. Г.,Ширшев О.Г., Акімов М. І, Громадянська оборона. Підручник для вузів М., 1986р.

УДК 004

О. Іванченко, магістр гр. КІ-18М-1,4
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ УПРАВЛІННЯ КОМПЛЕКСУ РІШЕНЬ «РОЗУМНИЙ ДІМ»

У статті розроблено програмне забезпечення, яке призначено для системи управління «Розумний будинок». Метою розробки є дослідження та програмна реалізація системи управління «Розумний будинок». Об'єктом дослідження є процес забезпечення управління розумним будинком. Предметом дослідження є методи реалізації систем управління розумним будинком. Методи дослідження базуються на методах теорії інформації, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи управління розумним будинком. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення. Розроблено зручний інтерфейс користувача. Наведені інструкції по роботі з програмними засобами. Програма може використовуватися на ПЕОМ архітектури IBM PC з ОС Windows XP/Vista/7/8/10. Програму розроблено в середовищі C++.

комп'ютерна інженерія, Smart Home, Arduino

Постановка проблеми. Будинок, в якому самі по собі відкриваються двері, включаються побутові прилади, регулюється температура і засуваються жалюзі, схожий на кадр з фільму про далеке майбутнє. Однак майбутнє набагато ближче, ніж нам здається. Система «розумний будинок» дозволяє повною мірою відчути блага технічного прогресу і позбавляє людину від вирішення безлічі побутових завдань. Вперше поняття «розумний будинок» з'явилося в 50-х роках минулого століття. Прародителькою системи, здатної

контролювати обстановку в цілому будинку, є технологія Java. Розробники цієї технології намагалися впровадити її в побутові прилади, тим самим зробивши їх більш «інтелектуальними».

Наприклад, вже в той час почали з'являтися перші вбудовуванні мікрохвильові печі, кондиціонери, здатні регулювати мікроклімат приміщення залежно від погоди за вікном і т. д.

Можливості системи «розумний будинок» багатогранні. Наприклад, щоб запобігти ймовірність пограбування, коли в будинку нікого немає, система імітує присутність господаря шляхом керування жалюзі, включення/вимикання світла і т. д. Якщо ж зловмисники все ж проникають всередину приміщення чи відбувається інша екстраординарна ситуація, система миттєво сповіщає про це господаря. Крім того, технологія «розумний будинок» дозволяє структурувати роботу всього технічного та інженерного обладнання, задавши йому певний сценарій.

Наприклад, перед вашим пробудженням система нагріє підлоги у ванній кімнаті, включить музичний центр, налаштує роботу кондиціонера на задану температуру, відрегулює оптимальну вологість в приміщенні і вирішить безліч інших побутових завдань.

«Розумний будинок» – це високотехнологічна система, яка може об'єднати всі комунікації вашого дому, і керувати ними одним натисканням кнопки. Освітлення, опалення, сигналізація, відеоспостереження – це далеко не всі системи, якими можна керувати з допомогою «розумного будинку».

Система керування світлом дає змогу запрограмувати світлові сцени у вашому будинку, чи створити видимість присутності господаря вдома під час його відпочинку в іншій країні. Система керування опаленням легко підтримуватиме задану температуру в цілому приміщенні або в окремих кімнатах, понижуючи її чи піднімаючи у відповідності до заданих параметрів.

Головна відмінність "розумного" будинку від просто житла, набитого сучасною технікою, полягає в тому, що в "розумному" будинку усі його пристрої об'єднані в єдину мережу і управляються спеціальним програмним забезпеченням.

У такому будинку в єдиній зв'язці працюють опалення, освітлення, водопровід, сигналізація, пральна машинка, холодильник, мікрохвильова піч, кавоварка і всі інші пристрої, які є в будинку. Наприклад, в "розумному" будинку можна налаштувати автоматичне включення опалення, якщо температура в квартирі, наприклад, впала нижче 18 градусів. Або можна задати автоматичне включення верхнього освітлення після 16 години на кухні.

Деякі елементи "розумного" будинку, наприклад, кавоварка, можуть спрацьовувати після сигналу зі смартфона, наприклад, якщо той відправив повідомлення, що господар вийшов з роботи і їде додому. А якщо раптом власники квартири затрималися на роботі і температура повітря прогрілася вище певного показника, "розумний" будинок відключить опалення і збереже таким чином ваші гроші. Друга відмінна риса "розумного" будинку - дистанційний контроль за подіями в ньому і віддалене керування будинком. Наприклад, спеціальний датчик повідомить власника про появу непрошених гостей, а камера покаже, чи дійсно в будинок пробралися зловмисники або це хтось із дітей загубив свої ключі. Датчики, встановлені в такому будинку, можуть реагувати не тільки на задимлення, але ще й на підвищену вологу, і блокувати надходження в будинок води, якщо раптом сталося затоплення.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні реалізації системи управління комплексу рішень «розумний дім».

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи управління розумним будинком.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем управління розумним будинком
– Дослідження системи систем управління розумним будинком
– Програмна реалізація системи управління розумним будинком

Об'єктом дослідження є процес управління розумним будинком.

Предметом дослідження є методи реалізації систем управління розумним будинком.

Методи дослідження базуються на методах теорії інформації, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Виходячи з теми роботи потрібно розробити програмне забезпечення системи управління для проекту «Розумний дім» та розробити саму автоматизовану систему управління з встановленням необхідних датчиків та ситем.

Система «розумний» дім може бути як і багато функціональною так і з обмеженням по функціоналу, для побудови можна використовувати як і мікроконтролери так і мікрокомп'ютери. В першому випадку функціонал системи може бути обмежений так як сучасні системи потребують великої обчислювальної потужності, яку не мають звичайні мікроконтролери, що не можна сказати про мікрокомп'ютери. Мікрокомп'ютери включають в себе окремий процесор, ОЗУ, відео процесор, що дасть можливість завантажити на такому пристрої навіть графічний інтерфейс або операційну систему, також мікрокомп'ютер має безліч портів та інтерфейсів вводу виводу даних.

Але в побудові системи на мікрокомп'ютері є й мінуси одним із яких є велика вартість та обслуговування такої системи. Що не можна сказати про використання мікроконтролерів для побудови тієї ж самої системи, ціна яких майже в половину менша.

Для побудови системи можна використовувати мікрокомп'ютери різних розробників таких як Raspberry PI, Orange PI, Banana PI, Latte Panda, навіть така відома фірма як Asus має свої однопалатні комп'ютери під назвою Asus Tinker Board. Якщо ж побудову робити на мікроконтролерах то в цьому випадку є також не мала кількість різних платформ для реалізації різних системи, прикладом є платформи STM, Arduino, Espruino, модулі ESP і безліч інших. Можлива навіть побудова системи з використанням поєднання мікрокомп'ютерів з мікроконтролерами.

В випадку побудови системи «розумний» дім потрібно також враховувати надійність платформ, їх стабільність в роботі, самостійність, автономність, енергоефективність та інші не менш важливі показники. Перед обранням платформ для розробки потрібно перш за все визначитись з функціоналом системи. Наприклад для забезпечення відеоспостереження одними контролерами не обійтись, тож потрібно застосовувати мікрокомп'ютер, що буде в змозі обробити відео потік з камер відеоспостереження і записувати їх на запам'ятовуючий пристрій.

Для побудови системи, що не потребує великого функціонала можна обрати мікроконтролери або платформи автоматизації побудовані на них. Тож я обрав за головний контролер, платформу від китайського виробника ESP8266, яка включає в себе достатній функціонал для розробки системи. Що стосується допоміжної периферії я обрав не менш відому платформу Arduino.

Базова концепція

Система управління являє собою сукупність апаратних та програмних засобів, які насамперед націлені на економічність, тобто на зниження можливих розходів (електроенергія, тепло) користувача, а також надає додаткові можливості, наприклад, контроль присутності. Розглянемо всі функції більш детально.

Розробка структурної схеми

Структурна схема системи – це сукупність об'єктів та частин та взаємозв'язки між ними. Призначенням структурної схеми є наглядне відображення складових частин розробляємої системи, її основних блоків, вузлів та взаємозв'язок між ними.

Структурна схема розробленої системи зображена на рисунку 3.1 . На ній показано структуру.

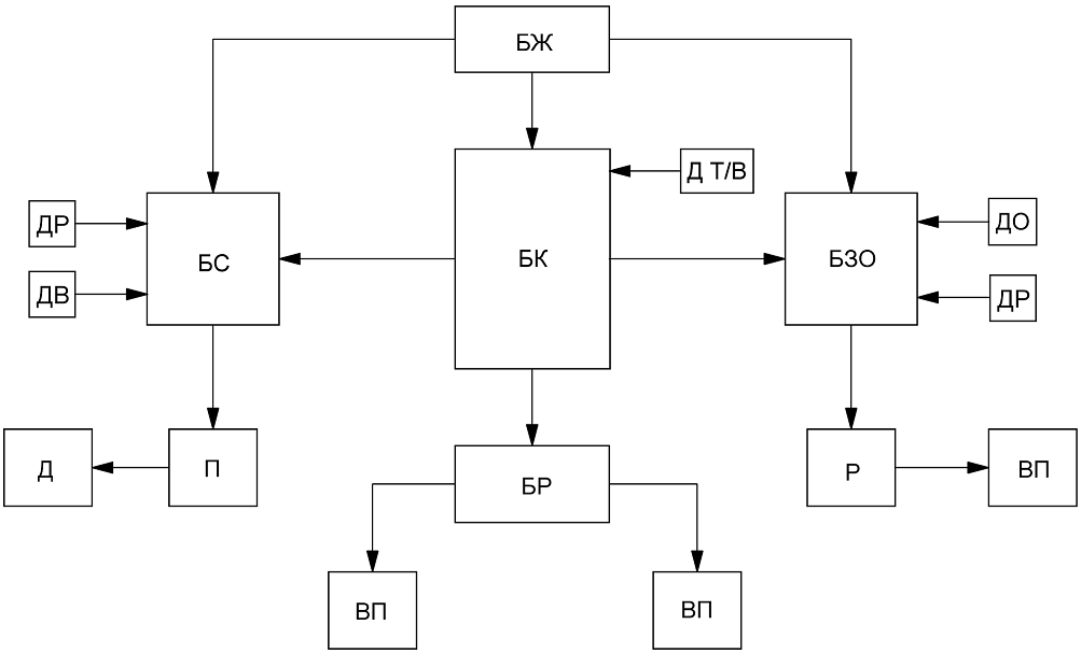


Рисунок 1 – Структурна схема системи «Розумний дім»

На схемі представленно:
БЖ- блок живлення
БК – блок контролю
БС – блок сигналізації
БЗО – блок зовнішнього освітлення
БР – блок реле
ДР – датчик руху
ДВ – датчик відкриття
ДО – датчик освітленності
Д Т\В – датчик температури та вологості
П – підсилювач
Д – динамік
ВП – виконавчий пристрій

Висновок. У статті розглянуто та проаналізовано програмне забезпечення, яке призначено для системи управління комплексу рішень «розумний дім». В межах України в недостатній мірі представлені вітчизняні розробки в цій області. У роботі наведені теоретичне узагальнення й рішення наукового завдання дослідження методів реалізації систем управління для рішень «розумний дім». Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем управління комплексами «розумний дім»; Досліджена система управління «розумний будинок» на основі комплексу рішень arduino; На основі отриманих результатів досліджень створена програмна реалізація для системи управління розумним будинком. Розроблені під час виконання роботи алгоритми дозволяють успішно вирішувати завдання управління системою «розумний дім». Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки. Розроблене програмне забезпечення має простий, дружній та зручний інтерфейс користувача, що забезпечує легкість у освоєнні роботи програмного продукту, зручність у використанні, і не потребує особливих спеціальних знань. При створені програмного забезпечення було використано об’єктно-орієнтований підхід, що відповідає сучасним тенденціям у галузі розробки комерційних програмних систем. Програма реалізована на мові високого рівня С++

та PHP. Дана мова програмування дозволяє найбільш ефективно обробляти дані. Це дозволило мінімізувати строк розробки програмного забезпечення, і, як слід, зменшити витрати на його розробку. Запропоноване програмне забезпечення ділиться на загальне програмне забезпечення, що поставляється із засобами обчислювальної техніки й спеціальне програмне забезпечення, що спеціально розроблене для даної конкретної системи й включає програми, що реалізують її функції. Програма призначена для виконання під управлінням багатозадачної операційної системи Windows XP/Vista/7/8/10 та системи Andorid. Для підвищення рівня безпеки запропоновано застосовувати BCrypt алгоритм та алгоритм crypt_blowfish. В цілому створене програмне забезпечення підтверджує правильність використаних проектних рішень та повністю відповідає вимогам технічного завдання. Створене програмне забезпечення має потенційну можливість для подальшого вдосконалення і застосування у різних галузях.

Список літератури

1. Смірнов О.А. Програмування комп'ютерних мереж. Основи HTML, CSS, JAVA-SCRIPT. Методичні вказівки. Кіровоград 2007–107 с.
2. Основы информационных и телекоммуникационных технологий: Книга 3: Сетевые информационные технологии. Автор: Попов В.Б.
3. Основы сетей передачи данных. Автор: Олифер В., Олифер Н.
4. Основы построения систем и сетей передачи информации. Учебное пособие для вузов. Автор: Щекотихин В.М., Шестак К.В., Михайлов А.И., Ломовицкий В.В.
5. Компьютерные сети и сетевые технологии. Автор: Спортак Марк.
6. Введение в сетевые технологии. Автор: Иртегов Д. В.
7. Сетевые технологии. Учебник-практикум. Автор: Л. Ф. Соловьева.
8. Информационные технологии. Автор: Б.Я. Советов, В.В. Цехановский.
9. Храмцов П.Б., Брик С.А., Русак А.М., Сурин А.И. Основы web-технологий БИНОМ. Лаборатория знаний, Интернет-университет информационных технологий - ИНТУИТ.ру, 2007.
10. Храмцов П.Б. Видеокурс: Введение в HTML и CSS (2 DVD) Интернет-университет информационных технологий - ИНТУИТ.ру, 2008

УДК 338.47

В. Капустеря, магістр гр. ОКД-19МЗ-1,4
Центральноукраїнський національний технічний університет

НАПРЯМКИ ПОЛІПШЕННЯ УПРАВЛІННЯ ВИРОБНИЧО-КОМЕРЦІЙНОЮ ДІЯЛЬНІСТЮ ПІДПРИЄМСТВА

Стаття присвячена дослідженню шляхів підвищення ефективності управління виробничо-комерційною діяльності підприємства, досліджено сутність поняття виробничо-комерційна діяльність, виявлено основні резерви підвищення її ефективності. Запропоновано стратегічні пріоритети розвитку виробничої та комерційної діяльності підприємств дорожньої галузі. Таким чином стаття має практичне значення для вітчизняних підприємств і містить вдосконалення теоретичних розробок з даного напрямку дослідження.
підприємство, дорожнє господарство, виробнича діяльність, комерційна діяльність

Постановка проблеми. Актуальність опрацювання теоретичних управління виробничо-комерційною діяльністю підприємств дорожньої галузі зумовлена необхідністю формування сучасних підходів до підвищення її ефективності. Сьогодні дорожнє господарство України є недостатньо розвиненим, що в свою чергу перешкоджає

відновленню економічної активності та виведення економіки України на траєкторію сталого зростання.

Тому дослідження питання ефективності управління виробничо-комерційною діяльності підприємства є актуальними з теоретичної і практичної точки зору.

Аналіз останніх досліджень і публікацій. Питання діяльності підприємств дорожнього господарства в сучасних умовах в Україні досліджують у своїх працях В. Семесько, В. Галушко, М. Дергаусов, С. Кулицький та інші.

Але, не дивлячись на значну кількість наукових праць, присвячених даній тематиці, питання удосконалення ефективності управління виробничо-комерційною діяльності підприємства України залишаються актуальними.

Мета статті. Метою написання даної статті є дослідження шляхів підвищення ефективності управління виробничо-комерційною діяльності підприємств дорожньої галузі України в сучасних умовах.

Виклад основного матеріалу. В Україні державну політику у сфері дорожнього господарства реалізує Державне агентство автомобільних доріг України (Укравтодор), діяльність якого спрямовується і координується Кабінетом Міністрів України через Міністра інфраструктури. Завданнями головного розпорядника є організація будівництва, реконструкції, ремонту й утримання автомобільних доріг загального користування, розробка пропозицій щодо формування державної економічної, науково-технічної, інноваційної, інвестиційної, кадрової, соціальної та зовнішньоекономічної політики у сфері дорожнього господарства, своєчасне виконання боргових зобов'язань за запозиченнями, підготовка й організація виконання державних програм розбудови транспортних коридорів та технологічне оновлення дорожнього господарства шляхом розроблення та впровадження сучасних технологій, обладнання та устаткування.

У 2020 році планується залучити до ремонтно-будівельних робіт 4000 км, для забезпечення цього масштабного проєкту передбачено фінансування в обсязі більше 60 млрд грн. Процес управління передбачає нульову терпимість до корупції та впровадження сучасних світових практик. Потрібно зауважити, що сьогодні наявна система управління дорожньою галуззю України має низку недоліків, основними з яких є зосередження всіх функцій з планування і організації ремонтно-будівельних робіт на місцевих дорогах в Укравтодорі; суміщення критичних повноважень (замовник – виконавець – контролер); фактична монополізація ринку робіт з експлуатаційного утримання автомобільних доріг загального користування державною компанією акціонерне товариство «ДАК «Автомобільні дороги України»», що приводить до відсутності конкуренції; неврахування інтересів та пріоритетів соціально-економічного розвитку регіонів; відсутність можливості органам місцевого самоврядування впливати на планування ремонтно-будівельних робіт на місцевих дорогах.

Справедливо буде зазначити, що діяльність дорожнього підприємства буде безрезультатною, якщо вона не завершується тим, заради чого було створене підприємство, тобто якщо не досягається мета його діяльності. Ефективність виробничої та комерційної діяльності – найважливіша якісна характеристика господарювання на всіх рівнях. Під економічною ефективністю виробництва розуміється ступінь використання виробничого потенціалу, що виявляється співвідношенням результатів і витрат суспільного виробництва. Чим вище результат при тих же витратах, чим швидше він зростає в розрахунку на одиницю витрат суспільно необхідної праці, або чим менше витрат на одиницю корисного ефекту, тим вищою є ефективність виробництва.

Ефективність виробничої діяльності – це показник діяльності виробництва по розподілу й переробці ресурсів із метою виробництва товарів, який визначається як відношення результатів на виході до ресурсів на вході або через обсяги випуску продукції, її номенклатури. Характер, зміст і спрямованість діяльності дорожнього підприємства визначаються збалансованістю інтересів безпосередніх учасників процесу стратегічного управління, що знаходить своє відображення у вигляді певної місії і цілей. При цьому,

перший крок полягає у формулюванні місії, яка є засобом вираження сутності існування підприємства, його призначення та має свою оригінальність і особливе значення для працівників.

Через те, що перед підприємством майже щоденно постають усе нові й нові завдання, життєвий цикл місії завжди обмежений у часі. Аналіз середовища забезпечує базу для вироблення стратегії та дозволяє підприємству здійснити свою місію і досягти своїх цілей. Аналіз зовнішнього середовища спрямований на з'ясування перспективних позитивних результатів, що можуть бути досягнуті підприємством у випадку успішного виконання стратегічних дій та прогнозування можливих ускладнень в результаті невизначеності зовнішніх факторів. Аналіз включає вивчення впливу економічної, правової, політичної, екологічної, соціальної, науково-технічної й технологічної складових суспільства на стан розвитку підприємств дорожньої галузі країни загалом. Аналіз внутрішнього середовища розкриває конкурентний потенціал дорожнього підприємства, що є дієвим у процесі досягнення визначених цілей, і проводиться за такими напрямами: організація управління; характеристика процесу виробництва; рівень інноваційного потенціалу; рівень кадрового потенціалу; фінанси; маркетинг; організаційна культура тощо.

Позитивним моментом, що позначиться на виробничій та комерційні діяльності дорожніх підприємств є представлення в «Укравтодорі» інтерактивної мапи, на якій можна буде залишати скарги про незадовільний стан доріг. Вона дозволить оперативно отримувати інформацію про ремонтні роботи. Для того, щоб залишити скаргу, користувача доріг потрібно завантажити фото проблеми на мапу з конкретною геолокацією.

На жаль, у 2019 році відзначалися випадки вандалізму на автомобільних дорогах державного значення, що загрожує безпеці дорожнього руху. Впродовж року час від часу дорожники області фіксували випадки крадіжок засобів організації дорожньої обстановки: бар'єрного огородження, стійок, компенсаторів, дорожніх знаків.

Забезпечення розвитку підприємств дорожнього господарства не можливо без наявності та впровадження ефективного механізму реформування означеної сфери. Такий механізм присутній та реалізується за чітко сформованою «дорожньою картою». За останні два роки спостерігається позитивна тенденція щодо збільшення обсягів фінансування дорожніх робіт і це наслідок створення цільового Дорожнього фонду, який має прогресивну структуру доходів і видатків. Крім того, наповнюваність фонду покращилася також за рахунок залучення коштів міжнародних інвестиційних інституцій під гарантії, надані державою. Спостерігається нарощування обсягів робіт з будівництва та ремонту автомобільних доріг з боку дорожніх підприємств для усіх рівнів замовників, що свідчить про поступовий перехід дорожнього господарства до стабільного фінансування будівництва та утримання автомобільних доріг у середньо- та довгостроковій перспективі.

Висновки. Оптимальне поєднання виробничої, комерційної та інноваційної діяльності дає змогу не лише постійно вдосконалювати виробничий процес і продукцію, а й діяти на випередження, виявляти нові перспективні напрями чи форми бізнесу, диверсифікувати (поєднувати багато видів) діяльність з метою задоволення нових суспільних потреб. Однак пошук напрямів сучасних змін має бути системним. Тільки шляхом цілеспрямованого і організованого аналізу можливостей, які надає середовище господарювання, своєчасного і обґрунтованого залучення економічно вигідних для підприємств нововведень можна постійно поліпшувати їх діяльність, підвищувати престиж і конкурентоспроможність.

Список літератури

1. Закон України «Про концесії на будівництво та експлуатацію автомобільних доріг» / Верховна Рада України. [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/1286-14.
2. Закон України «Про автомобільні дороги» / Верховна Рада України. [Електронний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/2862-15

3. Безуглий А.О., Ілляш С.І., Печончик Т.І. Організаційно-економічні аспекти ефективного використання фінансових ресурсів в дорожньому господарстві. Дороги і мости : зб. наукових праць / [А.О. Безуглий, С.І. Ілляш, Т.І. Печончик]. – К. : ДП «ДерждорНДІ». – 2011. – Вип. 13. – С. 25–28.
4. Галушко В.О. Проблеми та перспективи розвитку дорожньої галузі / В.О. Галушко // Дорожня галузь України. – 2011. – № 2. – С. 12-15.
5. Дергаусов М. Особливості транспортної політики в Україні при її адаптації на міжнародних ринках // http://www.vesna.org.ua.
6. Кулицький С. Проблеми розвитку мережі автомобільних доріг в Україні [Електронний ресурс] / С. Кулицький // Україна: події, факти, коментарі. – 2017. – № 22. – С. 56–65. – Режим доступу: http://nbuviap.gov.ua/images/ukraine/2017/ukr22.pdf. – Назва з екрану.
7. Луцкін Є. С., Серьогіна Н. В. Основні проблеми та можливості розвитку дорожньо-транспортної інфраструктури України. Вісник ОДАБА. 2016. № 63. С. 223-229. : сайт. URL : http://mx.ogasa.org.ua/handle/123456789/2108 (дата звернення : 01.12.2019).
8. Солодовнік О. О. Розвиток дорожнього господарства України у посткризовому періоді. Причорноморські економічні студії. 2017. Випуск 23. С. 55-59.: сайт. URL : http://bses.in.ua/journals/2017/23_2017/12.pdf (дата звернення : 01.06.2020).
9. Семесько В. М. Аутсорсинг і перспективи розвитку транспортної логістики / В.М. Семесько // Економіка та держава. – 2006. – №1. – С. 57–59.

УДК 336.7

Ю. Кирилюк, магістр гр. ФС-18М
Центральноукраїнський національний технічний університет

ОЦІНКА ЕФЕКТИВНОСТІ УПРАВЛІННЯ КРЕДИТНИМ ПОРТФЕЛЕМ КОМЕРЦІЙНОГО БАНКУ (НА ПРИКЛАДІ АТ КБ «ПРИВАТБАНК»)

У статті досліджено сутність кредитного портфелю комерційного банку. Проаналізовано кредитну діяльність АТ КБ «ПриватБанк» за 2014-2018 рр. Розглянуто процес управління кредитним портфелем банку. Наведені методи мінімізації кредитного ризику.
оцінка управління кредитним портфелем, кредитний портфель, кредитний ризик, дохід, ліквідність, ефективність

Актуальність теми. На сьогоднішній день в Україні спостерігається тенденція зростання загального обсягу простроченої заборгованості за кредитами банків, що є однією з проблем банківської системи. Така ситуація обумовлена тим, що кожен банк має свій механізм формування та управління кредитним портфелем, не всі фахівці якісно оцінюють кредитний ризик. Не дивлячись на те, що кредитний портфель виступає одним із найризикованіших напрямків банківської діяльності, він є одним із головних складових елементів у структурі відсоткових доходів. Тому, успішне кредитування залежить від повернення наданих позичок, банки повинні упровадити ефективну систему управління кредитним портфелем комерційного банку.

Постановка завдання. Метою статті є розкриття сутності кредитного портфеля комерційного банку та оцінка ефективності управління ним.

Виходячи з поставленої мети, були сформовані наступні завдання:

- дослідити сутність кредитного портфеля комерційного банку;
- проаналізувати кредитну діяльність АТ КБ «ПриватБанк»;
- розглянути методи управління кредитним ризиком.

Виклад основного матеріалу. Кредитний портфель комерційного банку відіграє важливу роль в банківській діяльності і являє собою сукупність усіх банківських кредитів та позичок (яка супроводжується певним рівнем ризику) сформовану з метою одержання

доходу. Особливу увагу в управлінні кредитним портфелем банку слід звертати на вибір кредитної політики (яка дає смогу планувати, регулювати, контролювати та раціонально організовувати взаємовідносини між кредитором і позичальником) та кредитні ризики (являють собою ступінь ймовірності настання небажаних подій та при правильному управлінні ними можуть стимулювати і спрямовувати до пошуку нових рішень проблеми, та підштовхувати для створення резервів).

Згідно із Положенням НБУ «Про порядок формування та використання банками України резервів для відшкодування можливих втрат за активними банківськими операціями» кредитний портфель – це сукупність усіх банківських позик, що структуровані за певними параметрами відповідно до завдань визначеної банком кредитної політики [3].

Л.О. Примостка пояснює, що кредитний портфель – це сукупність усіх кредитів, наданих банком для одержання доходів [2].

Свою думку має і Ю.В. Бугель: кредитний портфель – це сукупність наданих банком позичок, сформовану з метою отримання прийнятного рівня доходу та забезпечення платоспроможності банку при мінімальному рівні кредитного ризику [1].

Також сутність кредитного портфеля виражається і через його функції: розподільна та перерозподільна; функція заміщення грошових коштів кредитними операціями; функція мінімізації кредитного ризику; функція розширення та диверсифікації дохідної частини банку та підвищення його фінансової стійкості.

Тип сформованого портфеля є його характеристикою, яка базується на співвідношенні прибутку та ризику. Розрізняють три типи кредитного портфеля: портфель доходу, портфель ризику та збалансований портфель. Портфель доходу характеризується низьким рівнем прибутковості, оскільки ризики є мінімальними, відсотки виплачуються стабільно, тоді як у ризиковому портфелі рівень прибутку є вищим, однак й кредитні ризики є високими. Оскільки «дохідність» і «ризик» - це взаємопов’язані економічні категорії, оптимальним варіантом буде баланс між дохідністю та ризиком – збалансований кредитний портфель.

Також до характеристик кредитного портфеля відносять його розмір та структуру.

Розмір кредитного портфеля передбачає розмір всіх активно-пасивних операцій банку та оцінюється за балансовою вартістю всіх кредитів банку, у тому числі прострочених, пролонгованих, сумнівних.

Структура кредитного портфеля являє собою співвідношення певних видів кредитних операцій. Якщо питома вага кредитів без забезпечення (або прострочених, сумнівних, пролонгованих) складає не більше 50%, то така структура кредитного портфеля вважається задовільною.

Процес управління кредитним портфелем складається з декількох етапів:

- визначення видів кредитів і їх рівень ризику;
- аналіз структури портфеля;
- оцінка якості портфеля в цілому;
- виявлення та аналіз чинників, що впливають на структуру або якість портфеля;
- визначення розміру резерву, який необхідно створити для кредиту;
- визначення загальної суми резервів для загального ризику портфеля;
- розробка заходів, спрямованих на покращення якості портфеля.

Управління кредитним портфелем означає управління кредитними ризиками (можливість збалансовувати або мінімізувати ризик усього портфеля). В свою чергу, при управлінні кредитними ризиками доцільно проводити кількісний та якісний аналіз кредитного портфеля

За фінансовою звітністю АТ КБ «ПриватБанк» проаналізуємо кредитну діяльність за період 2014-2018 рр. (табл. 1).

Таблиця 1 Аналіз кредитної діяльності АТ КБ «ПриватБанк» за період 2014-2018 рр.

Показники	2014 р.	2015 р.	2016 р.	2017 р.	2018 р.
Кредити клієнтам, млн. грн.	159 173	189 314	32 616	38 335	50 140
Активи банку, млн. грн.	212 813	258 611	179 761	253 675	278 048
Питома вага кредитів в активах банку	74,8%	73,2%	18,1%	15,1%	18,0%

Джерело: [5]

Як бачимо з табл. 1, внаслідок націоналізації (вилучення з приватної власності у власність держави) кредитна діяльність ПриватБанку значно змінилась. Так, у 2016 р. порівняно з 2015 р. спостерігається зменшення кредитного портфеля на 156 698 млн. грн.

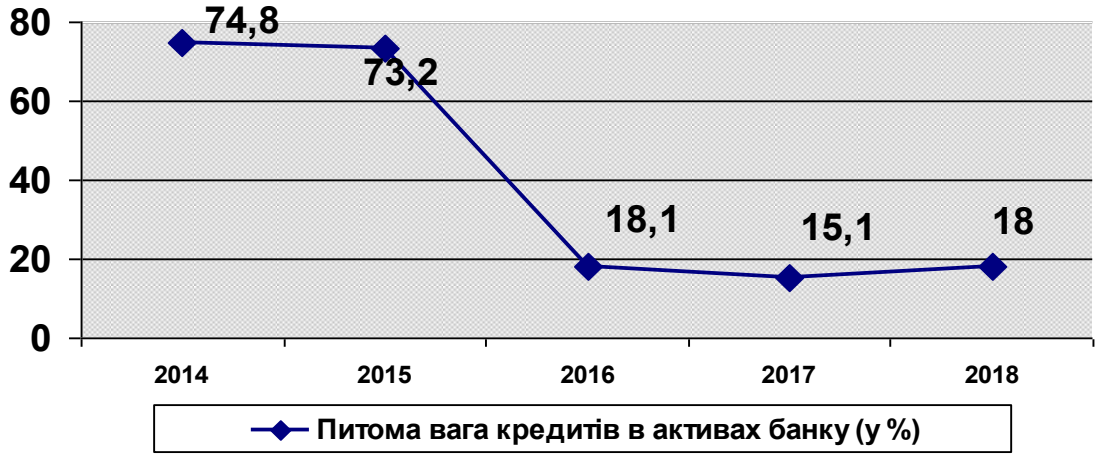


Рис. 1 – Динаміка кредитної діяльності АТ КБ «ПриватБанк» за період 2014-2018 рр.

Джерело: [5]

Неповернення кредитів позичальниками кредитору є однією із гостріших банківських проблем за останні роки. Проблемні кредити ПриватБанку негативно впливають на капітал банку.

Рис. 2 – Динаміка проблемної заборгованості АТ КБ «ПриватБанк» 2014-2018 рр.

Джерело: [5]

Як бачимо з рис. 2, найменша питома вага проблемних кредитів спостерігається в 2014 році – 5,5%. У 2015 р. питома вага непрацюючих кредитів становить 12,3%, але вже у 2016 р. даний показник зменшився на 3,84% (становив 8,46 %).

Однак вже у 2017 р. і 2018 р. можемо побачити негативну тенденцію зростання проблемних кредитів, питома вага яких становить 71,79% та 77,22% відповідно.

При цьому, рекомендований рівень проблемних кредитів має не перевищувати більше 5%.

Ефективність управління кредитним портфелем банку значною мірою залежить від управління ризиками. Оскільки повністю запобігти або ліквідувати кредитний ризик неможливо, банк повинен зосереджувати свою увагу щодо мінімізації ризику.

Багато науковців виділяють такі основні методи управління ризиками кредитного портфеля:

- диверсифікація кредитного портфеля – зменшення загального ризику портфеля, шляхом розміщення кредитів між позичальниками;
- концентрація кредитного портфеля – зосередження кредитних ресурсів у певних галузях економіки або кредитування певних категорій клієнтів, які мають однакові характеристики (наприклад, юридичний статус, обсяг валового доходу тощо) або на географічній території [4];
- лімітування (встановлення лімітів кредитування) – банк встановлює максимально допустимий розмір наданого кредиту чи позики або розмір всього кредитного портфеля в цілому;
- резервування (створення резервів) – створення резервних коштів для відшкодування можливих втрат (наприклад, при неповерненні кредиту) за кредитними операціями банку;
- страхування кредитних ризиків – процес передачі ризику неповернення кредиту банком страховій компанії;
- сек'юритизація – випуск цінних паперів, забезпечених грошовими потоками від певних активів.

Висновки. Отже від правильно обраної кредитної політики банку, від аналізу ринку кредитів, від грамотно сформованого кредитного портфеля та управління ним – залежить фінансовий успіх банківської установи, що, в свою чергу, впливає на банківську систему країни. Для запобігання фінансових втрат необхідно використовувати різні методи зниження рівня кредитних ризиків (які істотно впливають на якість кредитного портфеля), тим самим мінімізуючи їх.

Список літератури

1. Бугель Ю. Поняття кредитного портфеля комерційного банку та необхідність ефективного управління ним / Ю. Бугель // Світ фінансів. - 2011. - Вип. 2. - С. 98-107.
2. Примостка Л. О. Фінансовий менеджмент у банку: Підруч. – К.: КНЕУ, 2004. – 468 с.
3. Про порядок формування та використання резерву для відшкодування можливих втрат за кредитними операціями банків: Положення НБУ від 06.07.2000 р. № 279 [Електронний ресурс]. – Режим доступу: www.rada.gov.ua.
4. Онищенко В.О., Волкова Н.І. Методи управління кредитним портфелем банку – Економіка і регіон №5 (48) – 2014 – ПолтНТУ – 3-9 с.
5. Фінансова звітність Акціонерного Товариства КБ «Приватбанк» [Електронний ресурс]. – Режим доступу : https://privatbank.ua/about/fnansovaja-otchetnost/

УДК 004

О. Кислун, магістр гр. КН-18МЗ
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ ЗАХИСТУ ДАНИХ НА ОНОВІ ГЕНЕРАЦІЇ ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ

У статті розглянуто розроблене програмне забезпечення, яке призначено для захисту даних на основі генерації псевдовипадкових послідовностей. Метою роботи є дослідження та програмна реалізація системи захисту даних на основі генерації псевдовипадкових послідовностей. Об'єктом дослідження є процес захисту даних на основі генерації псевдовипадкових послідовностей. Предметом дослідження є методи захисту даних на основі генерації псевдовипадкових послідовностей. Методи дослідження базуються на методах захисту інформації, методах математичної статистики, методах розробки програмного забезпечення. - Результат роботи – програмна реалізація системи захисту даних на основі генерації псевдовипадкових послідовностей. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення. Розроблено зручний інтерфейс користувача. Наведені інструкції по роботі з програмними засобами.

комп'ютерна інженерія, захист даних, захист даних від несанкціонованого доступу

Постановка проблеми. На даний час значно виріс обсяг інформації, що зберігається в електронному вигляді, а отже, зросли й можливості, щодо одержання доступу до неї. Роботи, відповідно до інформації, яку зберігають в електронному вигляді, ведуться за таких основних напрямків: доступність, цілісність та конфіденційність. За класифікацією інформація поділяється на відкриту, конфіденційну та таємну. А оскільки значна частина інформації не призначена для публічного перегляду або навіть становить таємницю, то завдання обмеження доступу до інформації, що зберігається в електронному вигляді, є та буде актуальним.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини системи захисту даних на основі генерації псевдовипадкових послідовностей.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи захисту даних на основі генерації псевдовипадкових послідовностей.

Для досягнення поставленої мети визначена програма дослідження, що складається з таких завдань:

- Огляд існуючих систем захисту.
- Дослідження системи захисту даних на основі генерації псевдовипадкових послідовностей.
- Програмна реалізація системи захисту даних на основі генерації псевдовипадкових послідовностей.

Об'єктом дослідження є процес захисту даних на основі генерації псевдовипадкових послідовностей.

Предметом дослідження є методи захисту даних на основі генерації псевдовипадкових послідовностей.

Методи дослідження базуються на методах захисту інформації, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. По суті, робота системи захисту даних на основі генерації псевдовипадкових послідовностей зводиться до шифрування, тобто кодування визначеної послідовності (файла) для зберігання або передачі з подальшим відтворенням - розшифруванням (декодуванням). Послідовність кодується шляхом змішуванням з деякою псевдовипадковою послідовністю , що являє собою результат певного перетворення деякого ключа. Декодування проводиться шляхом виділення зашифрованої послідовності з суміші останньої та псевдовипадкової послідовності.Виходячи із зазначеного, система, що розробляється, має виконувати наступні операції:

- запуск програми та автентифіка́ція;
- вибір режиму роботи програми: шифрування інформації або дешифрування коду:
- для режимів шифрування та дешифрування, вибір методу шифрування , якщо такий наявний:
- для режимів шифрування та дешифрування, введення первинного ключа;
- для режимів шифрування та дешифрування, одержання шляхом перетворення первинного ключа псевдовипадкової послідовності для змішування;
- для режиму шифрування, вибір файла для кодування;
- для режиму дешифрування, вибір закодованого файла;
- дії для налагодження інтерфейсу програми: вибір кольорів, фонтів тощо, реалізована довідкова система з роботи для програмного забезпечення, що розробляється.

Розробка структурної схеми

Розгляд структури програми можливий з двох позицій: розгляд, як структурних одиниць програми самої Delphi або як описання зв'язків між різними структурними одиницями програми (структурні одиниці програми розглядаються в якості окремих частини - блоків,. що виконують різні функції) та проходженням інформаційних потоків через них. Будь-яка програма Delphi складається з файла проекту (файл з розширенням DPR) і одного чи кількох модулів (файли з розширенням PAS). Структурно модулі - це окремі програмні одиниці, що реалізують окремі частини програми. [37]. Тож для побудови програми скористаємося можливістю мінімального використання модулів - один модуль. Розглянемо структурну програму через призму виконання її з боку функції. Структурна схема системи зображена на рисунку 1.

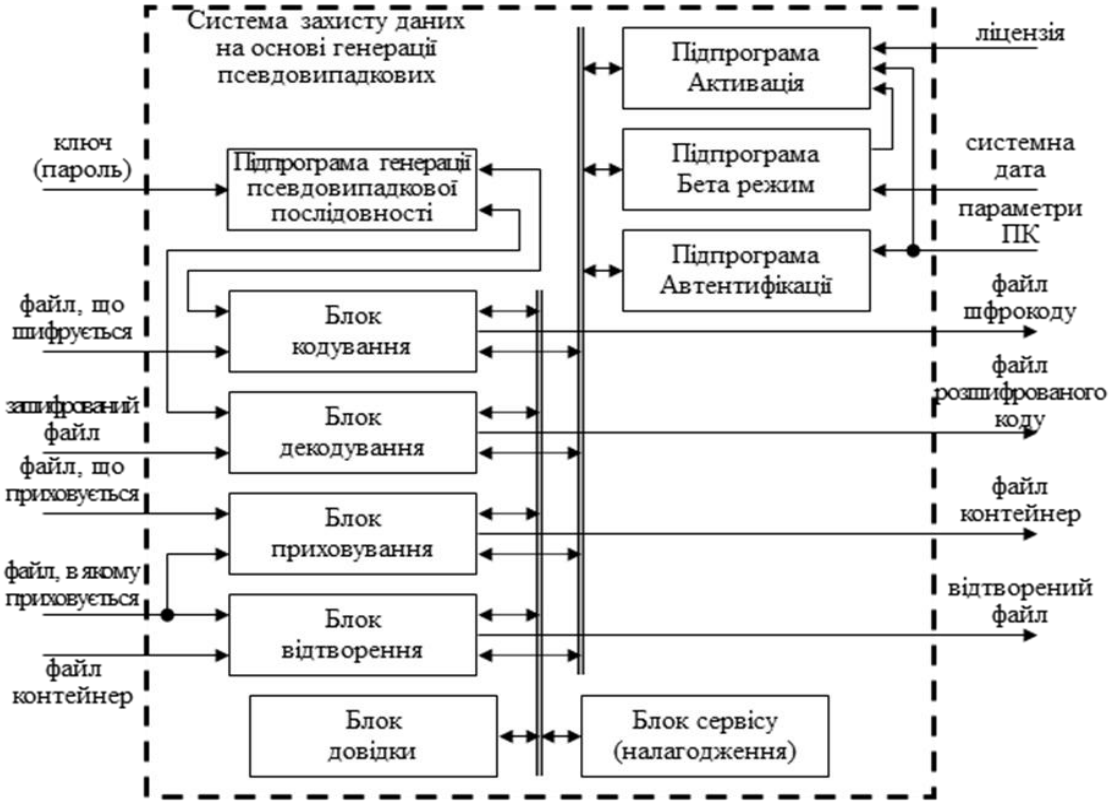


Рисунок 1 - Структурна схема

Зі схеми можна побачити, що до програми поступають наступні інформаційні потоки:

- ключ (пароль) - текстова послідовність, з якої генерується псевдовипадкова послідовність для режимів кодування та декодування;
- файл, що шифрується - вхідні дані для режиму кодування;
- зашифрований файл - вхідні дані для режиму декодування;
- файл, що приховується - вхідні дані для режиму приховування;
- контейнерний файл - вхідні дані для режиму відтворення;
- файл, у якому приховується - вхідні дані для режимів приховування та відтворення;
- ліцензія - дані для пропису активації програми;
- системна дата - дані для керування бета (демо) режимом;
- параметри ПК (за наших умов доцільно скористатися серійним номером диску) дані для керування Автентифікацією та прописом активації під конкретний ПК.

Також, із схеми можна побачити, що програма генерує наступні інформаційні потоки:

- файл шифрокоду - вихідні дані для режиму кодування;
- файл розшифрованого коду - вихідні дані для режиму декодування;
- файл контейнер - вихідні дані для режиму приховування;
- відтворений файл - вихідні дані для режиму відтворення.

На схемі також показані внутрішні інформаційні зв’язки:

- зв’язок між підпрограмою генерації псевдовипадкової послідовності і блоками режимів кодування та декодування, де по запиту блоків надходить потік псевдовипадкової послідовності;
- зв’язок між блоками режимів та блоками довідки і сервісу;
- зв’язок між блоками режимів і підпрограмами керування захистом: «Автентифікації», «Бета режим» та «Активація»;
- зв’язок між підпрограмами керування захистом: «Автентифікації» та «Активація».

Висновок. У статті розглянуто та проаналізовано програмне забезпечення, призначене для захисту даних на основі генерації псевдовипадкових послідовностей.У межах

України в недостатній мірі представлені вітчизняні розробки в цій галузі. У роботі наведено теоретичне узагальнення й вирішення наукового завдання дослідження методів захисту даних на основі генерації псевдовипадкових послідовностей. Вирішення даного завдання полягало у здійсненні наступних задач: досліджена система захисту даних на основі генерації псевдовипадкових послідовностей; на основі отриманих результатів досліджень створена програмна реалізація системи захисту даних на основі генерації псевдовипадкових послідовностей. Розроблені під час виконання роботи алгоритми дозволяють успішно вирішувати завдання захисту даних на основі генерації псевдовипадкових послідовностей. Проведено аналіз предметної галузі, в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудовано алгоритм і вибрано середовище розробки. Розроблене програмне забезпечення має простий, дружній та зручний інтерфейс користувача, що забезпечує легкість в освоєнні роботи програмного продукту, зручність у використанні, і не потребує особливих спеціальних знань. При створенні програмного забезпечення було використано об’єктно-орієнтований підхід, що відповідає сучасним тенденціям у галузі розробки комерційних програмних систем. Програма реалізована на мові високого рівня Delphi. Саме ця мова програмування дозволяє найбільш ефективно обробляти дані. Це дозволило мінімізувати строк розробки програмного забезпечення, і, як слід, зменшити витрати на його розробку. Запропоноване програмне забезпечення ділиться на загальне програмне забезпечення, що поставляється із засобами обчислювальної техніки, й спеціальне програмне забезпечення, що спеціально розроблене для даної конкретної системи й включає програми, що реалізують її функції.

Список літератури

1. Технології захисту інформації: підручник для студ. спеціальності 122 «Комп’ютерні науки», спеціалізацій «Інформаційні технології моніторингу довкілля», «Геометричне моделювання в інформаційних системах» / Ю. А. Тарнавський; КПІ ім. Ігоря Сікорського. - Київ : КПІ ім. Ігоря Сікорського, 2018. - 162 с.
2. Остапов С. Е. Технології захисту інформації: навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. - Х. : Вид. ХНЕУ, 2013. - 476 с.
3. Словари и энциклопедии на Академике [Електронний ресурс] -Режим доступу: https://people_and_cultures.academic.ru/462/Защита_данных
4. 500 лучших программ для Windows Уваров Сергей Сергеевич Шифрование данных [Електронний ресурс] - Режим доступу: https://it.wikireading.ru/42304
5. Приложение для шифрования данных. Программы, позволяющие надёжно зашифровать файлы и папки [Електронний ресурс] - Режим доступу: https://musfight.ru/igry/prilozhenie-dlya-shifrovaniya-dannyh-programmy-pozvolyayushchie-nad-zhno/
6. Программы для предотвращения несанкционированного доступа к информации [Електронний ресурс] - Режим доступу: - https://compress.ru/article.aspx?id=18759#Типы%20программ%20для%20несанкционированного%20доступа%20к%20данным
7. Порівняння можливостей шифрування архіваторів WinRar та WinZip [Електронний ресурс] - Режим доступу: https://studfile.net/preview/5470392/page:12/
8. Архіватори WinRar і WinZip[Електронний ресурс] - Режим доступу: http://pro-computer.pp.ua/5779-arhvatori-winrar-winzip.html
9. Security Software for Windows OS [Електронний ресурс] - Режим доступу: www.secureaction.com
10. Обзор Advanced Encryption Package [Електронний ресурс] - Режим доступу: https://soft.mydiv.net/win/download-Advanced-Encryption-Package.html

УДК 004

О. Коба, магістр гр. КН-18-1,4
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ ЗАХИСТУ ДАНИХ НА МОБІЛЬНИХ ПРИСТРОЯХ З ВИКОРИСТАННЯМ МАТРИЧНИХ ШТРИХ-КОДІВ

У статті розроблено програмне забезпечення, яке призначено для системи захисту даних на мобільних пристроях з використанням матричних штрих-кодів. Метою розробки є дослідження та програмна реалізація системи захисту даних на мобільних пристроях з використанням матричних штрих-кодів. Об’єктом дослідження є процес захисту даних на мобільних пристроях з використанням матричних штрих-кодів. Предметом дослідження є методи захисту даних на мобільних пристроях з використанням матричних штрих-кодів. Методи дослідження базуються на методах захисту інформації, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи захисту даних на мобільних пристроях з використанням матричних штрих-кодів. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення. Розроблено зручний інтерфейс користувача. Наведені інструкції по роботі з програмними засобами.

комп’ютерні науки, захист даних, мобільні пристрої, матричні штрих-коди

Постановка проблеми. Обрана тема роботи – розробка програмного забезпечення системи захисту даних на мобільних пристроях з використанням матричних штрих-кодів. Необхідно розуміти що ідентифікацію й автентифікацію можна вважати основою програмно-технічних засобів безпеки, оскільки інші сервіси розраховані на обслуговування іменованих суб'єктів.

Ідентифікація й автентифікація – це перша лінія оборони, "прохідна" інформаційного простору організації. Сучасні засоби ідентифікації та автентифікації повинні підтримувати концепцію єдиного входу до ПК.

Єдиний вхід до мобільного пристрою це, у першу чергу, вимоги зручності для користувачів. Традиційно в автентифікація ПК виробляється за допомогою Імені (Login) і Пароля (Password). Використання цього підходу, як і все у світі, має свої переваги й свої недоліки.

Переваги очевидні – простота реалізації, відсутність необхідності здобувати додаткові пристрої, за винятком клавіатури. Але є й недоліки, в основному пов'язані з «людським фактором», а саме те, що людині важко запам'ятовувати довгі й складні паролі й отут починаються проблеми – користувачі забувають паролі, передають свої паролі третім особам, або пишуть свої паролі на папірцях (і навіть прикріплюють їх на монітор), придумують собі прості паролі, або просто використовують той самий пароль «на всі випадки життя». Все це рано або пізно приводить до втрати пароля в найкращому разі або до його «крадіжки» і використанню без відома користувача. Наявність проблеми підігнало розробку альтернативних шляхів автентифікації й ідентифікації.

Була розроблена безліч рішень, що дозволяють так чи інакше замінити спосіб їхнього зберігання й введення або замінити саму схему Ім'я-пароль.

До першої групи рішень відносять різні пристрої, такі як смарт-карти й електронні таблетки й ключі, у яких зберігається Ім'я й Пароль або інформація, що їх заміняє, до останньої групи рішень відносять різні біопараметричні способи ідентифікації й

автентифікації по персональних особливостях користувача, таким як відбитки пальців, сітківка ока, форми особи й рук і інші.

Але як смарт-карти так і біопараметричні способи ідентифікації потребують капітальних вкладень що в деяких випадках є критичним параметром.

У роботі реалізується задача системи захисту мобільних пристроїв від несанкціонованого доступу за допомогою розпізнавання матричних штрих-кодів – коду який надруковано на папері.

Оригінальність задачі в тому, що потрібно "навчити" комп'ютер розуміти код з камери мобільного пристрою, як його бачить людина, тобто виділяти з масиву точок літери.

В результаті маємо текст, котрий потім можна порівняти з відомими паролями доступу до персонального комп'ютера. Існує декілька програмних продуктів, котрі мають схожу функціональність але вони призначені для редагування тексту, а не ідентифікації особи користувача та скеровані на роботу стаціонарних ПК.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи захисту даних на мобільних пристроях з використанням матричних штрих-кодів.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи захисту даних на мобільних пристроях з використанням матричних штрих-кодів.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем захисту даних на мобільних пристроях з використанням матричних штрих-кодів.

– Дослідження системи захисту даних на мобільних пристроях з використанням матричних штрих-кодів.

– Програмна реалізація системи захисту даних на мобільних пристроях з використанням матричних штрих-кодів.

Об'єктом дослідження є процес захисту даних на мобільних пристроях з використанням матричних штрих-кодів.

Предметом дослідження є методи захисту даних на мобільних пристроях з використанням матричних штрих-кодів.

Методи дослідження базуються на методах захисту інформації, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Завдання розпізнавання (точніше, класифікації) об'єкта ставиться в такий спосіб.

Є деякий спосіб кодування об'єктів (наприклад рукописних букв або зображення з мобільної камери), що належать заздалегідь відомій кінцевій множині класів C={C1,..., Cq}, і деяка кінцева множина об'єктів (навчальна множина), про кожний з яких відомо, якому класові він належить.

Потрібно побудувати алгоритм, який по будь-якому вхідному об'єкту навчальній множині, що не обов'язково належить, розв'язує, якому класу цей об'єкт належить, і робить це достатньо добре. Якість розпізнавання оцінюється як імовірність (частота) помилки класифікації на іншій кінцевій множині об'єктів із заздалегідь відомими відповідями (тестовій множині).

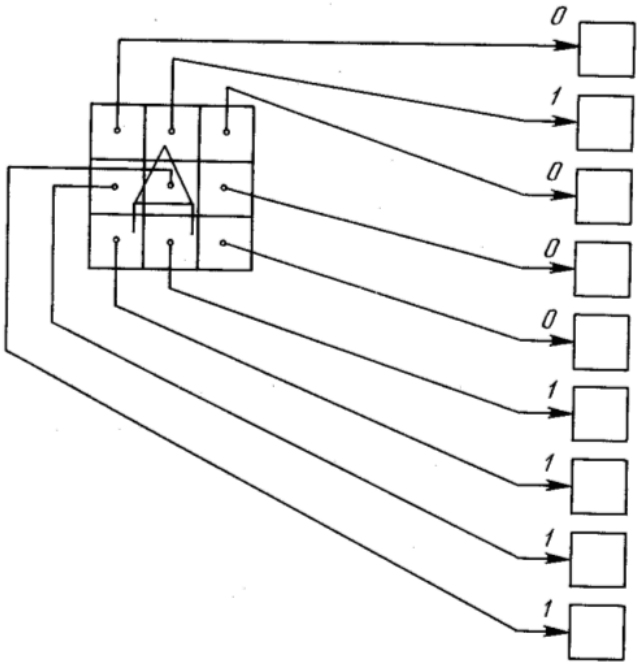


Рисунок 1 – Розпізнавання зображення отриманого з мобільного пристрою

При розпізнаванні на відміну від класифікації, буває потрібно оцінювати й чисельні характеристики об'єктів. Навчальна й тестова множина можуть не бути дані заздалегідь, а поповнюватися в процесі роботи алгоритму, що розпізнає. На вхід розпізнавання майже завжди потрапляють об'єкти, що не укладаються в класифікацію.

Крім того бажані гарантії (звичайно, статистичні) того, що на будь-якій іншій тестовій множині частота помилки розпізнавання буде майже аналогічною.

Типова система розпізнавання складається із трьох частин: витяг ознак з картинки, власне розпізнавання й ухвалення рішення.

Витяг ознак-це перетворення вхідних об'єктів до однакового, компактного й зручного вигляду із втратою більшої частини інформації, що не впливає на класифікацію. Зручним виявляється представлення об'єкта точкою стандартного евклідового простору R, що належить деякому фіксованому полю (кубу, кулі, сфері). Розмірність R повинна бути досить великою для успішного (якісного) розпізнавання.

Опис застосування алгоритмів розпізнавання

На перший погляд здається, що розпізнавання коду на картинці застосовується лише в наступних областях: Охоронні системи; Криміналістика; Комп'ютерна графіка.

Насправді, спектр застосування цих алгоритмів набагато ширше: Взаємодія комп'ютер-людина; Віртуальна реальність, комп'ютерні ігри; Права водія, паспорт; Контроль над імміграцією; Персоналізація побутових пристроїв; Шифрування даних; Електронна комерція; Криміналістика.

Особливості розпізнавання

При вирішенні задачі розпізнавання коду на картинці виникають дві проблеми. По перше, будь-яка картинка являє собою масив пікселів. У той же час один піксель картинки нічого не значить (його колір можна змінити, і ніхто не помітить різниці). Це робить таке представлення картинок надлишковою й неекономічним. Таким чином, для ефективного розпізнавання необхідно розробити деякий компактний і зручний формат представлення картинок.

На сьогоднішній день відома декілька способів стиску зображень із втратами, але використовуваний у них формат не зручний для класифікації коду на картинці, хоча б, тому що для рішення завдання розпізнавання потрібні, знову-таки, набагато менше інформації.

Це пов'язане в першу чергу з тим, що немає необхідності визначати, як виглядає код на зображенні з колекції, а потрібно розв'язати зворотне завдання: яка картинка з кодом з колекції виглядає даним образом.

Друга проблема полягає в тому, що одна й те ж картинка з кодом може бути отримана з мобільної камери при різних зовнішніх факторах, таких як світло, кут нахилу, швидкість руху.

Надалі будемо вважати, що всі фотографії з кодом одержувані з мобільної камери мають розмір 300 × 300 пікселів з 256 відтінками сірого.

Можна придумати багато варіантів постановки завдання розпізнавання. Один з таких варіантів представлений нижче.

Припустимо, що є деяка тренувальна колекція, що складається з 400 фотографій з кодами. Тоді завдання розпізнавання коду на картинці можна сформулювати в такий спосіб. Є деяке нове зображення в відомому форматі.

Необхідно видати одне з наступних відповідей:

– Зображення не є кодом;

– Зображення є кодом, картинки з колекції;

– Зображення є кодом, але його немає в колекції. У цьому випадку його можна додати в колекцію.

Опис етапів алгоритму розпізнавання

На першому етапі алгоритм виділяє із загального зображення код. Потім відбувається нормалізація зображення. До нормалізації зображення ставляться наступні дії:

– Зміна роздрукової спроміжності зображення до 300 × 300 пікселів;

– Перетворення кольорів до 256 відтінків сірого;

– Зміна сумарної яскравості зображення до деякого середнього значення. Для деяких алгоритмів потрібно, щоб код на картинці розташовувався як можна більш вертикально.

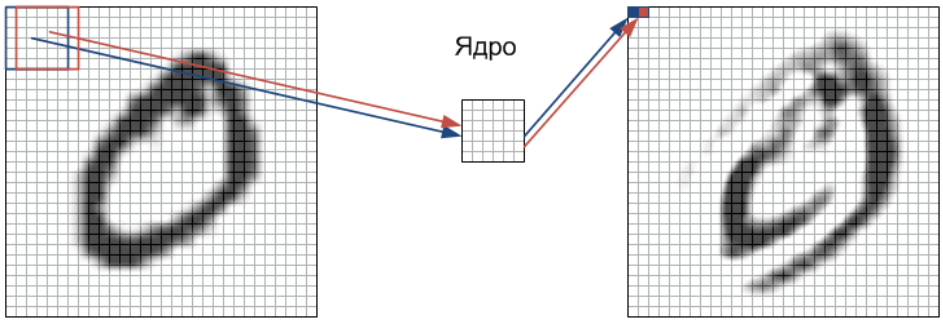


Рисунок 2 – Покрокове розпізнавання зображення

У такому випадку поворот коду на потрібний кут відбувається саме при нормалізації. Наступним етапом алгоритму розпізнавання є виділення характеристик наявного коду. Виділювані характеристики сильно залежать від алгоритму розпізнавання, тому їх приклади будуть наведені пізніше. Зауважимо, що після виділення характеристик картинка більше не потрібна.

Останнім етапом розпізнавання є застосування класифікатора, який по наявних характеристиках видає відповідь на завдання – кода співпадають чи ні. І як наслідок користувач одержує доступ до ПК.

Опис уніфікації зображення з кодом

На всіх картинках з кодом співвідношення між буквами приблизно однакові. Тому, доцільно виділити на коді деякі контрольні точки – просвіт між буквами, товщина лінії, розмір букви та ін.. Після цього для ідентифікації того або іншого коду, досить зчитати значення фільтрів Габора саме в контрольних точках.

Виділимо на довільному коді деякі контрольні точки. Для того, щоб визначити, де перебувають ці точки, необхідно мати деякі представлення про їхнє розташування. Для цього уніфікуємо зображення з кодом.

Зафіксуємо набір контрольних точок, що цікавлять нас (саме цей етап визначає якість алгоритму розпізнавання). Потім для кожного зображення з колекції вкажемо, де знаходиться кожна з контрольних точок, і порахуємо значення 40 фільтрів Габора в цих точках. Вектор, що складається з 40 значень фільтрів Габора, полічених у конкретній точці називається jet'ом цієї точки.

Тепер візьмемо середні значення відстані між контрольними точками. Також візьмемо середні значення jet'ів. Разом, ми одержали деякий граф, у якому вершинам відповідають контрольні точки, а довжини ребер дорівнюють середнім відстаням між даними контрольними точками.

Крім того, у кожній вершині зберігається один середній jet. Отриманий у такий спосіб граф називається уніфіковане зображення з кодом.

Опис знаходження контрольних точок

Після одержання на вхід нового коду насамперед треба знайти положення контрольних точок на ньому. Для кожної контрольної точки відомий її jet.

Необхідно знайти такий вектор точок, щоб jet кожної точки вектора був якнайближче до jet'у відповідної контрольної точки. При цьому, також щоб відстані між обраними крапками були як можна більш пропорційні довжинам ребер уніфікуємого графа.

Є досить багато методів мінімізації різних функцій. Для даного випадку підходить дуже простий метод. Спочатку великими кроками паралельно переміщаємо решітку та уніфікуємо зображення й порівнюємо, що виходять jet'и контрольних точок з еталонними.

Далі після того, як з'ясували приблизне розташування решітки, робимо зсув й повторюємо дію.

Потім незалежно переміщаємо кожну контрольну точку на незначну відстань. Цей метод використовує не повністю мінімизуючий набір точок, але в задачі розпізнавання кодів ці точки можна вважати контрольними точками зображення.

Опис і обґрунтування класифікації

Після того, як знайдені контрольні точки зображення, ми маємо вектор нового зображення, що є набором jet'ів усіх контрольних точках.

Потрібно визначити, якому коду відповідає даний вектор. Для цього застосовуються стандартні методи класифікації.

Переваги – метод класифікації графів має поруч перевагу навчання, для досягнення гарних результатів йому необхідна маленька вихідна колекція кодів.

Опис частин мобільної камери

Мобільна камера містить об'єктив, оптичний фільтр, ПЗС або CMOS матрицю, схему цифрової обробки зображення, схему компресії зображення й опціонально Web сервер для підключення до мережі.

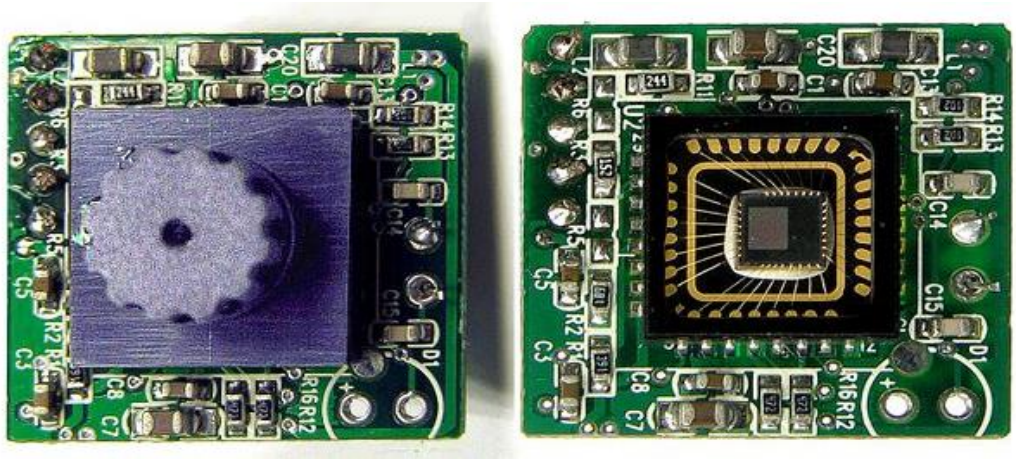


Рисунок 3 – Плата мобільної камери з об'єктивом та без

Опис ПЗЗ матриці

ПЗЗ – матриця (прилад із зарядовим зв'язком) або CCD-матриця (CCD, Charge-Coupled Device) – спеціалізована аналогова інтегральна мікросхема, що полягає зі світлочутливих фотодіодів, виконана на основі кремнію, що використовує технологію ПЗЗ – приладів із зарядовим зв'язком.

ПЗЗ – матриці випускаються й активно використовуються компаніями Nikon, Canon, Sony, Fuji, Kodak, Matsushita, Philips і багатьма іншими.

ПЗЗ-матриця складається з полікремнію, відділеного від кремнієвої підложки, у якої при подачі напруги через полікремінні затвори змінюються електричні потенціали поблизу електродів.

До експонування звичайно подачею певної комбінації напруг на електроди відбувається скидання всіх зарядів, що раніше утворилися, і приведення всіх елементів в ідентичний стан.

Далі комбінація напруг на електродах створює потенційну яму, у якій можуть накопичуватися електрони, що утворилися в даному пікселі матриці в результаті впливу світла при експонуванні. Чим інтенсивніше світловий потік під час експозиції, тим більше накопичується електронів у потенційній ямі, відповідно тем вище підсумковий заряд даного пікселя.

Після експонування послідовні зміни напруги на електродах формують у кожному пікселі й поруч із ним розподіл потенціалів, який приводить до перетеканню заряду в заданому напрямку, до вихідних елементів матриці.

На рисунку зображено приклад субпікселя ПЗЗ матриці з кишенею n-типу. Архітектура пікселів у виробників різна.

Позначення на схемі субпікселя ПЗЗ: 1-Фотони світла, що пройшли через об'єктив фотоапарата; 2-Мікролінза субпікселя; 3- R червоний світлофільтр субпікселя, фрагмент фільтра Байера; 4-Прозорий електрод з полікристалічного кремнію або оксиду олова; 5-Ізолятор (оксид кремнію); 6-Кремнієвий канал n-типу. Зона генерації носіїв (зона внутрішнього фотоефекта); 7-Зона потенційної ями (кишеня n-типу), де збираються електрони із зони генерації носіїв; 8-Кремнієва підложка p-типу;

Матриці з полнокадровим переносом. Сформоване об'єктивом зображення попадає на ПЗЗ-матрицю, тобто промені світла падають на світлочутливу поверхню ПЗЗ-елементів, завдання яких перетворити енергію фотонів в електричний заряд. Відбувається це приблизно в такий спосіб.

Для фотона, що впав на ПЗЗ-елемент, є три варіанти розвитку подій- він або «срикошетить» від поверхні, або буде поглинений у товщі напівпровідника (матеріалу матриці), або «проб'є наскрізь» її «робочу зону».

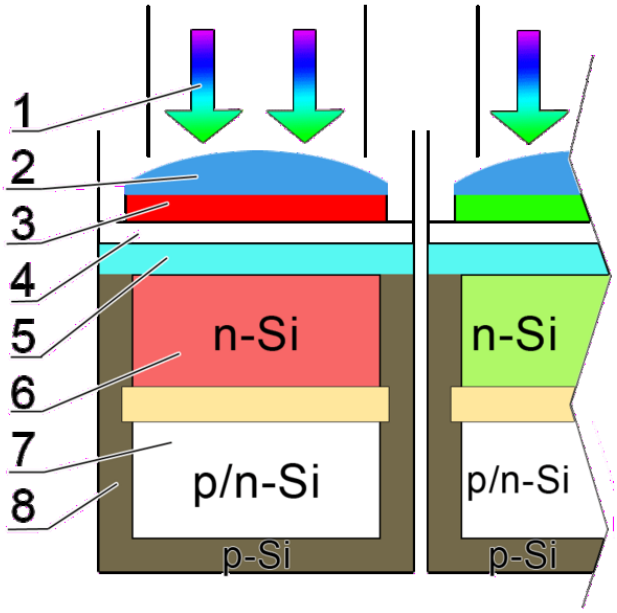


Рисунок 4 – Схема субпікселів ПЗЗ – матриці

Очевидно, що від розроблювачів потрібно створити такий сенсор, у якому втрати від «рикошету» і «прострілу навиліт» були б мінімізовані. Ті ж фотони, які були поглинені матрицею, утворюють пари електрон-комірка, якщо відбулася взаємодія з атомом кристалічних ґрат напівпровідника, або ж тільки електрон (або комірку), якщо взаємодія була з атомами донорних або акцепторних домішок, а обидва перелічених явища називаються внутрішнім фотоефектом.

Зрозуміло, внутрішнім фотоефектом робота сенсора не обмежується-необхідно зберегти «відняті» у напівпровідника носії заряду в спеціальнім сховищі, а потім їх лічити.

Елемент ПЗЗ-матриці в загальному виді конструкція ПЗЗ-елемента виглядає так: кремнієва подложка р-типу оснащується каналами з напівпровідника n-типу. Над каналами створюються електроди з полікристалічного кремнію з ізолюючим прошарком з оксиду кремнію.

Після подачі на такий електрод електричного потенціалу, у збідненій зоні під каналом n-типу створюється потенційна яма, призначення якої – зберігати електрони. Фотон, що проникає в кремній, приводить до генерації електрона, який притягається потенційною ямою й залишається в ній.

Більша кількість фотонів (яскраве світло) забезпечує більший заряд ями. Потім треба лічити значення цього заряду, іменованого також фотострумом, і підсилити його.

Зчитування фотострумів ПЗЗ-елементів здійснюється так званими послідовними регістрами зсуву, які перетворюють рядок зарядів на вході в серію імпульсів на виході. Дана серія являє собою аналоговий сигнал, який надалі надходить на підсилювач.

Таким чином, за допомогою регістру можна перетворити в аналоговий сигнал заряди рядка із ПЗЗ-елементів. Фактично, послідовний регістр зсуву в ПЗЗ-матрицях реалізується за допомогою тих же самих ПЗЗ-елементів, об'єднаних у рядок. Робота такого пристрою базується на здатності приладів із зарядовим зв'язком (саме це позначає абревіатура ПЗЗ) обмінюватися зарядами своїх потенційних ям. Обмін здійснюється завдяки наявності спеціальних електродів переносу (transfer gate), розташованих між сусідніми ПЗЗ-елементами. При подачі на найближчий електрод підвищеного потенціалу заряд «перетікає» під нього з потенційної ями.

Між ПЗЗ-елементами можуть розташовуватися від двох до чотирьох електродів переносу, від їхньої кількості залежить «фазність» регістру зсуву, яке може називатися двофазним, трифазним.

Подача потенціалів на електроди переносу синхронізована таким чином, що переміщення зарядів потенційних ям усіх ПЗЗ-елементів регістру відбувається одночасно. І за один цикл переносу ПЗЗ-елементи як би «передають по ланцюжкові» заряди ліворуч праворуч (або ж праворуч ліворуч). Ну а крайні елементи ПЗЗ віддають свій заряд пристрою, розташованому на виході регістру-тобто підсилювачу.

У цілому, послідовний регістр зсуву є пристроєм з паралельним входом і послідовним виходом. Тому після зчитування всіх зарядів з регістру є можливість подати на його вхід новий рядок, що потім формує у такий спосіб безперервний аналоговий сигнал на основі двовимірного масиву фотострумів.

У свою чергу, вхідний паралельний потік для послідовного регістру зсуву (тобто рядка двовимірного масиву фотострумів) забезпечується сукупністю вертикально орієнтованих послідовних регістрів зсуву, яка іменується паралельним регістром зсуву, а вся конструкція в цілому саме і є пристроєм, іменованим ПЗЗ-матрицею.

«Вертикальні» послідовні регістри зсуву, що становлять паралельний, називаються стовпцями ПЗЗ-матриці, а їх робота повністю синхронізована. Двовимірний масив фотострумів ПЗЗ-матриці одночасно зміщається вниз на один рядок, причому відбувається це тільки після того, як заряди попереднього рядка з розташованого послідовного регістру зсуву пішли на підсилювач.

До звільнення послідовного регістру паралельний вимушен простоювати. Ну а сама ПЗЗ-матриця для нормальної роботи обов'язково повинна бути підключена до мікросхеми, що подає потенціали на електроди як послідовного, так і паралельного регістрів зсуву, а також синхронізуючої роботу обох регістрів. Крім того, потрібний тактовий генератор.

Повноокадрова матриця. Даний тип сенсора є найбільш простим з конструктивної точки зору й іменується повноокадровою ПЗЗ-матрицею (full-frame CCD matrix).

Матриці з буферизацією кадра. Існує вдосконалений варіант повноокадрової матриці, у якої заряди паралельного регістру не надходять построчно на вхід послідовного, а «складуються» у буферному паралельному регістрі. Даний регістр розташований під основним паралельним регістром зсуву, фотоструми построчно переміщаються в буферний регістр і вже з нього надходять на вхід послідовного регістру зсуву.

Поверхня буферного регістру покрита непрозорою (частіше металевою) панеллю, а вся система одержала назву матриці з буферизацією кадру (frame-transfer CCD). Матриця з буферизацією кадра

Матриці з буферизацією стовпців. Спеціально для відеотехніки був розроблений новий тип матриць, у якому інтервал між експонуванням був мінімізований не для пари кадрів, а для безперервного потоку. Зрозуміло, для забезпечення цієї безперервності довелося передбачити відмову від механічного затвора.

Фактично дана схема, що одержала найменування матриці з буферизацією стовпців (interline CCD -matrix), у ній використовується буферний паралельний регістр зсуву, ПЗЗ-елементи якого сховані під непрозорим покриттям. Однак буфер цей не розташовується єдиним блоком під основним паралельним регістром-його стовпці «перетасовані» між стовпцями основного регістру.

У результаті поруч із кожним стовпцем основного регістру перебуває стовпець буфера, а відразу ж після експонування фотоструми переміщаються не «зверху вниз», а «ліворуч праворуч» (або «праворуч ліворуч») і всього за один робітник цикл попадають у буферний регістр, цілком і повністю звільняючи потенційні ями для наступного експонування.

Що потрапили в буферний регістр заряди у звичайному порядку зчитуються через послідовний регістр зсуву, тобто «зверху вниз». Оскільки скидання фотострумів у буферний регістр відбувається всього за один цикл, навіть при відсутності механічного затвора не спостерігається нічого схожого на «розмазування» заряду в повнокадрової матриці.

А під час експонування для кожного кадру в більшості випадків по тривалості відповідає інтервалу, затрачуваному на повне зчитування буферного паралельного регістру.

Завдяки всьому цьому з'являється можливість створити відеосигнал з високою частотою кадрів – не менш 30 кадрів у секунду. Матриця з буферизацією стовпців Найчастіше у вітчизняній літературі матриці з буферизацією стовпців помилково йменують рядковою.

Матриці зі зворотним засвіченням. У класичній схемі ПЗЗ-елемента, при якій використовуються електроди з полікристалічного кремнію, світлочутливість обмежена через часткове розсіювання світла поверхнею електрода. Тому при зйомці в особливих умовах, що вимагають підвищеної світлочутливості в синьої й ультрафіолетової областях спектра, застосовуються матриці зі зворотним засвіченням (back-illuminated matrix).

У сенсорах такого типу світло падає на подложку, але для необхідного внутрішнього фотоефекта подложка шліфується до товщини 10-15 мкм. Дана стадія обробки суттєво збільшувала вартість матриці, пристрої виходили досить тендітними й вимагали підвищеної обережності при складанні й експлуатації. А при використанні світлофільтрів, що послабляють світловий потік, всі дорогі операції по збільшенню чутливості втрачають зміст.

Опис світлочутливісті

Світлочутливість матриці складається зі світлочутливості всіх її фотодатчиків (пікселів) і в цілому залежить від:

– інтегральної світлочутливості, що представляє собою відношення величини фотоефекта до світлового потоку (у люменах) від джерела випромінювання нормованого спектрального складу;

– монохроматичної світлочутливості, відношення величини фотоефекта до величини світлової енергії випромінювання, відповідній до певної довжини хвилі;

– набір усіх значень монохроматичної світлочутливості для обраної частини спектра світла становить спектральну світлочутливість-залежність світлочутливості від довжини хвилі світла.

Світлочуттева матриця це спеціалізована аналогова або цифро-аналогова інтегральна мікросхема, що складається зі світлочутливих елементів-фотодіодів.

Призначена для перетворення спроектованого на неї оптичного зображення в аналоговий електричний сигнал або в потік цифрових даних (при наявності АЦП безпосередньо в складі матриці).

Є основним елементом цифрових фотоапаратів, сучасних Web камер, фотокамер, вбудованих у мобільний телефон, камер систем відеоспостереження й багатьох інших пристроїв.

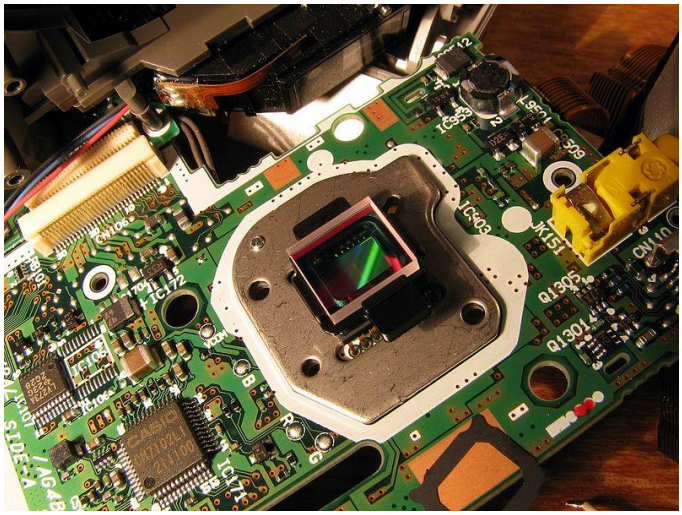


Рисунок 5 – Матриця на друкованій платі мобільного пристрою

Мобільна камера це цифрова відео або фотокамера, здатна в реальному часі фіксувати зображення, призначені для подальшої передачі по мережі Інтернет (у програмах типу Instant Messenger або в будь-якому іншому ПЗ).

Мобільні камери, що доставляють зображення через Інтернет, закачують зображення на Web сервер або по запиту, або безупинно, або через регулярні проміжки часу. Це досягається шляхом підключення камери до комп'ютера або завдяки можливостям самої камери.

Деякі сучасні моделі мають апаратним і програмним забезпеченням, яке дозволяє камері самостійно працювати в якості Web сервера, FTP-сервера, FTP-клієнта й (або) відсилати зображення електронною поштою.

Web камери, призначені для відеоконференцій, це, як правило, прості моделі камер, що підключаються до комп'ютера, на якіму запущена програма типу Instant Messenger.

Моделі камер, використовувані в охоронних цілях, можуть забезпечуватися додатковими пристроями й функціями (такими, як детектор руху, підключення зовнішніх датчиків і т.п.).

Перша в історії Web камера була запущена в 1991 році й показувала кавоварку в Троянській кімнаті Кембриджського університету. Зараз вона не працює, оскільки була відключено 22 серпня 2001 року. Останній фотознімок, зроблений цієї камерою, ще можна бачити на її домашній сторінці в Інтернеті.

Подібно багатьом мережним технологіям, Web камери та відео чати набули масову популярності. Необхідність в «живих» відео зображеннях породила Web камеру, здатні віщати через Інтернет у форматі відеопотоку, що не вимагає від глядача необхідності вручну обновляти зображення; а незабаром, непотрібними в сучасних браузерах стали спеціальні плагіни.

Опис світлочутливої матриці яка виконана на основі CMOS-технології

CMOS-матриця це світлочутлива матриця Web камери, виконана на основі CMOS-транзисторів.

У CMOS-матрицях використовуються польові транзистори з ізольованим затвором з каналами різної провідності.

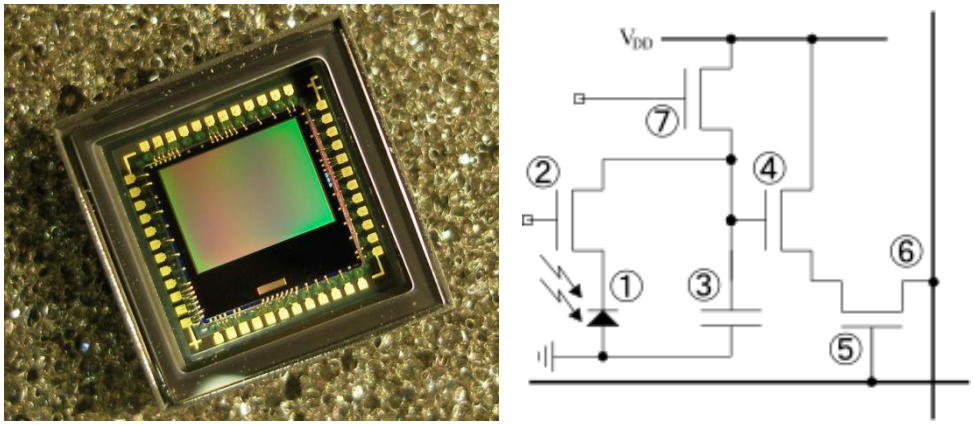


Рисунок 6 – CMOS матриця

Схема CMOS-матриці: 1-світлочуттевий елемент (діод); 2-затвор; 3-конденсатор, що зберігає заряд з діода; 4-підсилювач; 5-шина вибору рядка; 6-вертикальна шина, що передає сигнал процесору; 7-сигнал скидання.

Принцип роботи: До зйомки подається сигнал скидання; У процесі експозиції відбувається накопичення заряду фотодіодом; У процесі зчитування відбувається вибірка значення напруги на конденсаторі.

Основна перевага CMOS технології-низьке енергоспоживання в статичному стані. Це дозволяє застосовувати такі матриці в складі енергонезалежних пристроїв, наприклад, у датчиках руху й системах спостереження, що перебувають більшу частину часу в режимі «сну» або «очікування події».

Важливою перевагою CMOS матриці є єдність технології з іншими, цифровими елементами апаратури. Це приводить до можливості об'єднання на одному кристалі

аналогової, цифрової й обробної частини (CMOS-технологія, будучи в першу чергу процесорною технологією, має на увазі не тільки "захват" світла, але й процес перетворення, обробки, очищення сигналів не тільки властиво-захоплених, але й сторонніх компонентів), що послужило основою для мініатюризації камер для самого різного обладнання й зниження їх вартості через відмову від додаткових процесорних мікросхем.

За допомогою механізму довільного доступу можна виконувати зчитування обраних груп пікселів. Дана операція одержала назву кадрованого зчитування (windowing readout). Кадрування дозволяє зменшити розмір захопленого зображення й потенційно збільшити швидкість зчитування в порівнянні із ПЗЗ-сенсорами, оскільки в останні для подальшої обробки необхідно вивантажити всю інформацію. З'являється можливість застосовувати ту саму матрицю в принципово різних режимах.

Зокрема, швидко зчитуючи тільки малу частину пікселів, можна забезпечити якісний режим живого перегляду зображення на вбудованому в апарат екрані з відносно малим числом пікселів. Можна от сканувати тільки частини кадра й застосувати її для відображення на весь екран. Тим самим одержати можливість якісного ручного фокусування.

На додаток до підсилювача усередині пікселя, підсилювальні схеми можуть бути розміщені у будь-якому місці по ланцюгу проходження сигналу. Це дозволяє створювати підсилювальні каскади й підвищувати чутливість в умовах поганого освітлення. Можливість зміни коефіцієнта підсилення для кожного кольору поліпшує, зокрема, балансування білого. Дешевизна виробництва в порівнянні із ПЗЗ-матрицями.

Недоліки. Фотодіод гнізда займає суттєво меншу площу елемента матриці, у порівнянні із ПЗЗ матрицею з повнокадровим переносом. Тому ранні матриці CMOS мали суттєво більш низьку світлочутливість, чому ПЗЗ.

Фотодіод гнізда матриці має порівняно малий розмір, величина ж одержуваної вихідної напруги залежить не тільки від параметрів самого фотодіода, але й від властивостей кожного елемента пікселя. Таким чином, у кожного пікселя матриці виявляється своя власна характеристична крива, і виникає проблема розкиду світлочутливості й коефіцієнта контрасту пікселів матриці.

Наявність на матриці великого в порівнянні з фотодіодом обсягу електронних елементів створює додаткове нагрівання пристрою в процесі зчитування й приводить до зростання теплового шуму.

Розробка структурної схеми

Розглянемо розроблену структурну схему системи (рис. 7). Схема зображує систему захисту мобільного пристрою від несанкціонованого доступу. Спочатку йде отримання зображення з камери мобільного пристрою потім якщо це зображення є кодом проходить зменшення деталізації зображення для порівняння.

Зображення отримується шляхом фіксації кадру з роздрукованим кодом на листку папера. Якщо згортання пройшло невдало йде ще спроба доти поки вхідне отримане зображення не буде згорнуто до розмірів матриці пікселів.

Проводиться порівняння матриці пікселів з матрицею коду санкціонованого доступу через існуючу матрицю коду санкціонованого доступу.

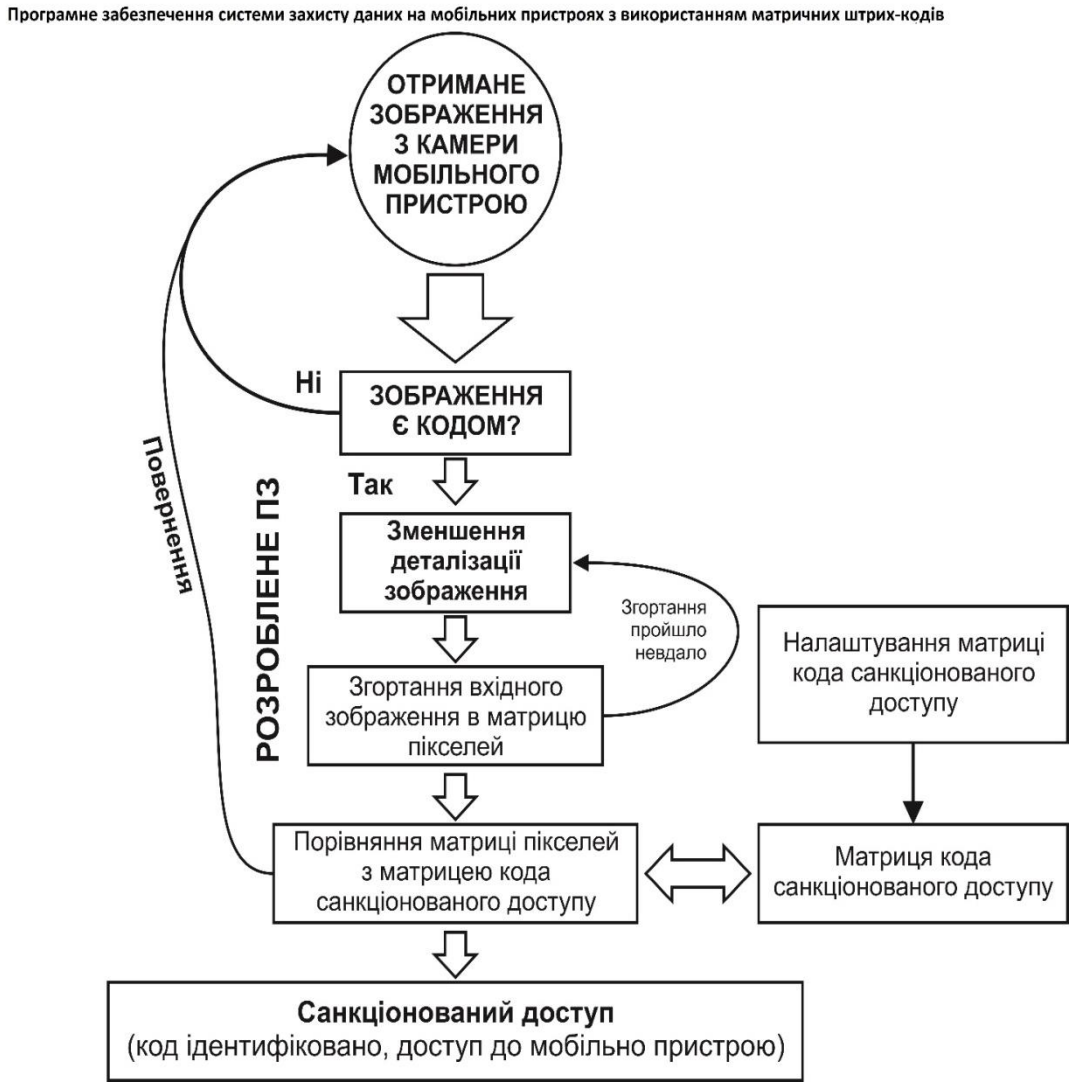


Рисунок 7 – Структурна схема системи

На зображенні виділяються характеристики та проходить розпізнавання зображення з застосуванням класифікатора (вибір із шаблонів шрифтів). Якщо зображення є кодом проходить ідентифікація коду та встановлюється код ідентифіковано чи ні. І якщо код ідентифіковано розроблене ПЗ дає доступ до мобільного пристрою.

Висновок. У статті розглянуто та проаналізовано програмне забезпечення, яке призначено для системи захисту даних на мобільних пристроях з використанням матричних штрих-кодів. В межах України в недостатній мірі представлені вітчизняні розробки в цій області. У роботі наведені теоретичне узагальнення й рішення наукового завдання дослідження методів захисту даних на мобільних пристроях з використанням матричних штрих-кодів. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем захисту даних на мобільних пристроях з використанням матричних штрих-кодів; Досліджена система захисту даних на мобільних пристроях з використанням матричних штрих-кодів; На основі отриманих результатів досліджень створена програмна реалізація системи захисту даних на мобільних пристроях з використанням матричних штрих-кодів. Розроблені під час виконання роботи алгоритми дозволяють успішно вирішувати завдання захисту даних на мобільних пристроях з використанням матричних штрих-кодів. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки. Розроблене програмне забезпечення має простий, дружній та зручний

інтерфейс користувача, що забезпечує легкість у освоєнні роботи програмного продукту, зручність у використанні, і не потребує особливих спеціальних знань. При створені програмного забезпечення було використано об'єктно-орієнтований підхід, що відповідає сучасним тенденціям у галузі розробки комерційних програмних систем. Програма реалізована на мові високого рівня Delphi 2010. Дана мова програмування дозволяє найбільш ефективно обробляти дані. Це дозволило мінімізувати строк розробки програмного забезпечення, і, як слід, зменшити витрати на його розробку. Запропоноване програмне забезпечення ділиться на загальне програмне забезпечення, що поставляється із засобами обчислювальної техніки й спеціальне програмне забезпечення, що спеціально розроблене для даної конкретної системи й включає програми, що реалізують її функції. Програма призначена для виконання під управлінням багатозадачної операційної системи Android. Даються необхідні рекомендації з установки розробленого програмного забезпечення. Для підвищення рівня безпеки запропоновано застосовувати алгоритм RSA. В цілому створене програмне забезпечення підтверджує правильність використаних проектних рішень та повністю відповідає вимогам технічного завдання. Створене програмне забезпечення має потенційну можливість для подальшого вдосконалення і застосування у різних галузях.

Список літератури

1. А.А. Смирнов, А.П. Доренський // Информационные технологии и системы в управлении, образовании, науке: монография под ред. проф. В.С. Пономаренко. – Х.: Цифрова друкарня № 1, 2014. – С. 22-36. – ISBN 978-617-7188-50-5.
2. Смірнов О.А. Дослідження впливу ступеня стиснення зображень на оперативність їх доставки у телекомунікаційній системі / О.А. Смірнов, О.М. Дрєєв, О.П. Доренський // Системи обробки інформації. – 2013. – Вип. 8(115). – С. 234-239.
3. Смірнов О.А. Аналіз процесів стиснення та відновлення зображень на основі цифрових методів // О.А. Смірнов, О.П. Доренський, О.М. Дрєєв // Наука і техніка Повітряних сил Збройних Сил України. – 2013. – № 3(12). – С.122-127.
4. Доренський О.П. Формалізація процесу зміни станів програмних об'єктів складних систем на основі формального апарату скінченних автоматів Мура / О.П. Доренський, О.А. Смірнов // Зв'язок : Науково-виробничий журнал. – 2014. – № 3 (109) – С. 27-31.
5. Доренський О.П. Синтез структури інтегрованої моделі об'єктно-орієнтованого програмного забезпечення / О.П. Доренський // Системи обробки інформації. – 2014. – Т. 2, Вип. 2(118). – С. 68-72.
6. Dorensky O. Method of the Models' Synthesis for Software Automated System Objects' States in Digital Images Processing / Oleksandr Dorensky // Збірник наукових праць Кіровоградського національного технічного університету: Техніка в сільськогосподарському виробництві, галузеве машинобудування, автоматизація. – 2014. – Вип. 27. – С. 283-292.
7. Доренський О.П. Метод синтезу тестових структур взаємодії програмних об'єктів під час проектування програмного забезпечення на основі об'єктно-орієнтовної технології / О.П. Доренський // Системи управління, навігації та зв'язку. – Полтава: ПолтНТУ, 2014. – Вип. 3 (31). – С. 107–114.
8. Доренський О.П. Метод синтезу тестових моделей поведінки програмних об'єктів інформаційно-телекомунікаційної системи спеціального призначення / О.П. Доренський // Збірник наукових праць Харківського університету Повітряних Сил. – 2014. – Вип. 3(40). – С. 109-112.
9. Dorensky O. Development of the theoretical bases of logical domain modeling of a complex software system / Oleksandr Dorensky, Alexey Smirnov // International Journal of Computational Engineering Research (IJCER). – India, Delhi, 2014. – Vol. 4, Issue 4. – P. 19-23.
10. Доренський О.П. Дослідження помилок програмного забезпечення // О.П. Доренський, О.М. Змеул // Актуальні задачі сучасних технологій : Міжнар. наук.-техн. конф., 19-20 груд, 2012 р. : збірн. тез доп. – Тернопіль, 2012. – С. 187-188.

УДК 004

Ю. Коваленко, магістр гр. КІ-18-1,4
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ УПРАВЛІННЯ ВЕБ-САЙТОМ ДЛЯ ДИСПЕЧЕРИЗАЦІЇ ВОДОКАНАЛУ

У статті розроблено програмне забезпечення, яке призначено для системи управління веб-сайтом для диспетчеризації водоканалу. Метою розробки є дослідження та програмна реалізація системи управління веб-сайтом для диспетчеризації водоканалу. Об'єктом дослідження є процес управління веб-сайтом для диспетчеризації водоканалу. Предметом дослідження є методи управління веб-сайтом для диспетчеризації водоканалу. Методи дослідження базуються на етапах спостереження - цілеспрямованого вивчення предметів, що спирається на дані вимірювання. Порівняння з програмними продуктами конкурентів. Пізнавальна операція, що лежить в основі суджень про подібність або відмінність між фінальними продуктами. Методи узагальнення результатів управління веб-сайтом для диспетчеризації водоканалу. Результат роботи – програмна реалізація системи управління веб-сайтом для диспетчеризації водоканалу. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. Розроблено зручний інтерфейс користувача.
комп'ютерна інженерія, онлайн моніторинг, водопостачання, ASP.NET

Постановка проблеми. Ручне і спрощене автоматичне керування роботою систем водопостачання вже не задовольняють зростаючі вимоги технічного персоналу комунальних підприємств до побудови інженерних систем. Все більшим попитом користується реалізація проектів по впровадженню систем диспетчеризації і повної автоматизації, які вже не тільки відображають технологічні параметри систем, а й виконують певні алгоритми управління, закладені самою програмою диспетчеризації, в тому числі - з функціями енергоефективності. Такі системи дозволяють оператору дистанційно коригувати роботу, змінювати параметри уставок і давати команди на віддалений запуск/зупинку насосних станцій в залежності від фактичного стану всієї системи.

Можливість (при наявності перетворювача частоти і відповідної комплектації станції управління) спостерігати оператору за параметрами системи водопостачання, віддалено змінювати налаштування (заданий робочий тиск і по необхідності інші), дистанційно включати і вимикати насоси, переходити з режиму частотного регулювання в резервне управління прямим пуском, віддалено відстежувати і реагувати на виникаючі аварії.

Якщо провести огляд сучасних систем віддаленого керування, то ми побачимо, що провідні світові держави мають свої автономні системи, які забезпечують роботу відстежування та запобігання певних надзвичайних ситуацій. У США це система ITT Corporation, у Японії – Kurita Water Industries, у Європейському Союзі – Veolia Environnement. В зв'язку з тим, що Україна поки не розвертає онлайн систему моніторингу системи водопостачання, то актуальним буде розробка вітчизняного програмного забезпечення даної системи.

У такий спосіб актуальним є завдання розробки системного програмного забезпечення яке буде виводити дані лічильника та маніпулювати ними в онлайн режимі.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні управління веб-сайтом для диспетчеризації водоканалу.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи управління водопостачання на основі ASP.NET.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем управління водопостачання на основі ASP.NET.
– Дослідження системи управління водопостачання на основі ASP.NET.
– Програмна реалізація системи управління водопостачання на основі ASP.NET.

Об'єктом дослідження є процес управління водопостачання на основі ASP.NET.

Предметом дослідження є методи управління водопостачання на основі ASP.NET.

Методи дослідження базуються на етапах спостереження - цілеспрямованого вивчення предметів, що спирається на дані вимірювання. Порівняння з програмними продуктами конкурентів. Пізнавальна операція, що лежить в основі суджень про подібність або відмінність між фінальними продуктами. Методи узагальнення результатів управління водопостачання на основі ASP.NET.

Виклад основного матеріалу. При розробці системи автоматизованого управління технологічним процесом водопостачання необхідно реалізувати автоматизоване робоче місце оператора з програмним забезпеченням, взаємодіє з контролером. Також необхідно визначити необхідні датчики, які надаватимуть інформацію про стан процесу і виконавчі механізми, що впливають на об'єкт. Технологічний процес в промисловості нерозривно зв'язаний з її автоматизацією технологічних процесів. Автоматизація ефективно застосовується на сучасному етапі розвитку людства з метою досягнення зростання показників ресурсозбереження, поліпшення екології навколишнього середовища якості та надійності продукції. В зв'язку з бурхливим розвитком мікропроцесорної техніки і персонально електронно-обчислювальних машин, функціональні можливості яких дають змогу використовувати найдосконаліші методи в рамках сучасних складних систем управління. Мікропроцесорні пристрої та електронно-обчислювальних машини, пов'язані між собою обчислювальними та керуючими мережами з використанням загальних баз даних, дозволяють впроваджувати комп'ютерні технології у нетрадиційній сфері діяльності підприємства, що проявляється в інтеграції виробничих процесів та управління ними.

Головним напрямом автоматизації в агропромисловому комплексі на сучасному етапі є створення комп'ютерно-інтегрованих виробництв. Основою систем автоматизації стали функціональні можливості мікропроцесорних систем управління, при створенні яких вирішальну роль відіграють такі фактори, як використання принципів інтеграції, розподіленого управління, програмних комплексів. При автоматизації виробництва об'єктом є не окремий технологічний процес чи агрегат, а технологічний комплекс із складними взаємозв'язками між його підсистемами. При системному підході автоматизація виробництва дає кращі результати, коли досконало вивчаються властивості об'єкта автоматизації, розробляється функціональна структура як сукупність виконуваних системою функцій.

У загальному плані автоматизація виробництва це етап машинного виробництва, що характеризується звільненням людини від безпосереднього виконання функцій управління виробничими процесами та передачею цих функцій технічним засобом - автоматичним пристроям і системам. В основі автоматизації виробництва лежить поняття "управління". Управління - цілеспрямована дія на процес (об'єкт), яка забезпечує оптимальний чи заданий режим його роботи. Процес управління, з точки зору автоматичних систем, складаються з ряду елементарних операцій та етапів, які є спільними для технічних систем і систем живої природи.

Незалежно від мети, призначення, структури об'єкта процес управління передбачає виконання таких операцій, як:

– одержання та попередня обробка інформації про фактичний стан об'єкта, системи і навколишнього середовища;
– аналіз одержаної інформації, порівняння існуючої виробничої ситуації із даною;
– прийняття рішення про дію на об'єкт у певному напрямку та оцінка можливості реалізації такої дії;

– реалізація управління, тобто формування дії за допомогою відповідних технічних засобів.

Якщо людина не бере участі у формуванні управляючої дії, управління називається автоматичним. У складних системах і ситуаціях прийняття остаточних рішень щодо управління залишається за людиною, тоді управління є автоматизованим. Відповідно до цього системи називаються автоматичними чи автоматизованими. В першому випадку за людиною залишаються лише функції по обслуговуванню системи і контролю за її функціонуванням. В другому - технічні засоби забезпечують людину оперативною інформацією, але остаточне рішення, тобто етапи оцінки ситуації та формування управлінь, приймає вона сама. Сучасні автоматичні та автоматизовані системи є за своєю структурою розподіленими і базуються на мережових технологій з використанням мікропроцесорних засобів.

Об'єкт автоматизації - будь-який технологічний апарат, процес, машина, установка які підлягають автоматизації.

Сучасні системи автоматизації об'єднуються у складні комп'ютерно - інтегровані системи. Розглядаючи їх, слід передусім, наголосити на тому, що сукупність взаємозв’язаних і взаємодіючих елементів у них призначена для досягнення певних цілей. сукупність елементів системи та характери зв'язків між ними визначаються структурою останньої. При створенні й аналізі систем автоматизації виділяються такі структури:

– функціональну - сукупність частин для виконання окремих функцій: одержання інформації, її обробки, передачі;

– алгоритмічну - сукупність частин для виконання певних алгоритмів обробки інформації;

– технічну - сукупність необхідних технічних засобів як відображення функціональної та алгоритмічної структур.

Основні переваги автоматизації полягають у можливостях забезпечити:

– зростання продуктивності та поліпшення умов праці;

– виконання робіт в важкодоступних та взагалі недоступних для людини сферах (радіоактивні зони, космос окремі види металургійного та інших виробництв);

– підвищення точності, якості технологічних процесів і відповідних виробів;

– зростання надійності та техніко - економічних показників і загальної культури виробництва та кваліфікації обслуговуючого персоналу.

Пристрої автоматичного контролю забезпечують контроль за перебігом технологічних процесів, станом насосів та відповідно сигналізацію. При нормальних умовах процесів використовується сигналізація тригером (якщо зв'язок з насосом втрачено, коли прибор вийшов за верхню/нижню межу), а при появі відхилень від цих умов - візуальна та акустична сигналізація. Автоматичне включення або виключення електродвигунів насосів і компресорів в системах водопостачання будівель можливо при зміні рівня води в контейнері, або тиску в трубопроводах мережі або швидкості руху води в трубопроводі. При зміні зазначених параметрів наводяться в дію датчики, пов'язані з виконавчими механізмами включення або виключення магнітного пускача, що з'єднує або розмикає лінію електроживлення насоса. Пристрої захисту забезпечують захист об’єктів, бази даних, при появі загрози для підприємства, продукції або обслуговуючого персоналу.

Обчислювально-лічильні пристрої виконують самостійно складні розрахунки параметрів. Вони передаються на одноплатні комп’ютера raspberry pi. За допомогою плат відбувається управління даними (зчитування, запис, видалення тощо). Управління даними- це цілеспрямована дія на об'єкт яка забезпечує оптимальний чи заданий режим його роботи. Процес управління складається з ряду елементарних операцій та етапів, які є спільними для технічних систем. Незалежно від мети, призначення, структури об’єкта процесу управління передбачає виконання таких операцій, як:

– одержання та попередня обробка інформації про фактичний стан обєкта,

системи і навколишнього середовища;

– аналіз одержаної інформації, порівняння існуючої виробничої ситуації із заданою;

– прийняття рішення про дію на обєкт у певному напрямку та оцінка можливості реалізації такої дії;

– реалізація управління, тобто формування і здійснення дії за допомогою відповідних технічних засобів.

Розробка структурної схеми

Структурна схема відображає склад і взаємодію частин розроблюваного програмного забезпечення і визначається його архітектурою.

Джерелом інформації для програмної системи є плати які підключаються до насосів, станцій живлення, приборів і т.д. Для взаємодії з сайтом була розроблена сесія, яка буде забезпечувати парсинг необіхноїі інформації з СКБД. Завантажена інформація зберігається в сесіях, взаємодія з якою відбувається через «JSON parse». Завантажувана інформація з приборів визначається запитом, який відправляється до одноплатного компьютера. В разі успіху результат повертається, після чого нові дані надсилаються до бази даних.

```
ajax = function( url, callback ) {
                var req = xmlHttp();
                if (!req){
                        return;
                }
                req.open( "GET", url, true );
                req.onreadystatechange = function () {
                        if ( req.readyState != 4 || req.status != 200 && req.status != 304 ){
                                return;
                        }
                        callback( req.responseText );
                }
                if ( req.readyState == 4 ){
                        return;
                }
                req.send( null );
        }
```

Список запитів створюється за допомогою sql скриптів, які виконують пошук, виведення, видалення, редагування, створення записів та інше. Кожен запит в залежності від його типу відправляється на виконання до локальної бази даних. Тип запиту обирається розробником при його створенні. Дані які були додані до бази автоматично додаються в сесію для подальшого використання. Сесії також оновлюються і вся інформація показується на екран без перезавантаження сторінки.

На рис. 1 наведено структурну схему розробленого програмного забезпечення.

Рисунок 1 – Структурна схема програмної системи

Висновок. У статті розглянуто та проаналізовано програмне забезпечення, яке призначено для системи управління веб-сайтом для диспетчеризації водоканалу. В межах України в недостатній мірі представлені вітчизняні розробки в цій області. У роботі наведені теоретичне узагальнення й рішення наукового завдання дослідження методів управління веб-сайтом для диспетчеризації водоканалу. Рішення даного завдання полягало у вирішенні наступних задач: - Був проведений огляд існуючих систем управління веб-сайтом для диспетчеризації водоканалу; Досліджена система управління веб-сайтом для диспетчеризації водоканалу; На основі отриманих результатів досліджень створена програмна реалізація системи управління веб-сайтом для диспетчеризації водоканалу. Розроблені під час виконання роботи алгоритми дозволяють успішно вирішувати завдання управління веб-сайтом для диспетчеризації водоканалу. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки. Розроблене програмне забезпечення має простий, дружній та зручний інтерфейс користувача, що забезпечує легкість у освоєнні роботи програмного продукту, зручність у використанні, і не потребує особливих спеціальних знань. При створені програмного забезпечення було використано об'єктно--орієнтований підхід, що відповідає сучасним тенденціям у галузі розробки комерційних програмних систем. Програма реалізована на мові високого рівня C#. Дана мова

програмування дозволяє найбільш ефективно обробляти дані. Це дозволило мінімізувати строк розробки програмного забезпечення, і, як слід, зменшити витрати на його розробку. Запропоноване програмне забезпечення ділиться на бекенд, що поставляється із засобами обчислювальної техніки й фронтенд, що спеціально розроблене для даної конкретної системи й включає обмін між сервером і клієнтом.

Список літератури

1. Дрєєв О.М. Середньостатистичний та найімовірніший час доставки багатопакетного повідомлення в телекомунікаційній системі або мережі / О.М. Дрєєв, О.А. Смірнов // V Всеукраїнська науково-практична конференція "Інформатика та системні науки" ІСН – 2014, 13-15 березня 2014 року, м. Полтава – С. 92
2. Дрєєв О.М. Визначення оптимального розміру блоку при бітовому арифметичному кодуванні / О.М. Дрєєв, Г.М. Дрєєва // Збірник тез доповідей Комбінаторні конфігурації та їх застосування, 11-12 квітня 2014 р. – Кіровоград – С. 44
3. Дреев А.Н. Экстраполяция квазипериодических процессов с аддитивными помехами / А.Н. Дреев, А.А. Смирнов // П’ята Міжнародна науково-практична конференція "Інформаційні технології та моделювання в економіці" 15-16 травня 2014 р. – Черкаси – С. 59
4. Дреев А.Н. Статистическая модель передачи многопакетного сообщения в телекоммуникационной системе или сети / А.Н. Дреев, А.А. Смирнов // «Компьютерное моделирование в наукоемких технологиях (КМНТ-2014)» Харьков, 28-31 мая 2014 года – С. 137-140 Дрєєв О.М. Метод прогнозування завантаженості серверу телекомунікаційної мережі / О.М. Дрєєв, О.В. Коваленко // Тези доповідей Новітні технології – для захисту повітряного простору. Дев’ята наукова конференція. 18-19 квітня 2011 р. – Х.: ХУПС. – 2012. – С. 206
5. Дрєєв О.М. Метод довгострокового прогнозування навантаження серверу телекомунікаційної мережі / О.М. Дрєєв, Г.М. Дрєєва // Комбінаторні конфігурації та їх застосування. Кіровоград. 13-14 квітня 2012 р. – Кіровоград: “Екслюзів-систем”. – 2012. – С. 50
6. Дрєєв О.М. Вдосконалення стиснення зображень SPIHT методу шляхом додаткового кодування та відкладеної передачі уточнення вейвлет коефіцієнтів / О.М. Дрєєв // Дискретна математика та її застосування у економіко-математичному моделюванні та інформаційних технологіях. 11-13 жовтня 2012 р. – Запоріжжя: ЗНУ – 2012. – С. 22-23.
7. Дрєєв О.М. Методи підвищення якості обслуговування у телекомунікаційних системах та мережах / О.М. Дрєєв, Г.М Дрєєва, О.А. Смірнов // Збірник тез доповідей. Академія внутрішніх військ МВС України “Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку” 20-21 березня 2013р. – Харків: АВВ. – 2013. С. – 18-19
8. Дреев А.Н. SPIHT кодирование с отложенной передачей значимых битов / А.Н. Дреев // Тези доповідей. Новітні технології – для захисту повітряного простору. Дев’ята наукова конференція 17 квітня 2013 р. – Х.: ХУПС. – 2013. – С. 206
9. Дреев А.Н. Повышение оперативности доставки данных повышенной востребованности в телекоммуникационных системах и сетях / А.Н. Дреев, А.А. Смирнов, Е.В. Мелешко // Проблеми і перспективи розвитку ІТ-індустрії 25-26 квітня 2013 р. Системи обробки інформації. – Випуск 3 (110). Том 2. – Харків: ХУПС. – 2013. С. – 199.

УДК 004

Д. Коломієць, магістр гр. КІ-18-1,4
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ КОДУВАННЯ ІНФОРМАЦІЇ З ВИКОРИСТАННЯМ ЕНТРОПІЇ КОЛМОГОРОВА-СІНАЯ

У статті розроблено програмне забезпечення, яке призначено для кодування інформації з використанням ентропії Колмогорова-Сіная. Метою роботи є дослідження проектування та розробка системи кодування інформації з використанням ентропії Колмогорова-Сіная, а також дослідження властивостей даної

математичної системи, які будуть основою для кодування та декодування інформації. Об'єкт дослідження – система для кодування інформації з використанням ентропії Колмогорова-Сіная. Предмет дослідження – можливості використання математичної системи, яка базується на моделі ентропії Колмогорова-Сіная, для створення ГПВЧ. Під час виконання роботи було використано наступні методи досліджень:Метод аналізу, який полягає у розчленуванні предмету пізнання та абстрагування його окремих аспектів, був використаний для аналізу існуючих ГПВЧ, їх властивостей та недоліків; Метод експерименту який є сукупністю дослідів які об'єднані постановкою їх систем, способом обробки і взаємозв'язків результатів використаний для дослідження швидкодії та стійкості відомих ГПВЧ; Наукове моделювання – метод досліджень об'єктів пізнання який ґрунтується на заміні деякого об'єкту досліджень іншим об'єктом, який є подібним до нього. Даний метод використаний для моделювання математичної системи кодування інформації, яка базується на моделі більярду Колмогорова-Сіная. Результат роботи – програмна реалізація кодування інформації з використанням ентропії Колмогорова-Сіная. У ході роботи був зроблений аналіз існуючих систем для шифрування і виявлені їх недоліки. Розгорнуто принципи генерування генератору псевдо випадкових чисел на засадах математичного більярду і зокрема використання ентропійних властивостей ентропії Колмогорова-Сіная. Розроблено: функціональну схему, структурну схему, алгоритми та блок схеми, програмне забезпечення для моделювання генератору псевдо випадкових чисел на ентропії Колмагорова-Сіная для мікроконтролерів на базі STM та клієнт-серверний додаток для демонстрації роботи генератору.

комп'ютерна інженерія, кодування, ентропія, STM

Постановка проблеми. Через збільшення об'ємів обміну інформацією зростає потреба у методах її безпечної передачі які зможуть задовільнити сучасні вимоги щодо надійності та доступності.

Актуальність вибраної теми роботи обумовлена тим, що існуючі в нинішній час апаратні та програмні рішення для кодування інформації мають ряд суттєвих недоліків, таких як висока собівартість та знання способів обходу кодування даних.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні реалізації кодування інформації з використанням ентропії Колмогорова-Сіная.

Мета й завдання дослідження. Метою роботи є дослідження проектування та розробка системи кодування інформації з використанням ентропії Колмогорова-Сіная, а також дослідження властивостей даної математичної системи, які будуть основою для кодування та декодування інформації.

Задачею до роботи є дослідження властивостей ГПВЧ, порівняння їх властивостей, дослідження можливості використання ГПВЧ на основі ентропії Колмогорова-Сіная.

Об'єкт дослідження –система для кодування інформації з використанням ентропії Колмогорова-Сіная.

Предмет дослідження –можливості використання математичної системи, яка базується на моделі ентропії Колмогорова-Сіная, для створення ГПВЧ.

Методи дослідження які було використано:

- Метод аналізу, який полягає у розчленуванні предмету пізнання та абстрагування його окремих аспектів,був використаний для аналізу існуючих ГПВЧ, їх властивостей та недоліків;
- Метод експерименту який є сукупністю дослідів які об'єднані постановкою їх систем, способом обробки і взаємозв'язків результатів використаний для дослідження швидкодії та стійкості відомих ГПВЧ;
- Наукове моделювання – метод досліджень об'єктів пізнання який ґрунтується на заміні деякого об'єкту досліджень іншим об'єктом, який є подібним до нього. Даний метод використаний для моделювання математичної системи кодування інформації, яка базується на моделі більярду Колмогорова-Сіная.

Виклад основного матеріалу. В першу чергу необхідні первинні налаштування, а саме до комп'ютера необхідно за допомогою USB інтерфейсу підключити плату STM32F4, яка зареєструється в системі. Після цього запускається клієнтський та серверний додатки, яків момент запуску шукають у системі зареєстрований мікроконтролер. У випадку, коли він не буде знайдений – з'явиться вікно з помилкою і програма завершить свою роботу. Після того як додаток знайде у середовищі STM32F4, у випадку якщо запущений серверний

додаток, буде створено TCP-сервер, який буде готовий до з'єднання, а у випадку з клієнтським додатком буде створено TCP-клієнт. Після чого додаток буде знаходитись у стані очікування поки користувач не введе повідомлення для кодування і не натисне відповідну кнопку для його відправки.

Процес генерації бітового ряду, створеного за допомогою використання математичної моделі основаній на ентропії Колмогорова-Сіная, відбувається на STM платі. Розроблена математична модель складається з площини, до складу якої входить чотири кола та математичної точки. На рисунку 1 зображено візуальне представлення математичної системи.

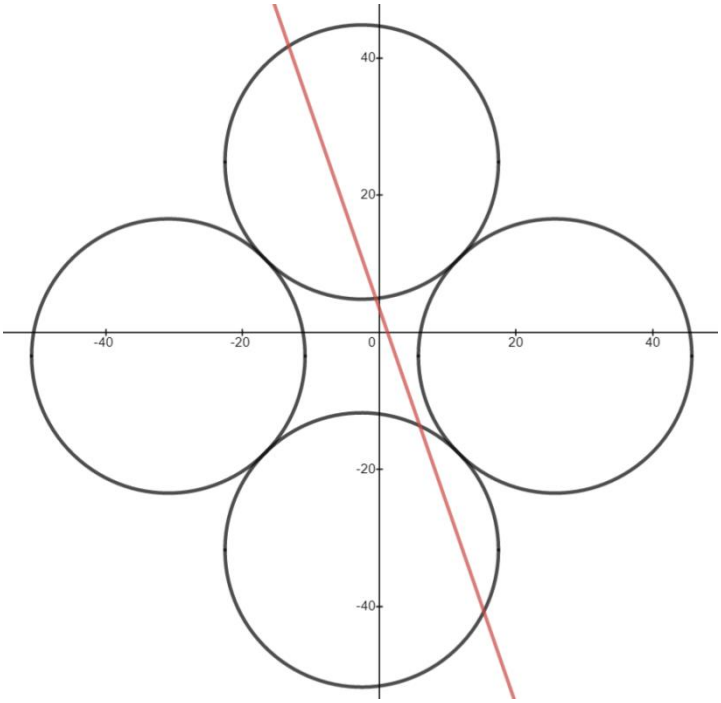


Рисунок 1 – Візуальне зображення математичної системи

Математична пряма рухається всередині простору, яке утворюють чотири кола. Формули кіл наведені у (1), (2), (3) та (4).

$$\big(x+(n+t)\big)^2+(y+p)^2=r^2, (1)$$
$$\big(x+(n-t)\big)^2+(y+p)^2=r^2, (2)$$
$$(x+n)^2+(y+(p-t))^2=r^2, (3)$$
$$(x+n)^2+(y+(p+t))^2=r^2 (4)$$

де n – параметр зміщення кіл по горизонталі,

p – параметр зміщення кіл по вертикалі,

r –радіус кіл,

t – коефіцієнт зсуву від центру, завдяки якому кожне коло буде мати єдину точку перетину з сусідніми колами. Формула даного коефіцієнту наведена у (5).

$$t=r\sqrt{2} (5)$$

З формул наведених у (1), (2), (3) та (4) видно, що до загальної формули кола додаються параметри зміщення по осям ординати та абсциси. Один з таких параметрів – t, є константним, потрібний для коректної побудови замкненої системи і залежить від радіусу, тоді як параметри n та p довільні та впливають на зміщення системи відносно початку координат. Всередині утвореної площини рухається математична точка, яка представлена у вигляді прямої, формула якої наведена у (6).

$$y=k\cdot x+b (6)$$

де k – кутовий коефіцієнт,

b – вільний коефіцієнт.

Додаток має змогу звернутися до мікроконтролеру із запитом на генерацію 64 байт інформації яка є частиною бітового ряду. У запиті необхідно вказати поточний системний час, який буде використано мікроконтролером для зміни первинного стану математичної системи. Завдяки зміні первинного стану математичної системи поточним часом, вдається досягти генерації унікального бітового ряду при кожному окремому запиті.

Повідомлення, введене користувачем на клієнтському додатку, перед відправкою проходить декілька стадій обробки. В першу чергу визначається кількість запитів до мікроконтролера. При кожному запиті клієнтський додаток визначає поточний системний час (таймкод) і використовує його як параметр запиту до мікроконтролера та зберігає його для подальшої відправки на серверний додаток. Отриманий у процесі генерації бітовий ряд відображається на графічному інтерфейсі користувача. Після генерації бітового ряду повідомлення кодується за допомогою побітової операції XOR. Закодоване повідомлення разом з таймкодами відправляється на серверний додаток. Серверний додаток використовуючи отримані таймкоди генерує бітовий ряд, який у випадку однакових первинних налаштувань математичних систем мікроконтролерів є аналогічний бітовому ряду отриманому на клієнтському додатку, і декодує повідомлення. Бітовій ряд разом в закодованим та декодованим повідомленням відображаються на графічному інтерфейсі користувача.

Для коректної роботи системи з можливістю відправки повідомлень необхідно мати декілька STM мікроконтролерів, один для серверного додатку та по одному для кожного клієнтського додатку. Також всі мікроконтролери повинні мати однакові початкові налаштування математичної системи.

Розробка структурної схеми

Розробка структурної схеми повинна відбуватися на початкових стадіях проектування і передувати розробці інших схем. На структурній схемі повинні бути відображені функціональні одиниці системи, їх переходи та призначення. При проектуванні структурної схеми не враховується справжнє розташування складових частин.

Для зображення ходу процесу, який відбувається у системі, її функціональні частини з’єднуються за допомогою стрілок.

На рисунку 2 зображено структурну схему клієнт-серверного програмного забезпечення для кодування інформації з використанням ентропії Колмогорова-Сіная. Блок математичного модулю який емулює ентропію Колмогорова-Сіная реалізований на мікроконтролері STM32F4.

Структурна схема програмного забезпечення включає у себе 3 блоки:

– Блок графічних операцій – демонструє всі можливі послідовні дії в роботі програми, які виводяться на графічний пристрій;

– Блок вихідних даних – відповідає за виведення результату;

– Блок вхідних даних – відповідає за введення даних у матриці;

Кожен з блоків складається з менших блоків, кожен з яких представляє реальні структурні компоненти. Напрям стрілок вказує на напрямок взаємодії компонентів між собою.

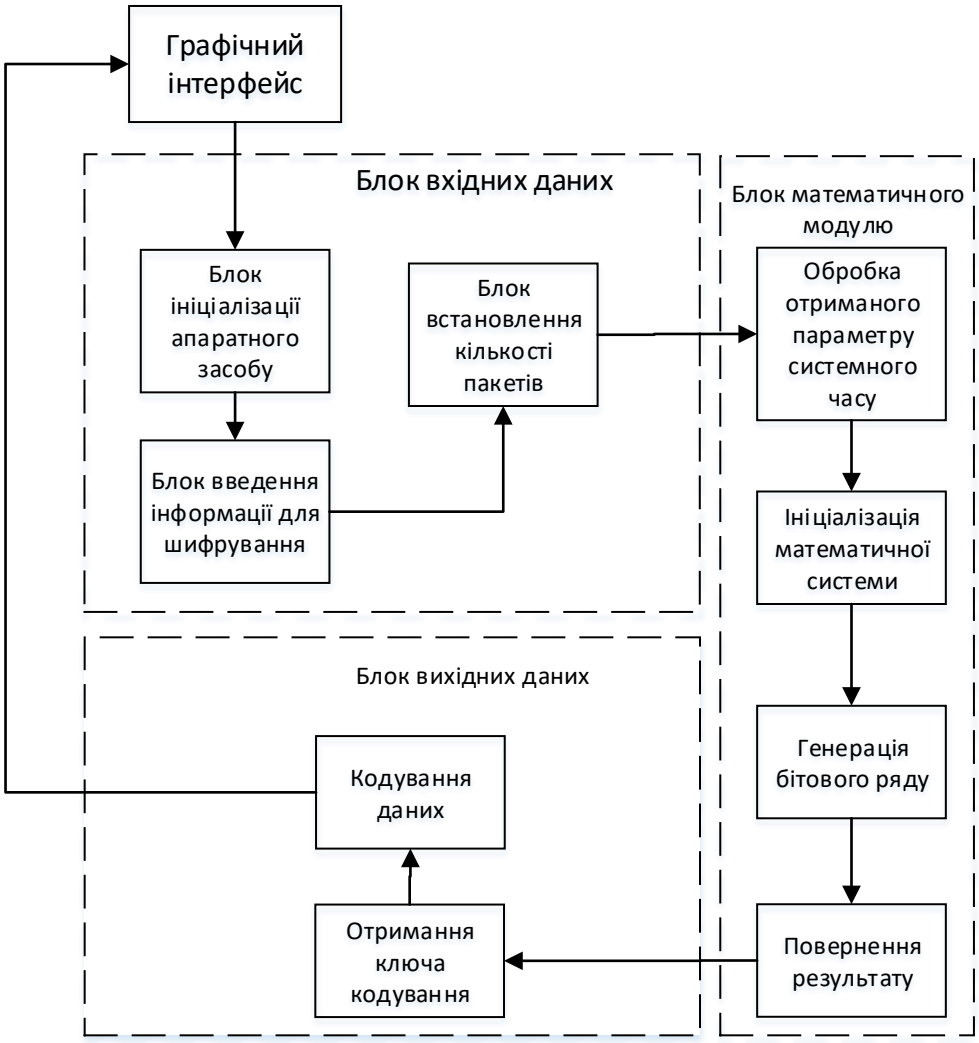


Рисунок 2 – Структурна схема системи

У системі наведені наступні функціональні частини:

– Блок ініціалізації апаратного засобу призначений для визначення наявності в системі мікроконтролеру на базі STM з коректними параметрами налаштування;

– Блок введені інформації для кодування. Завдяки ньому можливо ввести інформацію, яку програма буде кодувати;

– Блок встановлення кількості пакетів використовуючи дані, які були введені користувачем для кодування, встановлює необхідну кількість запитів до мікроконтролеру;

– Обробка отриманого параметру системного часу. Дана функціональна частина використовуючи отриманий системний час змінює початковий стан математичної системи;

– Ініціалізація математичної системи. Використовуючи початковий стан об’єктів системи ініцілізує її, перевіряючи можливість її вирішення. Якщо згенерована система не має рішень – програма певним чином за допомогою отриманого системного часу змінює початкові параметри так, щоб у системі існувало рішення і була можливість згенерувати бітовий ряд;

– Повернення результату. Завдяки даній функціональній частині математичний модуль повертає згенерований бітовий ряд до клієнт-серверного додатку;

– Отримання ключа кодування. Даний блок отримує дані від математичного модулю та генерує з них ключ кодування;

– Кодування даних призначене для кодування даних, введених користувачем за допомогою ключа кодування, згенерованного за допомогою моделювання на мікроконтролері математичної системи яка базується на ентропії Колмогорова-Сіная;

Графічний інтерфейс призначений для виведення результату роботи програми на екран.

Висновок. У статті розглянуто та проаналізовано програмне забезпечення, розроблене програмне забезпечення кодування інформації з використанням ентропії Колмогорова-Сіная для мікроконтролерів на базі STM та клієнт серверного додатку, який демонструє можливості кодування з використанням STM мікроконтролеру. Програмне забезпечення створене за допомогою об'єктного відходу програмування. Для реалізації клієнт-серверного додатку була використана мова програмування C#. Дана мова програмування надає можливість розробки у об'єктному стилі, завдяки чому вдалось розбити програму на модулі, що спростило загальне проектування системи. Математичний модуль, розроблений на базі математичної моделі ентропії Колмогорова-Сіная проходить більшість тестів на випадковість, завдяки чому можливо сказати, що створений ГПВЧ є стабільним, але потребує подальшого вивчення.

Список літератури

1. Нильс Фергюсон, Брюс Шнайер. Практическая криптография. – М.: Диалектика, 2004. – 432 с.
2. Баричев С. Г., Гончаров В. В., Серов Р. Е. Основы современной криптографии. 3-е изд. – М.: Диалог-МИФИ, 2011. – 176 с.
3. Джон Скит. C# для профессионалов: тонкости программирования. 3-е издание. – М.: «Вильямс», 2014. – 608 с.
4. Герберт Шилдт. C# 4.0: полное руководство. – М.: «Вильямс», 2010. – 1056 с.
5. Герберт Шилдт. Полный справочник по C++ = C++: The Complete Reference. – 4-е изд. – М.: Вильямс, 2011. – 800 с.
6. Бьёрн Страуструп. Дизайн и эволюция C++. – СПб.: Питер, 2007. – 445 с.
7. Бьёрн Страуструп. Язык программирования C++. Специальное издание The C++ programming language. Special edition. – М.: Бином-Пресс, 2007. – 1104 с.
8. Вернер М. Основы кодирования. Учебник для ВУЗов. – М.: Техносфера, 2004. – 288 с.
9. Березкин Е.Ф. Основы теории информации и кодирования. Учебное пособие. – М.: НИЯУ МИФИ, 2010. – 312 с.
10. Сидельников В.М. Теория кодирования. Справочник по принципам и методам кодирования. –М.: МГУ, 2006. – 289 с.

УДК 004

Д. Кононченко, магістр гр. КІ-18М-1,4
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ КОРПОРАТИВНОГО ЦЕНТРУ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ (SOC)

У статті розроблено програмне забезпечення, яке призначено для корпоративного центру управління інформаційною безпекою (SOC). Метою розробки є дослідження та програмна реалізація корпоративного центру управління інформаційною безпекою (SOC). Об'єктом дослідження є процес управління інформаційною безпекою. Предметом дослідження є методи управління інформаційною безпекою. Методи дослідження базуються на методах захисту інформації, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація корпоративного центру управління інформаційною безпекою (SOC). В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.
комп'ютерна інженерія, управління інформаційною безпекою, SOC

Постановка проблеми. Границі розподілених мереж швидко розмиваються, і організації змушені вирішувати складні завдання зі збору даних і керуванню ними від безлічі пристроїв, з їхнього контролю, обробки й зберігання в будь-якій точці планети, а також по масштабуванню й перерозподілу ресурсів для задоволення нових потреб. Поширення пристроїв Інтернету речей, хмарних обчислень, мобільних споживачів і онлайн-застосунків тільки прискорює ці зміни. У міру подальшого розширення й стирання границь мережі спостерігається збільшення числа й розмаїтості потенційних джерел погроз, які виникають частіше, стають усе більше розповсюдженими й здобувають комплексний характер. У результаті потенціал прориву системи безпеки сьогодні високий як ніколи. На жаль, успадковані методи, технології й процедури керування погрозами й реагування на порушення системи безпеки не дозволяють реалізувати стійкі й життєздатні стратегії захисту в сучасних динамічні й розподілених мережних середовищах. Незважаючи на безпрецедентні інвестиції в пристрої захисту, проломи продовжують зустрічатися повсюдно, у тому числі й там, де формально забезпечується «відповідність» стандартам. Все це приводить до виводу про те, що для ефективного функціонування сучасних мереж необхідні нові керівники, нове мислення, нові інструменти й нові процеси. Для одних організацій це стане спонукальним стимулом до створення корпоративного центра керування інформаційною безпекою (Security Operations Center, SOC) або розширенню його можливостей, інші зволіють звернутися до постачальників послуг аутсорсингу безпеки й керованих сервісів (Managed Service Provider, MSP).

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні корпоративного центру управління інформаційною безпекою (SOC).

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація корпоративного центру управління інформаційною безпекою (SOC).

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем управління інформаційною безпекою.

– Дослідження корпоративного центру управління інформаційною безпекою (SOC).

– Програмна реалізація корпоративного центру управління інформаційною безпекою (SOC).

Об'єктом дослідження є процес управління інформаційною безпекою.

Предметом дослідження є методи управління інформаційною безпекою.

Методи дослідження базуються на методах захисту інформації, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Протидія сучасним погрозам неможлива без адаптивного контролю, а також збору й зіставлення локальної й глобальної інформації, що дозволяє прогнозувати виникнення як уже існуючих, так і майбутніх погроз. Не менш важлива роль приділяється глибокому контекстно-залежному аналізу, що забезпечує більше швидке виявлення погроз і своєчасне реагування на них.

Якщо організація створює SOC уперше, потрібно чітко розуміти виклики, з якими їй має бути зштовхнутися й вплив яких бажано мінімізувати:

– Кількість і складність погроз ростуть. Моніторинг середовища дуже швидко веде до інформаційного перевантаження фахівців з безпеки: тривожних сигналів занадто багато, і немає простих способів їх ранжувати.

– Ефективно захистити все без винятку неможливо.

– Розподіл відповідальності між IT-групами, динамічна зміна мереж і роздроблена інфраструктура безпеки обмежують можливості контролю критично важливих активів і процесів компанії.

– Багато які SOC розвивалися природно, при цьому процеси, інструменти й методології розроблялися в міру необхідності, причому найчастіше вручну. Недостатня

автоматизація знижує можливості швидкого реагування на погрози з метою запобігання компрометації мережі.

– Неповне подання про супротивників у сфері безпеки не дозволяє прийняти адекватні рішення.

– Зростаючий розрив у рівні кваліфікації фахівців утрудняє керування середовищем і підвищує уразливість мереж.

Центр керування інформаційною безпекою

Де-факто SOC складається із трьох взаємозалежних стандартних компонентів: людей, процесів і технологій.

Люди. У вашім розпорядженні можуть бути самі нові технології й процеси, але цього недостатньо – потрібні грамотні фахівці, які могли б ефективно управляти SOC. Вони повинні не тільки мати технічні навички, але й уміти взаємодіяти з керівництвом і мати навички спілкування. Для втримання кваліфікованих співробітників потрібно організовувати навчання й створювати умови, що дозволяють їм реалізувати свої кар'єрні устремління. Необхідно працювати з усіма, хто має доступ до мережі, – з персоналом компанії, клієнтами й постачальниками.

Процеси. Правильно певні процеси важливі не менше, ніж люди. Гарні процеси – це база для досягнення бажаної продуктивності й ефективності. Вони повинні регулярно піддаватися аналізу й підкріплюватися грамотним керуванням, технологіями, операційними стандартами й контролем ключових показників ефективності.

Технології. Важлива роль приділяється й технологіям, застосовуваним в SOC. Для ефективного виявлення погроз необхідно визначити, які знадобляться продукти, типи даних про події, інструменти кореляції й додаткові ситуативні джерела інформації.

Зупинимося на кожному із цих компонентів більш докладно.

Люди

Насамперед варто поговорити про директорат і акціонерів, оскільки саме вони повинні бути залучені в загальну програму зміцнення безпеки й підвищення її ефективності в контексті реалізації стратегічних ініціатив. Саме їм доведеться ухвалювати рішення щодо того, що важливо для них, для бізнесу, для співробітників і клієнтів. Ці люди можуть стати основними союзниками в справі підвищення ефективності SOC, тому важливо, щоб вони були залучені в процес безперервної модернізації.

Залежно від розмірів SOC членам команди приділяються різні ролі. У великих центрах на кожній позиції потрібні фахівці, що розуміють, хто і як класифікує інциденти. У невеликих SOC кожний учасник виконує відразу кілька функцій. Чіткий розподіл завдань повинне гарантувати, що жоден аспект керування SOC не буде забутий.

Потрібно врахувати, що до персоналу SOC пред'являються дуже високі вимоги, багато співробітників швидко утомлюються й втрачають ентузіазм. Регулярне підвищення кваліфікації й навчання декільком спеціальностям мають істотне значення для підтримки мотивації. Крім того, кожний член команди повинен чітко розуміти, який може бути його кар'єру.

Процеси

SOC вимагає спеціальних процесів для бізнесу, технологій, операцій і аналітики.

Бізнес-Процеси. Вони визначають загальний напрямок діяльності SOC. На цьому етапі формулюються цілі й завдання, а також задаються пріоритети й функції. Звичайно все це робиться ще до початку створення центра. До критично важливих бізнес-процесам ставляться наступні:

Спонсор проекту. Головне завдання спонсора полягає в тім, щоб переконати в необхідності створення SOC директорів компанії й керівників окремих підрозділів у ході освітніх семінарів, тренінгів і т.д. Без підтримки керівництва ймовірність успішної побудови SOC невелика. Важливе значення в ході обґрунтування має визначення цілей і причин створення SOC.

Місія й орієнтири. Сюди ставиться визначення зон відповідальності, конкретних завдань і замовників. Формулювання, приміром, може звучати так: «Надання 24 години на добу й 7 днів у тиждень послуг, спрямованих на підвищення рівня безпеки всієї організації на основі безперервного моніторингу, за результатами якого будуть здійснюватися виявлення інцидентів і протидія їм з метою зниження ризиків і наслідків впливу потенційних кіберзагроз. У число цих функцій входить керування всіма мережними пристроями й засобами безпеки, включаючи робітники станції, мобільні пристрої й системи.

Цілі й завдання. Цілі й завдання SOC можуть включати, наприклад, виявлення кіберінцидентів і порушень системи безпеки, профілактику інцидентів, доповідь керівництву про поточну ситуацію, а також безперервне поліпшення безпеки на основі почерпнутих уроків.

Функції. Функції SOC забезпечують виконання місії й досягнення бізнес-цілей. Як приклад можна привести реєстрацію інцидентів, контроль за дотриманням нормативних вимог, керування конфігурацією (скажемо, при зміні правил міжмережного екрана й системи запобігання вторгнень), а також відновлення уразливих систем.

Заходи й зони відповідальності. Тут описується повсякденна діяльність у рамках кожної функції й визначаються ролі персоналу SOC. Так, контроль за дотриманням нормативних вимог може передбачати створення й моніторинг відповідних інструментальних панелей SIEM, формування й перегляд звітів про дотримання необхідних норм, а також забезпечення правильної конфігурації ресурсів.

Проконтролювати й захистити все компоненти середовища практично неможливо. Тому прийде визначати пріоритети для ключових бізнес-процесів, виділяти для них необхідні ресурси й конкретизувати важливі або дані, що підпадають під вимоги регулятора.

Суб'єкти, від яких виходить погроза. З'ясувавши, які дані циркулюють у вашім середовищі, ви зможете зрозуміти, які суб'єкти зацікавлені в їхньому викраденні. Хто вони? У чому їхній інтерес? Якими можливостями вони володіють і яка їхня тактика?

До суб'єктів, від яких виходить погроза, ставляться державні й галузеві кібершпигуни, організована злочинність, хактивисти, деструктивні інсайдери, безпринципні хакери, вандали, зломщики-дилетанти. Сюди ж можна віднести помилки користувачів.

Метрики. Щоб визначити ефективність SOC, вам доведеться описати показники продуктивності й ризиків. Метрики повинні бути конкретними, вимірними, доступними, актуальними й своєчасними. До високорівневих завдань для їхнього створення ставляться визначення ключових показників ефективності (KPI), ідентифікація основних вузлів для збору даних, опис нормального функціонування мережі, а також установлення цільових діапазонів, порядку розрахунку KPI і періодичності звітів.

Технологічні процеси

Багато продуктів установлюються й управляються некоректно, тому ви не одержуєте повноцінної віддачі від своїх технологічних інвестицій. Організація технологічних процесів забезпечує ефективне конфігурування, адміністрування технології й керування нею протягом усього її життєвого циклу.

Проектування мережі й сегментація. Розуміння того, як спроектована мережа, особливо в частині підключення пристроїв, розподілу потоків і місцезнаходження даних, усе більше ускладнюється через ріст хмарних мереж, віртуалізації даних, наявності віддалених вузлів, мобільних працівників і портативних пристроїв, підключень бізнес-партнерів і тіньових IT.

Складання карти мережі й потоків даних допомагає виявити можливі шляхи атаки й дозволяє створити основу для розгортання датчиків, точок збору даних, інструментів керування й аналізу. Крім того, наявність такої карти дозволяє з більшою ефективністю здійснити сегментування мережі й виділити логічні зони безпеки й проходження трафіку.

От простий приклад сегментації мережі:

– Незахищена зона. Містить невідомі й неконтрольовані системи, наприклад пристрою в Інтернеті.

– Демілітаризована зона. Область, що захищається, доступна для невідомих і неконтрольованих пристроїв, які запитують доступ до ресурсів мережі. Тут важливо фільтрувати й відслідковувати вхідний і вихідний трафік.

– Довірена зона. Внутрішня область для корпоративних систем, де перебувають поштова система, файлові сервери й корпоративні мережні пристрої.

– Зона з обмеженим доступом. Тут розташовуються системи, доступ до яких обмежений у силу важливості й конфіденційності даних. Найчастіше на такі області поширюються вимоги регулювальних органів. Сервери, установлені в цій зоні, не повинні мати доступу до Інтернету.

– Підзони. Усередині зони з обмеженнями доступу можна створити додаткові зони, при цьому необхідно забезпечити належне керування ними і їхній моніторинг.

Керування конфігурацією. Багато мережних проломів виникають через неправильно зконфігуровані пристрої. Споконвічно конфігурації пристроїв можуть бути безпечними, але після чергових змін у них з'являються уразливі місця. От чому необхідно управляти процесом конфігурації й контролювати зміни, які повинні вноситися тільки авторизованими користувачами й відповідати корпоративній політиці.

Контроль за змінами передбачає виконання чітко певних завдань: документування поточних конфігурацій мережних пристроїв, деталізацію будь-яких внесених змін з обґрунтуванням цілі, підтримку архіву колишніх конфігурацій (дозволяє повернути пристрою у відомий безпечний стан), визначення політик керування темпами змін і реєстрацію осіб, що володіють необхідними повноваженнями для внесення змін і повернення в попередні стани.

Операційні процеси. Атаки відбуваються швидко, а шкідливі програми звичайно запускаються автоматично, тому SOC повинен оперативно розпізнавати погрози й реагувати на них. Впровадження операційних процесів і процедур допомагає стандартизувати повсякденні операції, підвищуючи ефективність SOC. Там, де це можливо, для виконання повторюваних завдань потрібно використовувати технології автоматизації.

Процедури для контролю змінюваності персоналу. Незалежно від того, чи є у вашім SOC кілька категорій аналітиків або ж всі нечисленні аналітики мають той самий статус, важливо забезпечити контроль за роботою персоналу. Сюди ставляться процедури пересмінки (ведення журналів і виконання відновлень), складання розкладу змін із вказівкою конкретних співробітників, визначення процедур реєстрації відвідувачів. Деякі із цих процедур, наприклад системи фіксації інцидентів, повинні підтримуватися технологіями постачальників.

Плани реагування на інциденти. Процедури реагування на інциденти (Incident Response, IR) забезпечують вибір правильного рішення, документування й звітність по всіх прийнятих мірах і додаткових розслідуваннях інцидентів, пов'язаних з безпекою. Тут потрібні правильна ідентифікація, точне документування й збір доказів.

Плани розподілу ресурсів. Планування ресурсів дозволяє виділяти така кількість персоналу, який виявилося б досить для боротьби з певним обсягом погроз. Вибір і впровадження відповідних технологій допоможуть вирішити питання, пов'язані з ресурсами й бюджетом, а ранжирування інцидентів буде сприяти підвищенню ефективності процесів і мінімізації чисельності персоналу, що підтримує SOC.

Фізичний доступ. SOC є критично важливим ресурсом, тому фізичний доступ необхідно ретельно контролювати за допомогою карт доступу, цифрових замків і біометричних параметрів. Інструменти контролю фізичного доступу повинні реєструвати моменти входу й виходу персоналу SOC у журналах аудита.

Аналітичні процеси. Дуже важливо мінімізувати число дорогих помилок і промахів, пов'язаних з ідентифікацією й вирішенням інцидентів в області безпеки. Для рішення цього завдання в більшості організацій передбачаються формальні документовані процеси, яких повинні дотримуватися аналітики. Серед іншого в них вказуються порядок і строки

інформування керівництва про виявлені інциденти. До аналітичних процесів ставляться формування звітів, організація керування, а також аналіз вторгнення й шкідливих програм.

Формування звітів. Це один з найважливіших сервісів SOC, що забезпечує постійний контроль за ситуацією й виявлення високопріоритетних ризиків і погроз. Для рішення цього завдання звіти необхідно створювати як для персоналу, так і для керівництва. Більшість із них повинні генеруватися автоматично, орієнтуватися на конкретну аудиторію й містити аналіз тенденцій, що допомагає виявляти аномалії, які в загальному випадку не видні.

Аналіз шкідливих програм. Для розуміння контексту інциденту аналітикам SOC потрібні інструменти й навички, які допомагали б аналізувати шкідливі програми й виявляти правопорушення. Рівень фінансування й кваліфікації співробітників найчастіше недостатній для створення повноцінної лабораторії аналізу шкідливих програм. Як компенсація використовується технологія «пісочниці», що дозволяє автоматизувати процес аналізу шкідливого коду, і встановлюються додаткові засоби виявлення на міжмережних екранах, прикінцевих вузлах і в поштових системах. В ідеалі команда SOC повинна мати необхідні навички й використовувати новітню технологію «пісочниці».

Розробка структурної схеми

Інтегровані рішення керування безпекою

Створення SOC починається з розуміння особливостей вашого бізнесу, для чого необхідно відповісти на ряд важливих питань. Які ініціативи висуває сьогодні ваша компанія? Наскільки критична кожна з них для розвитку бізнесу? Що потрібно відслідковувати й контролювати? Які цільові показники підвищення продуктивності? Які з можливих проектів мають потребу в розгляді й реалізації? Якими існуючими й майбутніми ризиками потрібно управляти? Який рівень ризику вважається прийнятним для досягнення успіху?

Ми почали зі створення цілісної системи безпеки Security Fabric. Вона базується на загальній операційній системі й інтегрованих рішеннях, тому її можна динамічно адаптувати до потреб, що змінюються, IT-інфраструктури й захищатися від швидко розвиваються й непередбачених атак. Fabric допомагає грамотно й прозоро ділити мережа на сегменти й мікросегменти й глибоко інтегрувати в розподілене середовище передові засоби захисту проти складних погроз. Оскільки інструментарій заснований на загальному наборі відкритих стандартів, кожний елемент системи безпеки здатний взаємодіяти з усіма іншими елементами, що дозволяє обмінюватися політиками, примусово застосовувати їх, інтегрувати відомості про погрози, розуміти інформацію потоку застосунків і автоматично синхронізувати скоординовану відповідь на виявлені погрози.

До ключових компонентів Security Operations ставляться Analyzer, Manager, Guard Threat Intelligence і SIEM.

Analyzer забезпечує централізований аналіз даних, зібраних мережними пристроями й засобами безпеки, а також більше швидке й точне розпізнавання погроз.

Manager дозволяє персоналу SOC і центра керування мережею (Network Operations Center, NOC) ініціювати й синхронізувати скоординована відповідь на виявлені пристроями погрози незалежно від того, яка частина мережі була скомпрометована.

Guard Threat Intelligence динамічно додає інформацію про глобальні погрози до профілю атаки, забезпечуючи своєчасне й точне розпізнавання погроз у реальному часі.

SIEM формує для команди SOC централізоване подання про те, що необхідно зробити для поліпшення керування всією розмаїтістю швидко мінливих середовищ, призначених для забезпечення безпеки, функціональності, дотримання нормативних вимог і задоволення потреб бізнесу. За допомогою запатентованої технології виявлення погроз у реальному часі виконується порівняння результатів аналізу NOC і SOC, завдяки чому рішення SOC краще «розуміють» контекст свого середовища.

Формат віртуального програмно-апаратного комплексу SIEM пропонує просте й швидке розгортання рішення, забезпечуючи автоматичну інтеграцію сотень операційних і мережних пристроїв, а також апаратних засобів безпеки, у тому числі не стосовних до

сімейства net. Розвинені можливості виявлення підключених до мережі пристроїв і автоматизованого визначення їхньої конфігурації дозволяють сформувати динамічну централізовану базу керуючих даних (Dynamic Centralized Management Database, CMDB). Надалі зібрана інформація про погрози аналізується в контексті подій з використанням Guard Threat Intelligence і відомостей про погрози, надаваних незалежними постачальниками.

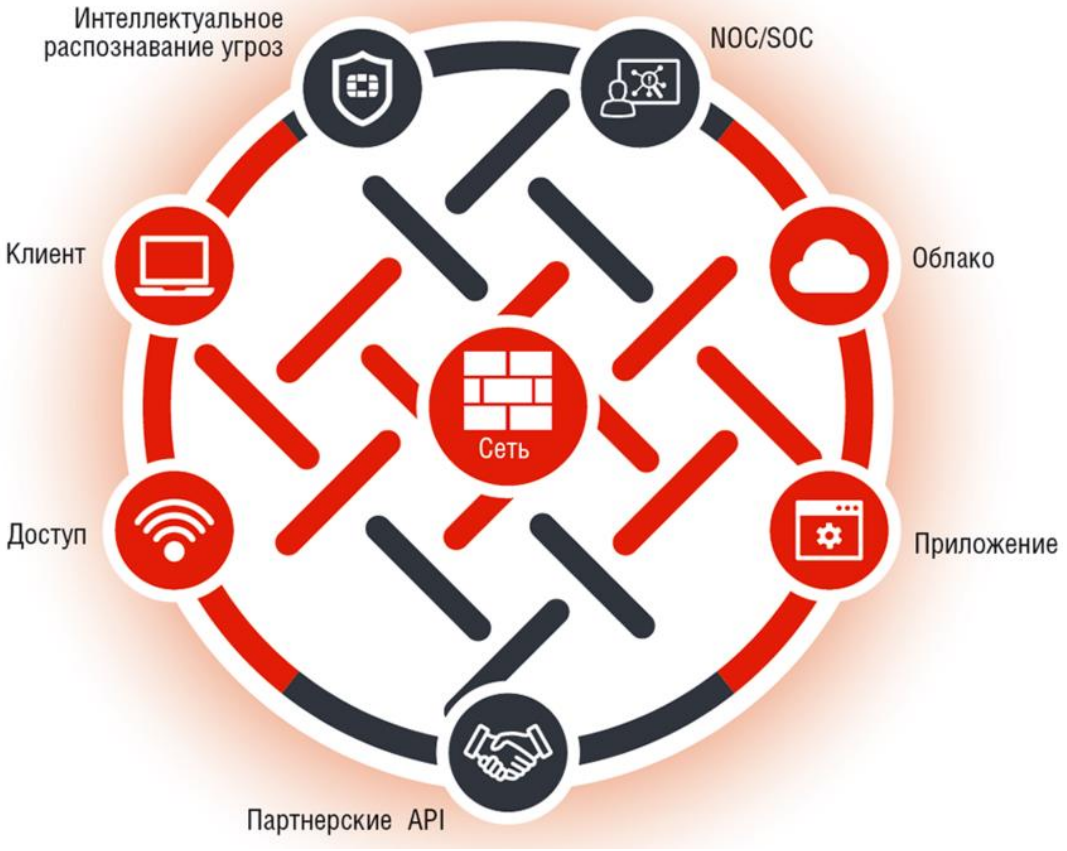


Рисунок 1 – Структурна схема системи

SIEM надає готові звіти для всіх типових ситуацій (у тому числі з урахуванням вимог стандартів і регуляторів), а також для керування бізнес-застосунками. Крім того, для формування звітів про окремі мережні сегменти й віртуальних або логічних середовищах підтримується архітектура із множинною орендою. Всіма цими можна способами управляти з єдиної консолі, що спрощує й прискорює виявлення погроз. Масштабована архітектура гарантує безперервну обробку постійно зростаючого обсягу записів у журналах і даних про події.

Об'єднаний набір рішень, інтегрований з динамічною й гнучкою структурою Security Fabric, дозволяє виконувати моніторинг прикінцевих вузлів, рівня доступу, застосунків, мережі, ЦОДа й хмари й здійснювати керування ними в рамках єдиного рішення безпеки, що забезпечує адаптивне подання, контроль і аналіз, необхідні навіть у самих складних середовищах SOC.

Технології

Крім людей і процесів, SOC будуть потрібні технології забезпечення безпеки. Ці інструменти мають вирішальне значення для виявлення погроз і вживання відповідних заходів. Наявність арсеналу пристроїв безпеки дуже важливо для нормального функціонування мережі й застосування вироблених політик, але для досягнення необхідної ефективності необхідно збирати й аналізувати дані про події, розуміти характер шкідливого поводження, а також мати можливість ефективно корелювати інформацію, зібрану з локальних пристроїв, з наявними відомостями про глобальні погрози.

Пристрої для забезпечення безпеки. Без сумніву, якісь пристрої для забезпечення безпеки вже працюють у мережі вашої організації. Дуже важливо в інвентаризувати наявні

ресурси для ідентифікації проломів з урахуванням потенційних зловмисників, яким може бути цікавий ваш бізнес, критичності оброблюваних і збережених даних, вимог наглядових органів і ваших можливостей по впровадженню існуючих інструментів з метою збору більше повних відомостей і видачі координованої відповіді на виявлені погрози.

Критичним ядром будь-який SOC є рішення для керування інформаційною безпекою й подіями безпеки (Security Incident and Event Management, SIEM). Всі інші системи безпеки повинні бути підлеглі цієї технології.

Крім SIEM, ефективному SOC знадобляться багато інших інструментів:

– міжмережний екран нового покоління (Next-Gen Firewall);

– система запобігання вторгнень (IPS);

– засобу захисти Web-застосунків (WAF), баз даних (Database Protection), Web і електронної пошти (Web and E-mail Security), а також окремих хостів (Host Protection);

– засоби виявлення погроз і протидії їм на кінцевих точках (Endpoint Detection and Response, EDR), запобігання втрати даних (Data Loss Prevention, DLP), забезпечення безпеки мобільних пристроїв (Mobile Device Security, MDM), розслідування комп'ютерних інцидентів і злочинів (Host Forensics) і контролю за доступом до мережі (Network Access Control, NAC);

– сканери уразливостей (Vulnerability Scanners);

– системи керування обліковими даними (Identity Management (Id) Systems) і активами (Asset Management), моніторингу баз даних (Database Monitoring);

– а також інші технології, що розвиваються, для аналізу безпеки.

Технології безпеки вибирають не тільки заради функцій захисту. Для нейтралізації сучасних складних і розподілених атак потрібна комплексна архітектура на базі відкритих рішень, що підтримують взаємодію й обмін інформацією, автоматичну реакцію на виявлені локальні проломи, а також участь у погоджених централізованих відповідних мірах.

Дані про події. SIEM повинна «бачити» і збирати інформацію від різних мережних засобів. Важливо розуміти, дані якого типу потрібні для одержання ясної картини. Більш точно оцінити ситуацію допомагають оповіщення й записи, реєструємі в журналах, сеансові дані, повна інформація про пакети, а також статистична інформація. Чим вище поінформованість, тим краще аналіз.

Контекстна інформація. Сюди ставляться дані про користувачів і застосунки, відомості про уразливості і аномалії, а також класифікація активів і визначення їхньої важливості. Наявність цієї додаткової контекстної інформації дозволяє розставити пріоритети й зрозуміти, які повідомлення варто переглядати в першу чергу.

Зовнішні джерела відомостей про погрози. Домігшись гарної поінформованості про стан внутрішньої мережі, можна оформити передплату на одержання інформації про існуючі погрози. Відповідні розсилання звичайно містять відомості про підозрілі IP-адреси, URL, домени, хеш-функції і навіть зміни у процесах і реєстрі. Система SIEM повинна бути здатна приймати цю інформацію й зіставляти її з локальними даними. Це дозволить визначити, чи підтримує пристрій зв'язок з відомим джерелом погроз або скомпрометованою системою.

Кореляція. Об'єднання всієї зібраної інформації – центральна функція будь-якого SOC. Як правило, чим більшим обсягом інформації ви розташовуєте, тим краще створюваного правила кореляції й прийняті рішення. На щастя, у більшості технологій SIEM присутні заздалегідь певні правила кореляції, які можна скорегувати з урахуванням унікальних особливостей вашої мережі. Крім того, системи SIEM повинні формувати сценарії використання, що є логічним компонентом звітів SIEM. Сценарій може бути правилом, звітом, попередженням або інструментальною панеллю для рішення конкретних завдань і задоволення певних потреб. Створення сценаріїв – це безперервний процес, якість якого згодом підвищується.

Висновок. У статті розглянуто та проаналізовано програмне забезпечення, яке призначено для корпоративного центру управління інформаційною безпекою (SOC). В межах України в недостатній мірі представлені вітчизняні розробки в цій області. У роботі наведені теоретичне узагальнення й рішення наукового завдання дослідження методів

управління інформаційною безпекою. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем управління інформаційною безпекою; Досліджена система управління інформаційною безпекою; На основі отриманих результатів досліджень створена програмна реалізація корпоративного центру управління інформаційною безпекою (SOC). Розроблені під час виконання роботи алгоритми дозволяють успішно вирішувати завдання управління інформаційною безпекою. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки. Розроблене програмне забезпечення має простий, дружній та зручний інтерфейс користувача, що забезпечує легкість у освоєнні роботи програмного продукту, зручність у використанні, і не потребує особливих спеціальних знань. При створені програмного забезпечення було використано об'єктно-орієнтований підхід, що відповідає сучасним тенденціям у галузі розробки комерційних програмних систем. Програма реалізована на мові високого рівня Embarcadero Embarcadero Delphi 10.2 Tokyo 10.2 Tokyo. Дана мова програмування дозволяє найбільш ефективно обробляти дані. Це дозволило мінімізувати строк розробки програмного забезпечення, і, як слід, зменшити витрати на його розробку. Запропоноване програмне забезпечення ділиться на загальне програмне забезпечення, що поставляється із засобами обчислювальної техніки й спеціальне програмне забезпечення, що спеціально розроблене для даної конкретної системи й включає програми, що реалізують її функції. Даються необхідні рекомендації з установки розробленого програмного забезпечення. Для підвищення рівня безпеки запропоновано застосовувати алгоритм REDOC III.

Список літератури

1. Смирнов А.А. Анализ и сравнительное исследование перспективных направлений развития цифровых телекоммуникационных систем и сетей / А.А.Смирнов, В.В.Босько, Е.В.Мелешко // Системи обробки інформації. – Х.: ХУ ПС, 2008. – Вип.7(74). – С.120-123.
2. Смирнов А.А. Усовершенствование метода управления очередями в многопротокольных узлах телекоммуникационной сети / А.А.Смирнов, Е.В.Мелешко // Збірник тез та доповідей другої всеукраїнської науково-практичної конференції «Системний аналіз. Інформатика. Управління». Запоріжжя. Тези доповідей. Запоріжжя: КПУ, 2011.
3. Смирнов С.А. метод безопасной маршрутизации метаданных в облачные антивирусные системы / А.К. Дидык, С.А. Смирнов // Информационные технологии в управлении, образовании, науке и промышленности: монография / Под редакцией профессора В.С. Пономаренко. – Х.: Видавець Рожко С.Г., 2016. – 566 с.
4. Смирнов С. А. Сравнительные исследования математических моделей технологии распространения компьютерных вирусов в информационно-телекоммуникационных сетях / Мохамад Абу Таам Гани, А. А. Смирнов, А. В. Коваленко, С. А. Смирнов // Системи обробки інформації: зб. наук. праць. – Х.: ХУПС, 2014. – Вип. 9(125). – 105-110.
5. Смирнов С. А. Математическая модель интеллектуального узла коммутации с обслуживанием информационных пакетов различного приоритета / Мохамад Абу Таам Гани, А. А. Смирнов, Н. С. Якименко, С. А. Смирнов // Збірник наукових праць Харківського університету Повітряних Сил. – Харків: ХУПС, 2014. – Вип. 4 (41). – С. 48-52.
6. Смирнов С. А. Исследование показателей качества функционирования интеллектуальных узлов коммутации в телекоммуникационных системах и сетях / Мохамад Абу Таам Гани, А. А. Смирнов, Н. С. Якименко, С. А. Смирнов // Наука і техніка Повітряних Сил Збройних Сил України: наук. журн. – Х.: ХУПС, 2014. – № 4(17). – С. 90-95.
7. Смирнов С. А. Усовершенствованный алгоритм управления доступом к «облачным» телекоммуникационным ресурсам / Мохамад Абу Таам Гани, А. А. Смирнов, Н. С. Якименко, С. А. Смирнов // Системи обробки інформації: зб. наук. праць. – Х.: ХУПС, 2015. –Вип. 1(126). – С. 150-153.
8. Smirnov S.A. Method of controlling access to intellectual switching nodes of telecommunication networks and systems / A.A. Smirnov, Mohamad Abou Taam, S.A. Smirnov // International Journal of Computational Engineering Research (IJCER). – **Volume 5, Issue 5. –** India. Delhi. – 2015. – P. 1-7.
9. Смирнов С. А. Анализ и исследование методов управления сетевыми ресурсами для обеспечения антивирусной защиты даннях / Мохамад Абу Таам Гани, А. А. Смирнов, С. А. Смирнов // Системи озброєння і військова техніка: наук. журн. – Х.: ХУПС, 2015. – № 3(43). – С. 100-107.

10. Смирнов С. А. Исследование эффективности метода управления доступом к облачным антивирусным телекоммуникационным ресурсам / Мохамад Абу Таам Гани, А. А. Смирнов, С. А. Смирнов // Наука і техніка Повітряних Сил Збройних Сил України: наук. журн. –Х.: ХУПС, 2015. –№ 3(20). – С. 134-141.
11. Смирнов С. А. Комплекс gert-моделей технологии облачной антивирусной защиты телекоммуникационной системы / А. А. Смирнов, А. К. Дидык, А. Н. Дреев, С. А. Смирнов // Безпека інформації: наук. – практ. журн. – К.: НАУ, 2015. – Т. 21, № 3. – С. 251-262.

УДК: 633.35:631.87

О. Корик, магістр гр. АГ-18М-1,9
В. Резніченко, канд. с.-г. наук, доц.
Центральноукраїнський національний технічний університет

ПІДВИЩЕННЯ ПРОДУКТИВНОСТІ СОЧЕВИЦІ ЗА РАХУНОК МІНЕРАЛЬНОГО ЖИВЛЕННЯ

Проаналізовано сучасні технології вирощування сочевиці на території України із застосуванням різних доз мінеральних добри та їх вплив на урожайність досліджуваної культури
сочевиця, дози мінеральних добрив, азот, фосфор, калій

Враховуючи особливості ведення сільськогосподарського виробництва агрохімічні властивості ґрунту знижуються щорічно, в результаті чого спостерігається зменшення вмісту гумусу, від'ємний баланс азоту, фосфору, калію, мікроелементів, і, як наслідок, зниження врожаїв сільськогосподарських культур.

Для сочевиці, як і для інших культур, при застосуванні мінеральних добрив необхідно, враховувати агрохімічний аналіз ґрунтів на вміст доступних елементів живлення. Але слід враховувати, що сочевиця слабо реагує на застосування добрив. При високому вмісті азоту в грунті азотфіксація не відбувається, а при значній кількості вологи азот сприяє наростанню зеленої маси, а кількість бобів та насіння при цьому буває незначною.

Азоту для формування врожаю 2 т/га зерна сочевиці потрібно в середньому в межах 100 кг азоту. За нормальної азотфіксації сочевиця може забезпечити до 50-80% своєї потреби в азоті за рахунок фіксації азоту бульбочковими бактеріями, а решту вона засвоює з ґрунту. Проте, якщо в ґрунті азотозабезпечення нижче 17 кг/га, початковий ріст рослин буде повільним, у рослин відмічається жовте забарвлення листків протягом певного періоду часу із-за нестачі вологи. Тому при сівбі на таких полях бажано вносити до 20 кг/га азоту. Хоча стартова доза азоту на початковій стадії розвитку рослин сприятиме їх кращому росту, істотної прибавки врожаю можна не отримати. Необхідно, також враховувати те, що якщо сочевицю вирощують на полі вперше, а гідротермічні показники відносяться до посушливих, то надмірні дози азоту сприятимуть наростанню надмірної вегетативної маси культури, що може викликати не реалізацію генетично обумовленого потенціалу врожаю насіння. Якщо ж будуть спостерігатися підвищена вологість, то за густої вегетативної маси будуть створюватися сприятливі умови для розвитку інфекційних захворювань.

Важливо зазначити, що за краще розвиненої вегетативної маси, рослини будуть вищими і відповідно висота кріплення бобів буде вищою, що в певній мірі полегшить збір врожаю [20].

Фосфор – важливий елемент для живлення сочевиці, хоча й потребує культура його в невеликій кількості. Для формування врожаю насіння 2 т/га потрібно в межах 20 кг фосфору. Фосфор, активно сприяє розвитку кореневої системи, що відповідно в подальшому позитивно відобразиться на всій рослині, в цілому. В подальшій вегетації, активно впливає на процес азотфіксації та сприяє одночасному та швидкому дозріванню насіння [1].

Що стосується калію, то зазвичай його кількість міститься в достатній кількості у всіх ґрунтах. Для формування врожаю сочевиці 2 т/га необхідно близько 85 кг/га K_2O. Зазвичай калій вносять, як припосівне добриво [1, 2].

В своїх дослідженнях Адамень Ф.Ф. зазначає, що в середньому на формування 1 т зерна сочевиця виносить з ґрунту 58 кг азоту, 20 - фосфору та 28 – калію [3].

Урожайність сочевиці значною мірою залежить від застосування фосфорних і калійних добрив. Враховуючи високу фізіологічну активність її кореневої системи, під основний обробіток опідзолених чорноземів, дерново-підзолистих ґрунтів раціонально вносити з фосфорних добрив фосфоритне борошно в дозі 45 - 60 кг/га за д. р. Проте на чорноземних ґрунтах краще вносити суперфосфат в указаній дозі діючої речовини. Калійні добрива дають також з розрахунку 45 - 60 кг/га за д. р. Безпосередньо під неї гній не вносять, так як при цьому вона розвиває велику зелену масу і знижує врожай зерна. При посіві використовують гранульований суперфосфат [3, 4].

Сочевиця найбільш чутлива до фосфорних та калійних добрив. Калійні добрива особливо ефективні на легких супіщаних і піщаних ґрунтах, а також в сівозмінах з великою питомою вагою картоплі, коренеплодів, соняшнику і силосних культур, які виносять з ґрунту велику кількість фосфору і калію. Азотні добрива, як правило, під сочевицю не вносять вони, як і гній, викликають інтенсивний розвиток зеленої маси, затягують цвітіння і дозрівання, знижуючи урожай насіння. Однак в перші фази вегетації рослин внесення їх в невеликій кількості (10-15 кг/га діючої речовини) цілком доцільно. В цьому випадку їх застосовують поверхнево, краще після появи сходів сочевиці [5, 6].

Сочевиця є перспективною культурою для умов зони ризикованого землеробства, але для забезпечення стабільних урожаїв культури необхідно забезпечити її надходженням поживних речовин протягом вегетаційного періоду.

Високі врожаї зернобобових культур можна одержати лише при оптимальному забезпеченні рослин тепловими і водними ресурсами, а також необхідними для росту та розвитку елементами живлення. Якщо впродовж вегетаційного періоду навіть тимчасово порушити оптимальний хід життєвих процесів у рослин, то інтенсивність зниження рівня врожайності буде суттєво залежати від взаємодії рослини і середовища. Одержання високих урожаїв забезпечується системою заходів, орієнтованих на створення належних умов для повноцінного росту та розвитку рослин. Відомо, що найпродуктивнішою зернобобовою культурою (за кількістю бобів) є сочевиця. Навіть у вкрай посушливі роки на одній рослині сочевиці може сформуватися до 20–24 бобів, в той час як у гороху, чини і нуту – по 3–5 бобів [7, 8].

Ріст рослин – важливий процес для дослідження, і перш за все, особливостей нагромадження ними вегетативної маси, формування кореневої системи, генеративних органів, а відтак – і величини врожаю.

Дослідження проведені в Полтавській ДСГДС ім. М. І. Вавилова впродовж 2012–2013 рр. показали, що внесення мінеральних добрив призводило до збільшення висоти рослин сочевиці на 3,3–3,4 %, за рахунок інокуляції насіння та підживлення рослин її показники зростали на 5,1 та 4,8 % відповідно, а при суміщенні цих заході було зростання висоти на 10,8–12,2 %. Застосування засобів інтенсифікації в технології вирощування позитивно впливало на кількість бобів і зерен на рослині [9].

В дослідженнях Лавриненка С.О. було встановлено, що найвищий фотосинтетичний потенціал в посівах сочевиці у міжфазні періоди «гілкування–цвітіння» та «цвітіння–дозрівання» відповідно 0,876 і 1,245 млн. м2/га за добу забезпечувало зрошення на фоні зорани на глибину 28–30 см, внесенні мінеральних добрив дозою $N_{90}P_{90}$ та густоти рослин 3,0 млн/га [10].

Також, Гирка А.Д. та інші, встановили, що внесення мінеральних добрив сприяло зростанню кількості бобів на одній рослині сочевиці – від 17,1 до 20,5 %, при цьому кількість зерен в них збільшувалася від 14,5 до 19,2 % залежно від варіанту удобрення (в контролі їх

було відповідно 17,1 та 19,3 шт.). Кращі результати за цими показниками виявилися на фоні, де мінеральні добрива вносили у дозі $N_{10}P_{40}K_{55}$ [11].

В дослідженнях О. М. Данильченко, Г.О. Жатової, що проходили в умовах північно-східного Лісостепу України на базі науково-виробничого центру Сумського національного аграрного університету протягом 2010–2013 рр. показалили, що максимальний рівень врожайності насіння сочевиці було отримано на варіанті з інокуляцією ризогуміном у поєднанні з повним мінеральним добривом в дозі $N_{60}P_{60}K_{60}$, що відповідно забезпечило 1,51 т/га [12].

В польових дослідженнях НУБіП, Каленською С.М. та Шихман Н.В. було встановлено, що найвища урожайність сочевиці різних досліджуваних сортів забезпечили варіанти за внесення мінеральних добрив у дозі $N_{30}P_{60}K_{60}$, що в середньому по досліду склало 1,76-2,01 т/га [13].

В дослідженнях Максимова В.М., було втановлено, що за внесення мінерального добрива у дозі $N_{45}P_{45}$, в умовах Південного Степу України, рівень продуктивності сочевиці склав 1,30 т/га [14].

Отже, для вирощування високих врожаїв сочевиці для задоволення господарських потреб людини, необхідно створити оптимальні умови мінерального живлення, а також застосування мікробіологічних препаратів дозволить економно використовувати природній азот, як для самої сочевиці так і наступних культур в сівозміні.

Список літератури

1. Черенков А.В. Сучасна технологія вирощування сочевиці: [науково-виробниче видання] / А.В.Черенков, А.І. Клиша, А.Д. Гирка, О.О. Кулініч, Ю.Я. Сидоренко, О.В. Бочевар, О.В. Ільєнко, А.О. Кулик. – Дніпропетровськ, 2013. – 48 с.
2. Клыша А.И. Чечевица / А.И. Клыша, Т.В. Невмывако // Информационный листок Министерства Украины по делам науки и технологий. – Харьков: ХАРПНТЭИ, 1997. – № 48. – С. 1–3.
3. https://agrarii-razom.com.ua/culture/sochevicya
4. Кобизєва Л.Н. Генетичні ресурси зернобобових культур в Україні: вивчення, збереження і використання в селекційних програмах / Л.Н. Кобизєва, О.М. Безугла, Л.М. Потьомкіна, Т.О. Дрепіна // Генетичні ресурси рослин. – 2004. – № 1. – С. 88–93.
5. Зерновые и зернобобовые культуры. Под общей редакцией акад. И.В. Якушкина и под редакцией П.Е. Маринича. Государственное издательство сельскохозяйственной литературы, Москва, 1956.
6. Комракова Ю. Чечевица (Lensculinaris) / Ю. Комракова // Зерновые культуры. – 1998. – № 4. – С. 11.
7. Камінський В. Ф. Інтенсифікація виробництва зернобобових культур в умовах північного Лісостепу / В. Ф. Камінський, А. В. Голодна, Д. С. Шляхтуров // Землеробство. – 2008. – Вип. 80. – С. 109–115.
8. Коноплев Ю. И. Влияние биологических и агротехнических факторов на формирование продукционного процесса повышения урожайности семян новых сортов чечевицы / Ю.И. Коноплев // Автореф. дис. канд. с.-х. наук. – Орел. – 2004. – 22 с.
9. http://www.institut-zerna.com/library/pdf6/29.pdf
10. https://journal.udau.edu.ua/assets/files/89/Agro/Ukr/23.pdf
11. Досягнення та перспективи селекції зернобобових культур / [А. М. Шевченко, І. А. Шевченко, В. Ю. Скитський, Т. Є. Степанова] // Вісн. ЦНЗ АПВ Харківської обл. – Х., 2008. – № 1. – С. 145–151
12. Данильченко О.М., Жатова Г.О. Урожайність і якість насіння кормових бобів та сочевиці залжно від інокуляції бактеріальними препаратами і внесення мінеральних добрив/ О. М. Данильченко, Г.О. Жатова// Вісник ЖНАЕУ – 2016 - №1 (53) – С. 94-101
13. Каленська С. М. Продуктивність сочевиці залежно від мінерального живлення та передпосівної обробки насіння в умовах правобережного Лісостепу України / С. М. Каленська, Н. В. Шихман // Наук. доповіді НУБіП – 2011 – 4
14. Максимов В.М. Вплив способу обробітку ґрунту, мінеральних добрив та густоти рослин на урожайність зерна сочевиці за різних умов зволоження в умовах південного степу україни. / В.М. Максимов// Таврійський науковий вісник - 2016 - № 95 – С. 74- 79.

УДК 004

С. Кравченко, магістр гр. КН-18М-1,9
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ ЗБЕРЕЖЕННЯ ІНФОРМАЦІЇ У ВИГЛЯДІ ОБРАЗІВ НА ОСНОВІ ВИКОРИСТАННЯ API-ФУНКЦІЙ

У статті розглянуто програмне забезпечення, яке призначено для системи збереження інформації у вигляді образів на основі використання API-функцій. Метою розробки є дослідження та програмна реалізація системи збереження інформації у вигляді образів на основі використання API-функцій. Об’єктом дослідження є процес збереження інформації у вигляді образів на основі використання API-функцій. Предметом дослідження є методи збереження інформації у вигляді образів на основі використання API-функцій. Методи дослідження базуються на методах теорії зберігання даних, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи збереження інформації у вигляді образів на основі використання API-функцій. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення. Розроблено зручний інтерфейс користувача.
комп’ютерні науки, збереження інформації, API-функції

Постановка проблеми. В наш час інформація перетворюється на найдорожчий ресурс. Її оперативне отримання дає перевагу над конкурентами, які її не мають. Проте конфіденційна інформація про діяльність фізичної чи юридичної особи, що потрапила до рук зловмисників, може серйозно їм нашкодити.

Для кожного користувача, без сумніву, було б неприємним сюрпризом, коли б мишка його комп'ютера перестала реагувати на дотик, раптово з'явилось повідомлення, що Metallica is the best group in the world, раптово пропав фінансовий звіт за минулий рік, або носій інформації перестав відповідати на запити, тощо. До основних факторів, що призводять до втрат інформації відносять: програмні збої; апаратні збої; несанкціонований доступ; помилки користувачів; робота вірусної програми.

Одним з шляхів, що приводить до зменшення втрат інформації є застосування програм, які створюють копію важливої інформації на інший жорсткий диск, флеш пам'ять, або на CD-DVD диски. Ефективність відновлення інформації при резервному копіюванні побудована на ряді припущень, а саме:

– обладнання та носії інформації повинні бути функціональними;

– дані повинні бути неушкодженими;

– резервне копіювання повинне виконуватись періодично.

ОС Windows, фактично монопольна операційна система, має в своєму складі засоби для резервного копіювання. У останніх версіях Windows вбудовані засоби копіювання як файлів, так і самої системи. Причому збереження системи відбувається незалежно від користувача. Ці програми мають як переваги, так і недоліки.

До переваг можна віднести те, що програм архівації досить багато і вони готові до роботи відразу після завантаження системи.

Серед недоліків потрібно виділити наступне: малий набір сервісних функцій, використання власного (а не загальнодоступного) формату архівного файла, копіювання системних файлів до самої операційної системи.

Якщо першими двома недоліками ще можна знехтувати, то копіювання системи "саму в себе" робить всі зусилля, витрачені на резервування даних даремними, якщо дасть збій

MBR (головний завантажувальний запис). Тому слід віддати перевагу більш спеціалізованому програмному забезпеченню.

Програм для створення образу носіїв інформації дуже багато. До недавнього часу на ринку програм створення точного образу панували Norton Ghost і PowerQuest Drive Image. Але вихід на ринок інших компаній змінив ситуацію. Вони стали цілком гідними конкурентами цим світовим брендам. Це програми Paragon Drive Backup від компанії Paragon Software Group і Acronis True Image від компанії Acronis. Проте такі програми коштують недешево і тому в багатьох випадках стають недоступними для багатьох пересічних користувачів.

Саме тому розробка та впровадження автоматизованої системи збереження копій носіїв інформації у вигляді образів, яка забезпечить: простоту інсталяції і використання, можливість гнучкого настроювання конфігурації та швидкого виконання різноманітних операцій, інтегрування з уже наявними в експлуатації автоматизованими системами на даний час є дійсно актуальною задачею для багатьох користувачів нашої країни, які використовують електронний документообіг на основі локальних та глобальних мереж, а також для власних потреб вдома.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини системи збереження інформації у вигляді образів на основі використання API-функцій.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи збереження інформації у вигляді образів на основі використання API-функцій.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем збереження інформації у вигляді образів на основі використання API-функцій.

– Дослідження системи збереження інформації у вигляді образів на основі використання API-функцій.

– Програмна реалізація системи збереження інформації у вигляді образів на основі використання API-функцій.

Об'єктом дослідження є процес збереження інформації у вигляді образів на основі використання API-функцій.

Предметом дослідження є методи збереження інформації у вигляді образів на основі використання API-функцій.

Методи дослідження базуються на методах теорії зберігання даних, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу.

Опис функціонування системи

Згідно ТЗ в процесі виконання МР передбачена розробка ПЗ системи автоматизованої системи збереження інформації у вигляді образів на основі використання API-функцій. Як результат роботи очікується автоматизована система, яка надасть наступні можливості користувачу: створення та запис образів будь-яких типів накопичувачів інформації.

Образ диска – це файл, який містить в собі повну копію даних і структури файлової системи будь-якого ЕНІ. CD/DVD/Blu-Ray, розділ жорсткого диска, тощо. Фактично, цим терміном позначається будь-який файл з інформацією, достатньою для дублювання структури і умісту пристрою зберігання інформації. Причому, неважливо, чи був цей конкретний образ ЕНІ отриманий з реального фізичного носія, або ж був сформований за допомогою спеціального софтвера. Як правило, у файлі образу диска дублюються сектори носія інформації, а файлова система ігнорується.

В першу чергу, образи дисків потрібні для резервного копіювання. Ця технологія дозволяє зробити копію будь-якого носія з можливістю відтворити його в первозданному виді, навіть якщо оригінал загублений. Наприклад, зручно мати образ системного розділу

комп'ютера або ноутбука. Адже якщо станеться крах системи, то досить буде відновити системний розділ з такого образу, збереженого десь у безпечному місці.

Окрім резервного копіювання, образи дисків часто використовуються геймерами для того, щоб прискорити роботу з інформацією на зовнішньому носії. Доступ до образу диска, що лежить на HDD, відбувається на порядок швидше, ніж доступ до CD або DVD в звичайному дисководі. За рахунок цього часто виходить значимий виграш в швидкості завантаження гри і її роботи.

Є ще один аспект резервного копіювання даних – створення резервних копій мобільних носіїв. До них відносяться переносні НЖМД (USB –накопичувачі, тощо) і флеш-носії (так звані «флешки» – флеш-драйви). Особливістю цих пристроїв є можливість її використання в якості сторонніх, повністю функціональних завантажувачів ОС (приміром, на дискету неможливо помістити ОС Windows XP, тоді як на мобільний НЖМД вона встановлюється дуже легко, і легко з нього завантажується), або секретних ключів (певна програма або файл відкриється тільки при вставленому флеш-драйві).

При втраті працездатності такого накопичувача, користувач може виявитися абсолютно безсилий: програма є, файл є, але запустити він нічого не може – відсутній ключ. Тому має сенс дублювати такі ключі на аналогічний носій, тим більше, що вартість флеш-драйвів зараз відносно невелика. Найпростіше створити образ носія і перенести його на інший такий же носій з використанням програмного забезпечення, яке буде розроблене в процесі виконання МР.

Згідно ТЗ розробці підлягає автономна система автоматизованого збереження інформації, але слід передбачити можливість її роботи в складі більш потужної системи аналогічного класу та спрямування. Тобто, до складу ПЗ системи, що підлягає розробці, необхідно ввести функції-заглушки. Це в подальшому забезпечить підключення нових модулів до існуючого ПЗ без будь-суттєвої його доробки.

Відповідно до методики побудови систем аналогічного класу та спрямування (розділ 2 пояснювальної записки), система повинна забезпечити виконання функцій за призначенням у двох режимах:

– автоматичному;

– інтерактивному.

Інтерактивний режим передбачений для роботи користувача з системою.

Отже, основними задачами по розробці ПЗ створення образів, які підлягають програмній реалізації в процесі виконання МР є:

– визначення та розробка програмних інструментів для реалізації операцій читання/запису з цифрових ЕНІ на жорсткий диск і навпаки;

– визначення переліку файлових систем, з якими буде працювати ПЗ, що підлягає розробці, та означення можливості їх розширення в майбутньому;

– розробка механізму створення образу з командного рядка для вирішення задач по автоматизації за допомогою планувальників задач ОС.

Визначимо джерела вхідної інформації. Ними будуть:

– носії інформації, каталоги та файли;

– мережеві ресурси.

Таким чином, враховуючи вищеозначене, формуємо вимоги, які повинна задовольнити організаційна структура системи:

– забезпечення оперативності та надійності керування робочими файлами;

– виключення можливості дублювання і появи некерованих ланок і процесів;

– забезпечення прийняття рішень системою тільки через центральну ланку;

– забезпечення достатньої інформативності користувача та наявності в системі розвиненого режиму HELP і режиму візуалізації.

Для реалізації операцій читання/запису з цифрових ЕНІ на жорсткий диск і навпаки оберемо в якості базової функцію DeviceIoControl. Це дозволить організувати в системі

пряму роботу з драйверами ОС. На нижньому рівні, використавши також функції WinAPI та API, означимо синтаксис DeviceIoControl:

```
BOOL DeviceIoControl(
  HANDLE hDevice,
  DWORD dwIoControlCode,
  LPVOID lpInBuffer,
  DWORD nInBufferSize,
  LPVOID lpOutBuffer,
  DWORD nOutBufferSize,
  LPDWORD lpBytesReturned,
  LPOVERLAPPED lpOverlapped
);
```

Параметри:

– hDevice.

– [in] – дескриптор пристрою, на якому повинна виконатися операція. Цей пристрій – том, каталог, файл або потік. Щоб витягнути дані про дескриптор пристрою, використаємо функцію CreateFile:

dwIoControlCode

[in] – керуючий код для операції.. Це значення ідентифікує конкретну операцію для виконання і тип пристрою, на якому вона повинна здійснитися. Документація для кожного управляючого коду розглядає деталі використання параметрів:

lpInBuffer, nInBufferSize, lpOutBuffer і nOutBufferSize.

lpInBuffer

[in]

[in] – покажчик на буфер введення даних, який містить дані, необхідні, для виконання операції. Формат цих даних залежить від значення параметра dwIoControlCode.

Цей параметр може бути порожнім (NULL), якщо dwIoControlCode визначає операцію, яка не вимагає введення даних.

nInBufferSize

[in] – розмір буфера введення даних, у байтах.

lpOutBuffer

[out] – покажчик на буфер виведення даних, який повинен отримати дані, повернені операцією. Формат цих даних залежить від значення параметра dwIoControlCode.

Цей параметр може бути порожнім (NULL), якщо dwIoControlCode визначає операцію, яка не повертає дані.

nOutBufferSize

[in] – розмір буфера виведення даних, у байтах.

lpBytesReturned

[out] – покажчик на змінну, яка отримує розмір даних, збережених у буфері виведення даних, у байтах.

Якщо буфер виведення даних є занадто маленьким, щоб отримати які-небудь дані, виклик завершується помилкою, GetLastError повертає значення ERROR_INSUFFICIENT_BUFFER, а параметр lpBytesReturned дорівнює нулю.

Якщо буфер виведення даних є занадто маленьким, щоб вмістити усі дані, але може вмістити деякі дані, що вводяться, деякі драйвери повернуть стільки даних, скільки їх вмістилося. У цій ситуації, виклик завершується помилкою, GetLastError повертає значення ERROR_MORE_DATA, а параметр lpBytesReturned вказує обсяг отриманих даних. Програмний додаток буде викликати функцію DeviceIoControl знову з тією ж самою операцією, визначаючи нову точку відліку.

Якщо параметр lpOverlapped – порожній (NULL), lpBytesReturned не може бути порожнім (NULL). Навіть тоді, коли операція не повертає ніякого виведення даних і

lpOutBuffer є порожнім (NULL), DeviceIoControl використовує lpBytesReturned. Після такої операції значення lpBytesReturned немає сенсу.

Якщо параметр lpOverlapped – не порожній (NULL), lpBytesReturned може бути порожнім (NULL). Якщо цей параметр – не порожній (NULL), і операція повертає дані, параметр lpBytesReturned немає сенсу до тих пір, поки асинхронна операція не завершилася.

Щоб витягнути інформацію про число повернених даних, викличемо функцію GetOverlappedResult. Якщо hDevice пов'язаний з портом завершення введення/виведення даних (I/O), можемо витягнути число повернених даних за допомогою виклику функції GetQueuedCompletionStatus.

lpOverlapped

[in] – покажчик на структуру OVERLAPPED.

Якщо параметр hDevice відкриється без визначення FILE_FLAG_OVERLAPPED, то параметр lpOverlapped слід проігнорувати.

Якщо параметр hDevice відкрився з прапорцем FILE_FLAG_OVERLAPPED, операція виконається як асинхронна. У цій ситуації параметр lpOverlapped повинен вказати на допустиму структуру OVERLAPPED, яка містить дескриптор об'єкту події. Інакше функція завершиться помилкою.

Для асинхронних операцій, DeviceIoControl повертає значення негайно, а об'єкт події подає сигнал, коли операція завершується. Інакше, функція не повертає значення до тих пір, поки операція не завершиться або не станеться помилка.

Означимо перелік значень, які повертаються в процесі виконання/завершення операцій:

– Якщо операція завершується успішно, DeviceIoControl повертає ненульове значення.

– Якщо операція завершується помилкою, DeviceIoControl повертає нуль. Щоб отримати додаткову інформацію про помилку, викличемо GetLastError.

Щоб витягнути дані про дескриптор пристрою, необхідно викликати функцію CreateFile або з ім'ям пристрою, або з ім'ям драйвера, пов'язаного з пристроєм. Щоб визначити ім'я пристрою, використаємо нижче перерахований формат:

\\.\DeviceName

Функція DeviceIoControl може прийняти дескриптор конкретного пристрою.

Тепер визначимо прапорці доступу FILE_SHARE_READ і FILE_SHARE_WRITE при виклику CreateFile, щоб відкрити дескриптор драйвера пристрою. Проте, коли будемо відкривати комунікаційний ресурс (ресурс обміну даними), тип послідовного порту, необхідно визначити монопольний доступ до нього. При відкритті дескриптора пристрою, використаємо інші параметри CreateFile, як зазначено нижче:

– параметр fdwCreate треба визначити як OPEN_EXISTING;

– параметр hTemplateFile має бути ПОРОЖНЬО (NULL);

– параметр fdwAttrsAndFlags може бути визначений як FILE_FLAG_OVERLAPPED, щоб вказати, що повернений дескриптор може бути використаний в асинхронних операціях введення-виведення (I/O).

Список управляючих кодів, які будуть підтримуватись системою, що підлягає розробці:

– Коди, які використовуються комунікаційними пристроями.

– Коди, які використовуються в управлінні пристроями.

– Коди, які використовуються в управлінні каталогами.

– Коди, які використовуються в управлінні дисками.

– Коди, які використовуються в управлінні файлами.

– Коди, які використовуються файловими системами.

– Коди, які використовуються в управлінні живленням комп'ютера.

– Коди, які використовуються в управлінні томами.

Файлова система зв'язує носій інформації з одного боку і API для доступу до файлів – з іншою. Коли прикладна програма звертається до файлу, вона не має ніякого уявлення про

те, яким чином розташована інформація в конкретному файлі, так само, як і на якому фізичному типі носія (CD, жорсткому диску, магнітній стрічці, блоці флеш-пам’яті або іншому) він записаний. Все, що знає програма – це ім'я файлу, його розмір і атрибути. Ці дані вона отримує від драйвера файлової системи. Саме файлова система встановлює, де і як буде записаний файл на фізичному носії (наприклад, жорсткому диску).

З погляду операційної системи (ОС), весь диск це набір кластерів (як правило, розміром 512 байт і більше). Драйвери файлової системи організовують кластери у файли і каталоги, які реально є файлами, що містять список файлів в цьому каталозі. Ці ж драйвери відстежують, які з кластерів в даний час використовуються, які вільні, які помічені, як несправні.

Проте файлова система не обов'язково має бути безпосередньо пов'язаною з фізичним носієм інформації. Існують віртуальні файлові системи, а також мережеві файлові системи, які є лише способом доступу до файлів, що знаходяться на віддаленому комп'ютері.

Програмою, що підлягає розробці, будуть підтримуватись наступні файлові системи: FAT, FAT12/16, FAT32, NTFS, ISO 9660, Ext2/3/4. Це майже всі самі розповсюджені ОС для носіїв інформації на даний час.

Файлові системи FAT і FAT32 (від File Allocation Table – таблиця розміщення файлів) походять від 16-розрядної файлової системи (FAT16), що спочатку використалася в MS-DOS і Windows 3.1. FAT32 вперше була введена в Windows 98 для підтримки жорстких дисків великого об'єму і інших вдосконалених можливостей; далі під терміном FAT матимемо на увазі будь-яку з вищезгаданих версій. FAT є єдино доступною файловою системою для дисків (але не CDів), що працюють під управлінням Windows 9x, а також гнучких дисків. Різновидом FAT є TFAT, яка орієнтована на підтримку механізму транзакцій. Поступово FAT виходить з вживання і в більшості випадків її можна зустріти лише на застарілих системах, особливо тих, оновлення яких після первинної установки на них Windows 9x виконувалося без перетворення типу існуючої файлової системи.

Файлова система NT (NTFS) – сучасна файлова система, яка підтримує довгі імена файлів, а також безпеку, стійкість до збоїв, шифрування, стиснення, розширені атрибути, і дозволяє працювати з дуже великими файлами і об'ємами даних.

Файлова система CDів (CDFS) призначена для доступу до інформації, записаної на CDax. CDFS задовольняє вимогам стандарту ISO 9660.

Файлові системи Ext2/3/4 використовуються в ОС Linux. Операційні системи на базі Linux є лідерами на ринках суперкомп'ютерів, мікрокомп'ютерів, серверів і смартфонів, Означимо шляхи реалізації функції визначення типу файлової системи.

Ця функція буде складатися з набору умовних операторів if, які вкладені один в одного. В кожному тілі оператора послідовно буде викликатися функція перевірки на конкретну файлову систему і при її визначенні функція дасть результат або повідомлення про наявність невизначеної файлової системи:

```
function TSystemFile.GetFSType() : string ;
begin
   Result := '' ;
   if isISO9660()
   then
      Result := 'ISO 9660'
   else if isFAT()
   then
      Result := 'FAT'
   else if isFAT12()
   then
      Result := 'FAT12'
   else if isFAT16()
   then
```

```
            Result := 'FAT16'
          else if isFAT32()
          then
            Result := 'FAT32'
          else if isNTFS()
          then
            Result := 'NTFS'
          else if isExt2_3_4()
          then
            Result := 'Ext2/3/4'
          else if isReiserFS()
          then
            Result := 'ReiserFS'
          else if isHFS()
          then
            Result := 'HFS'
          else if isMFS()
          then
            Result := 'MFS'
          else
            Result := '???' ;
        end ;
```

До складу ПЗ, яке підлягає розробці необхідно ввести:

– Функцію перевірки на відповідну файлову систему ISO 9660. При відповідності – функція поверне значення True, якщо не відповідає, то False:

```
        function TSystemFile.isISO9660() : boolean ;
        Var ReadStart  : _Large_Integer;
          ActualLengthRead : DWORD;
          Seek : DWORD;
        begin
          ReadStart.QuadPart := $8000 ;
          Result := False ;
          Seek := SetFilePointer(FileHandle, ReadStart.LowPart, @ReadStart.HighPart,
FILE_BEGIN);
          if Seek <> $FFFFFFFF
          then begin
            if ReadFile(FileHandle, Buffer, 8, ActualLengthRead, nil)
            then begin
              if (Buffer[0] = Char(01)) and (Buffer[1] = 'C') and (Buffer[2] = 'D') and (Buffer[3] =
'0')
                and (Buffer[4] = '0') and (Buffer[5] = '1') and (Buffer[6] = Char(01)) and
(Buffer[7] = Char(0))
              then begin
                Result := True ;
                SizeOfLabel := 31 ;
                PositionOfLabel.QuadPart := $8028 ;
              end ;
            end ;
          end
        end ;
```

– Функцію перевірки на відповідну файлову систему FAT. При відповідності – функція поверне значення True, якщо не відповідає, то False.

```
function TSystemFile.isFAT() : boolean ;
Var ReadStart  : _Large_Integer;
   ActualLengthRead : DWORD;
   Seek : DWORD;
   i : integer ;
   tmp : string ;
begin
   ReadStart.QuadPart := 54 ;
   Result := False ;
   Seek := SetFilePointer(FileHandle, ReadStart.LowPart, @ReadStart.HighPart,
FILE_BEGIN);
   if Seek <> $FFFFFFFF
   then begin
      if ReadFile(FileHandle, Buffer, 8, ActualLengthRead, nil)
      then begin
         for i := 0 to 7 do
            tmp := tmp + Buffer[i] ;
         if tmp = 'FAT     '
         then begin
            Result := True ;
            SizeOfLabel := 11 ;
            PositionOfLabel.QuadPart := 43 ;
         end ;
      end ;
   end
end ;
```

Означимо синтаксис команди по розбору командного рядка (команди для запису файла):

rawwritewin [--password] [--write] [--copies n] [--drive driveno] [--yes] file.img

--password: пароль;

--write: команда ЗАПИСАТИ;

--copies n: кількість копій для запису n – копії;

--drive driveno – це фізичний номер пристрою або літера логічного пристрою;

--yes : автоматична відповідь "так" на всі запитання.

Синтаксис команди для читання файла:

rawwritewin --read [--drive driveno] file.img.

Якщо file.img вже існує – він буде перезаписаний.

Зберігання інформації окремо від системних файлів вже довгі роки є неписаним правилом для багатьох користувачів та системних адміністраторів. Для персонального користувача це означає, як мінімум, поділ жорсткого диска на три логічні диски: для системи, для додатків, для даних. Для корпоративного користувача з великим обсягом інформації – розміщення інформації на інших – не системних – фізичних дисках. Цей захід полегшить і саму операцію копіювання даних.

Принцип роздільного зберігання інформації стосується файлових архівів та образів дисків. Їх необхідно також зберігати, як мінімум, на несистемних розділах одного жорсткого диска. Для корпоративного користувача принцип роздільного зберігання інформації повинен реалізовуватися ще жорсткіше: як мінімум, одна з копій повинна зберігатися в іншому офісі, філії, відділенні – щоб не втратити корпоративну інформацію у разі повені, землетрусу або, скажімо, пожежі, крадіжки.

Розробка структурної схеми

ПЗ, що підлягає розробці, повинно бути компактним та оглядовим, легким для сприйняття, надавати користувачу в процесі роботи з системою необхідну теоретичну

допомогу. Тому до її складу необхідно ввести зручний, україномовний графічний інтерфейс та забезпечити легкі для розуміння формати виведення результатів на екран монітора.

Мінімальна конфігурація апаратних засобів, що забезпечать в повному обсязі функціонування програмного забезпечення, має наступний вигляд:

– персональний комп'ютер, сумісний з IBM PC;

– мінімальний обсяг оперативної пам'яті – 64 МБ;

– операційна система WINDOWS.

Образ будь-якого електронного накопичувача інформації (ЕНІ) – це файл, який утримує повну копію умісту і структури файлової системи і даних, що знаходяться на ЕНІ. Тобто, образ ЕНІ утримує всю інформацію, необхідну для дублювання структури, розташування і отримання даних будь-якого пристрою збереження інформації. Зазвичай образ ЕНІ іншого типу просто повторює набір секторів носія, ігноруючи файлову систему, побудовану на ньому.

При розробці ПЗ МР використаємо не звичний підхід до створення образу ЕНІ (без файлової системи, побудованої на ЕНІ-джерелі вхідної інформації), а будемо вирішувати більш складну задачу – створення образу ЕНІ з урахуванням його файлової системи.

Спочатку образи дисків використовуватись для резервного копіювання дисків, при якому точне збереження вихідної структури було необхідним і/чи доцільним. З появою оптичних носіїв (CD-DVD) більш часто стали використовуватись саме їх образи, найчастіше в формі *.ISO-файлу, який утримував файлову систему ISO 9660, яку зазвичай використовують CD-DVD. Але цей формат не підтримує багатосесійні дані та аудіо-CD.

Окрім формата ISO, на сьогодення існує ряд інших форматів образу дисків, таких, як *.IMG і *.DMG, а також проприєтарних: *.NRG (Nero Burninq ROV), *.MDS/.MDF (ДАЕМОN Tools.Alcohol 120 %), *.DAA (Power ISO), *.PQI (Drivelmaqe) та *.CCD/*.IMG/*.SUB (ClonCD). Проте найбільш універсальним для ЕНІ є формат *.imq, тому свою розробку будемо орієнтувати на створення образів ЕНІ саме в цьому форматі.

В основу розробки ПЗ майбутньої системи планується покласти модульний принцип, тобто є головний, керуючий модуль та підлеглі модулі, кожен з яких виконує якусь одну функцію.

Це дозволить розробнику без особливих труднощів допрацювати модуль, виправити можливі помилки, додати нові функціональні можливості до даного модуля (наприклад, нові операції) та без особливих зусиль передати модуль користувачу на ЕНІ або використовуючи Internet. Користувач просто скопіює новий модуль до директорії, в якій знаходиться програма – і все, пакет оновлено. Навіть не треба перезавантажувати систему. Можна одразу запускати систему на виконання та виконувати необхідні операції.

При розробці концепції побудови майбутньої системи та шляхів її реалізації основний наголос робився на швидкості, зрозумілості, легкості використання в роботі з електронними носіями інформації.

Отже, розробці в процесі виконання МР підлягає складна (в сенсі реалізації) багатофункціональна система, тому доцільно використати функції WindowSAPI-Win32. Win32 – це набір функцій, які є частиною ОС і реалізовані у вигляді DDL-бібліотек. Вони забезпечують пряме звертання програм до необхідних процедур: підпрограм чи функцій. При роботі над розробкою ПЗ системи використаємо наступні бібліотеки Win32 API ядра ОС Windows.

– Kernel32: низькорівневі функції керування пам'яттю, задачами та іншими ресурсами системи;

– User32: функції керування інтерфейсом користувача;

– Advapi32: функції доступу до системного реєстра.

Окрім вищеозначених бібліотек, які будуть одними з основних елементів системи, при розробці ПЗ необхідно використати наступні компоненти і інтерфейси системних викликів ядра ОС Windows: бібліотеку драйверів пристроїв (на які нам необхідно створити образи) та

рівні: NativeAPI (NTdll.dll), NativeAPI Ядра (ntoskrul.exe), рівень абстракції від обладнання (hal.dll).

Використання цих компонентів дозволить організувати взаємодію пристроїв з ПЗ системи для реалізації основної задачі – створення електронних образів цих пристроїв. Наводимо на рисунку 1 схему взаємодії ПЗ на основі використання функцій API ОС Wndows з ЕНІ при створенні їх образів.

Розроблену структурну схему будемо розглядати в якості базової для побудови структури майбутньої системи, тому визначимо більш детально компоненти структурної схеми та означимо функції, які вони будуть виконувати в системі:

– HAL.dll – рівень абстракцій від обладнання. Використання цієї бібліотеки дозволить забезпечити незалежність розробленої системи від апаратної платформи.

– NTdll.dll – ця бібліотека – своєрідний «місток» між тими бібліотеками, які працюють в ядрі ОС, і бібліотеками, що будуть працювати в системі.

– Графічна підсистема (Win32.sys) та бібліотека Gdi32.dll забезпечать організацію та чітку роботу графічного інтерфейса користувача. Вони надають додаткам та іншим бібліотекам графічні примітиви для малювання вікон та різноманітних віконних елементів керування.

– Функція DeviceloControl, яка забезпечить керування драйверами пристроїв, змушуючи обраний пристрій виконати відповідну операцію. Для визначення типу пристрою використаємо функцію GetDriveType.

При створенні образу диску необхідно наперед знати (тобто, визначати) його параметри: вільне місце в байтах; ємність диска в байтах; інформацію про файлову систему, розташовану на обраному накопичувачі (в разі необхідності); ім’я диска; кореневий каталог диска; серійний номер диска (службовий).

Для цього в процесі виконання МР будуть розроблені відповідні алгоритми двох процедур та виконана їх програмна реалізація:

– визначення місткості дискового простору;

– визначення одиниці виміру дискового простору.

Для забезпечення виконання основної задачі необхідно ввести до складу ПЗ системи наступні режими, які також підлягають програмній реалізації в процесі розробки МР:

– читання накопичувача електронної інформації;

– запис прочитаної інформації на жорсткий диск;

– копіювання з жорсткого диску на будь-якій інший носій інформації;

– визначення надходження невідомої/незрозумілої команди (лексичний розбір);

– визначення помилок, їх типу та візуалізація (для забезпечення інформативності користувача);

– ведення протоколу процесу зчитування/запису пошарово;

– індикація стану читання/запису;

– планування створення образів певних носіїв інформації по розкладу (через певні проміжки часу) в автоматичному режимі.

Таким чином, ми розглянули механізм створення образів електронних носіїв інформації та визначили шляхи реалізації цього механізму, тобто – фактично провели теоретичну побудову системи. Визначено і обґрунтовано:

– базову структурну схему взаємодії системи, ядра ОС Windows та ЕНІ, які підлягають обробці;

– структуру основних складових механізму створення образів електронних накопичувачів інформації;

– основні режими роботи майбутньої системи, які забезпечать виконання нею запланованих функцій.

Система, що підлягає розробці, буде мати ієрархічну структуру побудови. До її складу необхідно ввести наступні компоненти:

– головна програма: графічний інтерфейс користувача, який забезпечить реалізацію в системі інтерактивного режиму; обробку помилок та їх візуалізацію; організацію і роботу інтерактивної довідки, індикацію стану створення образів;

– жорсткий диск: накопичувач образів електронних носіїв інформації;

– носії інформації CD, DVD-диски, USB Flash; оптичні диски; жорсткий диск, які підлягають обробці в процесі функціонування системи.

Графічний інтерфейс забезпечить візуалізацію для користувача:

– службових повідомлень про успішне/неуспішне виконання операцій;

– службових повідомлень про успішне/неуспішне проведення перевірок;

– протоколу реєстрації нестандартних ситуацій, які можуть виникнути в процесі роботи системи/обладнання;

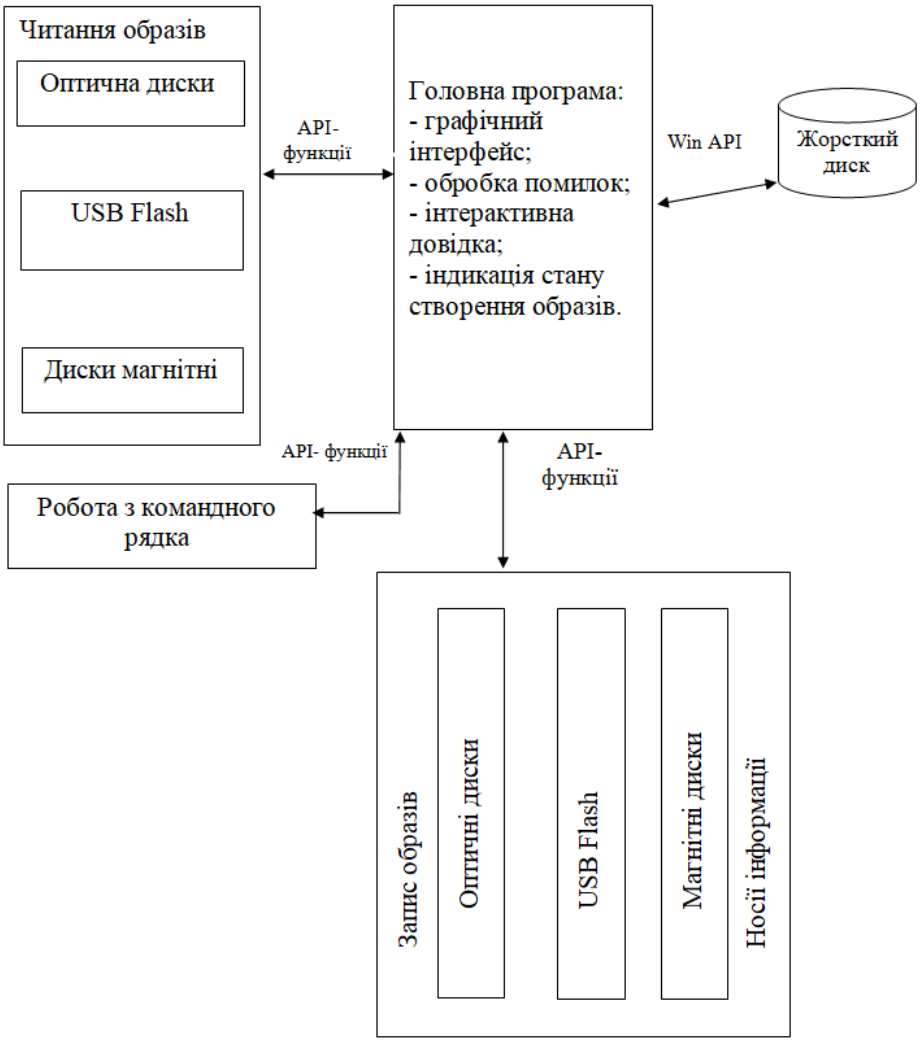


Рисунок 1 – Структурна схема системи

– звітної інформації в будь-який відлік часу за будь-який термін роботи системи по безпосередньому призначенню.

Функції контролю/спостереження не будуть безпосередньо впливати на роботу системи в цілому, а виконувати означені для них задачі в фоновому режимі, без безпосередньої участі користувача. Розподілимо операції, які будуть виконуватись, на 2 типи:

– операції високого рівня: інтерфейс користувача, передача/приймання даних по мережі, обробка даних, збереження образів на жорсткий диск, формування звітів, друк звітів;

– операції низького рівня: робота з API-функціями Win API.

Таким чином, нами визначені складові майбутньої системи, їх функції в системі та взаємозв'язок. Тому будуємо структурну схему системи, яка надається на рисунку 1.

Висновок. У статті розглянуто та проаналізовано програмне забезпечення, створене в результаті виконання роботи, призначено для системи збереження інформації у вигляді образів на основі використання API-функцій. В межах України в недостатній мірі представлені вітчизняні розробки в цій області. У роботі наведені теоретичне узагальнення й рішення наукового завдання дослідження методів збереження інформації у вигляді образів на основі використання API-функцій. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем збереження інформації у вигляді образів на основі використання API-функцій; Досліджена система збереження інформації у вигляді образів на основі використання API-функцій; На основі отриманих результатів досліджень створена програмна реалізація системи збереження інформації у вигляді образів на основі використання API-функцій. Розроблені під час виконання роботи алгоритми дозволяють успішно вирішувати завдання збереження інформації у вигляді образів на основі використання API-функцій. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки. Розроблене програмне забезпечення має простий, дружній та зручний інтерфейс користувача, що забезпечує легкість у освоєнні роботи програмного продукту, зручність у використанні, і не потребує особливих спеціальних знань. При створені програмного забезпечення було використано об'єктно-орієнтований підхід, що відповідає сучасним тенденціям у галузі розробки комерційних програмних систем. Програма реалізована на мові високого рівня Delphi 10.3.2. Дана мова програмування дозволяє найбільш ефективно обробляти дані. Це дозволило мінімізувати строк розробки програмного забезпечення, і, як слід, зменшити витрати на його розробку. Запропоноване програмне забезпечення ділиться на загальне програмне забезпечення, що поставляється із засобами обчислювальної техніки й спеціальне програмне забезпечення, що спеціально розроблене для даної конкретної системи й включає програми, що реалізують її функції. Даються необхідні рекомендації з установки розробленого програмного забезпечення. Для підвищення рівня безпеки запропоновано застосовувати алгоритм MMB.

Список літератури

1. Коваленко А.С. Разработка структуры базы данных интегрированной информационной системы / А.С. Коваленко, А.В. Коваленко // Информационные технологии и защита информации в информационно-коммуникационных системах: монографія / Под редакцией профессора В.С. Пономаренко. – Х.: Вид-во ТОВ «Щедра садиба плюс», 2015. – С. 54-64.
2. Кожанова А.С. Обґрунтування необхідності створення систем технічної діагностики інтегрованих інформаційних систем / О.А. Смірнов, А.С. Кожанова, О.В. Коваленко // Системи обробки інформації. – Х.: ХУПС, 2013. – Вип. 6(113). – С. 255-257.
3. Коваленко А.С. Задачи распознавания ситуаций в ERP системах / А.В. Коваленко ., А.А. Смірнов, А.С. Коваленко // Системи обробки інформації. – Х.: ХУПС, 2014. – Вип. 4(120). – С. 161-164.
4. Коваленко А.С. Підсистема технічної діагностики для автоматизації процесів керування в інтегрованих інформаційних системах / А.С. Коваленко , О.А.Смірнов, О.В. Коваленко // Системи озброєння і військова техніка.– Х.: ХУПС, 2014. – № 1(37). – С. 126-129.
5. Коваленко А.С. Анализ эффективности использования экспертной системы технической диагностики с традиционной структурой / А.С. Коваленко, А.А. Смирнов, А.В. Коваленко // Системи озброєння і військова техніка. – Х.: ХУПС, 2014. – № 2(38). – С. 106-108.
6. Коваленко А.С. Разработка структуры экспертной системы технической диагностики интегрированной информационной системы / А.С. Коваленко, А.А. Смирнов, А.В. Коваленко // Наука і техніка Повітряних Сил Збройних Сил України. – Харків: ХУПС, 2014. – № 2(15). – С.154-157.
7. Коваленко А.С. Разработка структуры экспертной системы технической диагностики интегрированной информационной системы / А.С. Коваленко, А.А. Смирнов, А.В. Коваленко // Наука і техніка Повітряних Сил Збройних Сил України. – Харків: ХУПС, 2014. – № 2(15). – С.154-157.
8. Коваленко А.С. Структура системи технічної діагностики інтегрованих інформаційних систем / А.С. Коваленко, О.А. Смірнов, О.В. Коваленко // Збірник наукових праць Кіровоградського

національного технічного університету / техніка в сільськогосподарському виробництві, галузеве машинобудування, автоматизація. – Кіровоград: Вид-во КНТУ, 2014. – Вип. 27. – С. 245-251.
9. Коваленко А.С. Дослідження будови інтегрованої інформаційної системи та її елементів / А.С. Коваленко, О.А. Смірнов, О.В. Коваленко // Системи озброєння і військова техніка. – Х.: ХУПС, 2014. – № 4(40). – С. 85-88.
10. Коваленко А.С. Розробка структури бази даних для обліку технічного стану елементів інтегрованої інформаційної системи з урахуванням вимог споживачів інформації / А.С. Коваленко, О.А. Смірнов, О.В. Коваленко // Системи обробки інформації. – Х.: ХУПС, 2015. – Вип. 1(126). – С. 75-79.

УДК 004

С. Кублій, магістр гр. КН-18МЗ-1,4
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ ЗАХИСТУ КОРПОРАТИВНОЇ МЕРЕЖІ ВІД КІБЕРЗАГРОЗ

У статті розроблено програмне забезпечення, яке призначено для системи захисту корпоративної мережі від кіберзагроз. Метою розробки є дослідження та програмна реалізація системи захисту корпоративної мережі від кіберзагроз. Об’єктом дослідження є процес захисту корпоративної мережі від кіберзагроз. Предметом дослідження є методи захисту корпоративної мережі від кіберзагроз. Методи дослідження базуються на методах захисту інформації, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи захисту корпоративної мережі від кіберзагроз. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення. Розроблено зручний інтерфейс користувача. Наведені інструкції по роботі з програмними засобами.
комп’ютерні науки, захист інформації, корпоративна мережа, кіберзагрози

Постановка проблеми. На сьогоднішній день, часом, як у розроблювачів, так і в споживачів системних засобів, відсутнє розуміння того, що завдання, розв'язувані будь-яким системним засобом, у тому числі, і засобом захисту інформації, повністю визначаються областю його практичного використання. Вимоги й підходи до побудови системного засобу для альтернативних областей його застосування, як правило, не те, щоб були різні, вони повністю суперечливі. Застосування ж засобу, створеного для одних застосунків, в інших застосунках, може привести до сумного наслідкам, особливого це критично, коли мова заходить про IT-безпеку. Розглянемо всі ці питання на прикладі побудови корпоративної (відразу ж позначили область практичного використання) VPN.

Починаючи розмову про побудову або про використання системного засобу, насамперед необхідно визначитися з областю його практичного застосування (для чого воно створено, як наслідок, чим визначається його споживча вартість). Все це відноситься й до засобів захисту інформації. Саме область практичного використання диктує ті вимоги до системного засобу, які, у першу чергу, будуть реалізовані розроблювачем, щоб підвищити споживчу вартість даного засобу. Не складно показати, що подібні вимоги для різних областей практичного використання можуть дуже сильно розрізнятися, а часом, і суперечити один одному, що не дозволяє створити єдиного засобу "на всі випадки життя".

Коли мова заходить про інформаційні технології, можна виділити два їхній основних додатки – це особисте використання в домашніх умовах і корпоративне використання – на підприємстві. Якщо задуматися, то різниця вимог, у тому числі й до засобів захисту, у даних застосунках величезна. У чому ж вона складається.

Наприклад, коли мова йде про особисте використання комп'ютера в домашніх умовах, ми відразу ж починаємо замислюватися про надаваний системним засобом сервіси – це максимально можливе використання пристроїв, універсальність застосунків, мріємо про всілякі ігри, програвачі, графіку й т.д. і т.п.

Найважливішими ж відмінностями використання системного засобу в даних застосунках є наступне:

– По великому рахунку, відсутність якої-небудь конфіденційності (принаймні, формалізуємої) інформації, що вимагає захисту.

– Відсутність критичності не тільки в частині розкрадання оброблюваної інформації, але й у частині її несанкціонованої модифікації, або знищення. Не так критичні в цих застосунках і атаки на системні ресурси, у великій мері, вони зв'язані лише з незручністю для користувача.

– Відсутність кваліфікації користувача в питаннях забезпечення інформаційної безпеки, та й природне небажання займатися цими питаннями (захищати нема чого).

– Відсутність якого-небудь зовнішнього адміністрування системного засобу, у тому числі, у частині налаштування механізмів захисту – всі завдання адміністрування вирішуються безпосередньо користувачем – властиво користувач повинен самостійно вирішувати всі питання, пов'язані з безпекою. Інакше кажучи, користувач і є адміністратор – сам собі й захисник, і безпечник (якщо хоче, то саме він і захищає свою власну інформацію).

– Відсутність якої-небудь недовіри до користувача – користувач обробляє власну інформацію (він же власник комп'ютера, він же власник інформації).

– Здебільшого, обробка інформації користувачем здійснюється на одному комп'ютері, локально.

Тепер подивимося, які ж підходи до побудови засобів захисту виявилися на практиці найбільш затребуваними в даних застосунках. Природно, що подібними рішеннями стали не засоби захисту, а засоби контролю, у першу чергу – це всілякі антивірусні засоби, засновані на сигнатурному аналізі. Очевидно, що засоби захисту, що вимагають певної кваліфікації для налаштування (а просто ефективний захист не забезпечити), у даних застосунках малозастосовні. Контроль же вимагає найпростіших дій від користувача – "нажав кнопку, і готово". Всі питання, що вимагають кваліфікованого рішення, тут "перекладаються на плечі" розроблювачів антивірусних засобів, зокрема, підтримку бази вірусів у максимально актуальному стані. Помітимо, що, тому що ніякого адміністрування не передбачається, весь діалог здійснюється з кінцевим користувачем, а не з адміністратором, що, до речі кажучи, навіть при використанні засобів контролю, часом, відносить користувача "у тупик", тому що вимагає підвищення кваліфікації користувача, а йому цього об'єктивно не потрібно.

Наскільки ефективні такі засоби? Природно, що з погляду забезпечення якого-небудь прийнятного рівня захисту інформації, подібні засоби неефективні. Це твердження очевидно – у будь-який момент часу база виявлених сигнатур не повна (повної вона не може бути навіть теоретично). Але інші засоби в даних застосунках взагалі незастосовні.

Якщо ж ми починаємо говорити про корпоративні додатки, то тут, як умови використання системні засобів, так і вимоги до засобу захисту не те, щоб були кардинально інші, вони прямо протилежні. Зокрема, тут уже немає необхідності у великій номенклатурі пристроїв, застосунків, іграшок та інше є відволікаючим від службової діяльності фактором, можливість їхнього запуску в принципі бажано запобігти, і т.д. і т.п.

Найважливішими умовами використання засобів захисту в даних застосунках є наступне:

– У даних застосунках апріорі присутнє конфіденційна інформація, що вимагає кваліфікованого захисту.

– Критичним є не тільки факт розкрадання оброблюваної інформації, але й можливість її несанкціонованої модифікації, або знищення. Критичним у цих застосунках

також стає вивід з ладу системних засобів на тривалий час, тобто найважливішими об'єктами захисту стають системні ресурси.

– Відсутність кваліфікації користувача в питаннях забезпечення інформаційної безпеки, та й небажання займатися цими питаннями (захищати потрібно не його особисту інформацію), і разом з тим, наявність адміністратора безпеки, основним службовим обов'язком якого є захист інформації), тобто саме для рішення цього завдання він і прийнятий на роботу), що апріорі повинен мати високу кваліфікацію, тому що, у противному випадку, про який-небудь ефективний захист у сучасних умовах говорити не доводиться.

– Всі завдання адміністрування засобів захисту повинні вирішуватися безпосередньо адміністратором (до речі кажучи, це одне з вимог нормативних документів).

– Апріорна недовіра до користувача – користувач обробляє не власну, а корпоративну, або іншу конфіденційну інформацію, що потенційно є "товаром", як наслідок, користувач повинен розглядатися як потенційного зловмисника (останнім часом, навіть з'явилося таке поняття, як інсайдер, а внутрішня IT-погроза – погроза розкрадання інформації санкціонованим користувачем, деякими споживачами й виробниками засобів захисту позиціонується, як одна з домінуючих погроз, що не позбавлено підстав).

– Здебільшого, обробка конфіденційної інформації здійснюється в корпоративній мережі, причому, не завжди в локальної – це обумовлює неможливість ефективного рішення завдання адміністрування безпеки локально на кожному комп'ютері – без відповідного інструментарію (АРМа адміністратора в мережі).

Бачимо, що в цих застосунках уже "у главу кута" відноситься завдання ефективного захисту інформації, що повинна вирішуватися професійно. Не випадково, що захист інформації в даних застосунках регламентується відповідними нормативними документами, засобу захисту припускають їхню сертифікацію, а автоматизована система (АС) обробки інформації – атестацію, а все в сукупності – кваліфікований аналіз достатності й коректності реалізації механізмів захисту.

Основу забезпечення інформаційної безпеки в даних застосунках уже становлять саме механізми захисту, що реалізують розмежувальну політику доступу до ресурсів, а не найпростіші механізми контролю!

Найважливішою умовою побудови захисту в корпоративних застосунках є те, що властиво користувач повинен розглядатися в якості основного потенційного зловмисника (інсайдера). Це обумовлюється тим, що користувач тут обробляє не власну інформацію, а корпоративну, отже, може бути зацікавлений у її розкраданні. Це обумовлює необхідність виключення користувача зі схеми адміністрування засобу захисту. Коли мова заходить про криптографічний захист даних у корпоративних застосунках, необхідне виконання певних вимог до реалізації ключової політики – ключ шифрування повинен генеруватися адміністратором (бажано взагалі автоматично, тоді й адміністратор не зможе порушити конфіденційність даних), ключ же, надаваний користувачеві (якщо він взагалі надається користувачеві) не повинен дозволяти порушити конфіденційність даних, при їхньому розкраданні користувачем.

Все це істотно ускладнює завдання адміністрування, як наслідок, у корпоративних застосунках досить актуальним стає спрощення завдання адміністрування, відразу обмовимося, що не за рахунок спрощення механізмів захисту – основним параметром подібних систем, поза залежністю ні від чого, є ефективність захисту (все інше вдруге, інакше, цей не засіб захисту для корпоративних застосунків).

Все сказане відноситься до будь-якого засобу захисту, у тому числі, і до VPN.

Корпоративна VPN – це "накладена" (віртуальна) на мережу загального користування мережна інфраструктура, обмежена рамками корпорації. Подібну інфраструктуру в загальному випадку становлять локальні обчислювальні засоби, поєднувані в корпоративну локальну мережу, корпоративні локальні мережі, поєднувані в єдиний комунікаційний простір, до якого, крім того, підключаються віддалені й мобільні користувачі. Зберігання й обробка в рамках віртуальної (заснованої на використанні каналів зв'язку загального

користування) мережі корпоративної інформації вимагає її захисту, що складає в реалізації розмежувальної політики доступу до корпоративних ресурсів і в криптографічному захисті віртуальних ("накладених" на існуюче телекомунікаційне встаткування) каналів зв'язку.

З обліком усього сказаного раніше, спробуємо сформулювати загальні вимоги до корпоративного VPN:

– Всі завдання адміністрування, як у частині завдання розмежувальної політики доступу до корпоративних ресурсів, так і в частині реалізації ключової політики (створення й поширення ключів шифрування віртуальних каналів), повинні вирішуватися безпосередньо адміністратором безпеки централізовано (до складу VPN повинен входити АРМ адміністратора безпеки).

– Користувач повинен бути виключений зі схеми адміністрування – повинен працювати в корпоративній мережі "під примусом" адміністратора – повинен спілкуватися тільки з тими користувачами (або комп'ютерами), з якими йому дозволене адміністратором, при цьому повинен обмінюватися з ними даними тільки в тім виді (відкритими, або зашифрованими), у якому йому дозволено адміністратором. Як наслідок, шифрування віртуальних каналів повинне здійснюватися автоматично ("під примусом") "прозоро" для користувача, ключ шифрування користувача (надаваний йому адміністратором) не повинен дозволяти порушити користувачеві конфіденційність даних при їхньому розкраданні.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи захисту корпоративної мережі від кіберзагроз.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи захисту корпоративної мережі від кіберзагроз.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем захисту корпоративної мережі від кіберзагроз.
– Дослідження системи захисту корпоративної мережі від кіберзагроз.
– Програмна реалізація системи захисту корпоративної мережі від кіберзагроз.

Об'єктом дослідження є процес захисту корпоративної мережі від кіберзагроз.

Предметом дослідження є методи захисту корпоративної мережі від кіберзагроз.

Методи дослідження базуються на методах захисту інформації, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Постачальники VPN-послуг, як правило, надають своїм користувачам наступні протоколи:

– PPTP.
– L2TP/IPSec.
– OpenVPN.
– IKEv2.
– SSTP.
– SoftEther.

Архітектура кожного VPN-протоколу значно відрізняється від інших, і тому в кожного з них є свої переваги й недоліки. Тобто, попереднє знайомство може пізніше зіграти вам на руку.

Порівняння VPN-протоколів

У нижчеподаній таблиці ми підбили основні характеристики кожного протоколу, і, таким чином, буде легше підібрати протокол, що підходить вам найбільше.

На жаль, не існує універсального стандарту для всіх, тому що потреби відрізняються від людини до людини. Але безумовно можна знайти найбільш підходящий вам протокол, що буде відповідати практично всім вашим вимогам. Існує кілька характеристик VPN-протоколів: продуктивність, рівень шифрування, безпека, сумісність, стабільність і налаштовуємість.

Давайте розглянемо кожний VPN-протокол у контексті згаданих вище характеристик.

Таблиця 1 – Таблиця порівняння VPN-протоколів

Протокол	Швидкість	Шифрування й безпечний серфінг	Стабільність	Стримінг медиаресурсов	Скачивание торрентов	Доступність у застосунках CactusVPN	Сумісність
PPTP	Швидко	Погано	Середньо	Добре	Добре	Windows	Більшість ОС і пристроїв
L2TP/IPSec	Швидко	Середньо	Добре	Добре	Добре	Windows	Більшість ОС і пристроїв
IKEv2/IPSec	Швидко	Добре	Добре	Добре	Добре	Windows, macOS і iOS	Більшість ОС і пристроїв
OpenVPN TCP	Середньо	Добре	Добре	Середньо	Добре	Windows і Android	Більшість ОС і пристроїв
OpenVPN UDP	Швидко	Добре	Середньо	Добре	Добре	Windows і Android	Більшість ОС і пристроїв
SSTP	Середньо	Добре	Середньо	Середньо	Добре	Windows	Windows
SoftEther	Швидко	Добре	Добре	Добре	Добре	Немає	Windows

Який VPN-протокол самий безпечний?

Якщо мова заходить про безпеку, то отут PPTP відразу відпадає, тому що в нього найнижчий рівень захисту.

L2TP/IPSec і IKEv2 уважаються безпечними, тому що шифрують дані двічі.

OpenVPN надає високий рівень безпеки й дозволяє перевіряти дійсність цифрових сертифікатів.

SoftEther підтримує OpenVPN, EtherIP, L2TP/IPSec і SSTP, а це значить, що він використовує переваги всіх протоколів одночасно.

SSTP уважається дуже безпечним, тому що пропонує високий рівень шифрування й уміє підключатися до HTTPS-сайтів через 443 порт, що використовується TLS.

Переможець: OpenVPN.

Який VPN-протокол найшвидший?

Швидкість і шифрування корелюють по очевидних причинах: шифрування гарного рівня вимагає не тільки більше обчислювальної потужності, але й більше часу, що й сповільнює загальну швидкість роботи мережі.

Протокол PPTP є одним з найшвидших VPN-протоколів тунелювання саме через низький рівень шифрування.

IKEv2, SoftEther і L2TP/IPSec теж швидше, а от OpenVPN уважається самим повільним.

SSTP не так вражає своєю продуктивністю, як PPTP, але по швидкості обходить OpenVPN.

Переможець: PPTP.

Який протокол пропонує краще шифрування?

Говорячи максимально просто, шифрування – це перетворення даних у нерозбірливу форму при передачі на інший пристрій або для тривалого зберігання. Цілком очевидно, що VPN-шифрування використовується, щоб виключити несанкціонований доступ до даних. Всі види конфіденційної інформації й даних зберігаються в зашифрованому виді; Це захищає організації, підприємства й звичайних людей від шахрайства й інших безладь.

PPTP використовує 128-бітне шифрування на базі протоколу MPPE, що належить компанії Microsoft. Протокол MPPE використовує шифрування RC4 від RSA, що підтримує шифрування до 128 біт.

L2TP/IPSec і IKEv2/IPSec використовують 256-бітне шифрування на базі стандартизованого протоколу IPSec. У ньому для шифрування застосовуються 3DES і AES, використовувані АНБ для роботи із секретною інформацією.

OpenVPN використовує бібліотеку OpenSSL, що підтримує 3DES, а також інші бібліотеки, які підтримують 160-бітне й 256-бітне шифрування.

SoftEther також використовує 256-бітне шифрування, у той час як SSTP використовує TLS-підключення з 2048-бітним шифруванням.

Переможець: OpenVPN і SoftEther.

Який VPN-протокол самий стабільний?

PPTP використовується в більшості Wi-Fi маршрутизаторів і вважається стабільним.

L2TP/IPSec сполучимо із пристроями, у яких передбачена підтримка NAT.

OpenVPN відмінно працює навіть у ненадійних мережах.

SoftEther, завдяки своєму постійному підключенню, що самопідтримується, уміє обходити більшість фаєрволов.

SSTP також уважається стабільним, і вміє обходити фаєрволи NAT.

Протокол IKEv2 дійсно дуже стабільний при перемиканні між мережами, як наприклад при переході від стільникової мережі до Wi-Fi з'єднання.

Переможець: L2TP/IPSec, SoftEther і IKEv2

Який VPN-протокол підтримує більшість платформ?

Протокол PPTP підтримує найбільше число ОС.

Протокол L2TP/IPsec також підтримує досить багато ОС.

OpenVPN не має нативної підтримки основних ОС, і тому прийде використовувати стороннє програмне забезпечення.

IKEv2 підтримується на різних платформах, але що саме головне – на пристроях BlackBerry, тоді як більшість VPN-протоколів не працюють на BlackBerry.

SSTP обмежується лише ОС Windows, але при цьому підтримує всі версії цієї платформи.

SoftEther не має нативної підтримки основних ОС, і тому прийде використовувати стороннє програмне забезпечення.

Переможець: PPTP і L2TP/IPSec.

Який VPN-протокол легше всього настроїти?

PPTP-протокол найпростіший у налаштуванні.

L2TP/IPSec і IKEv2 також легко налаштовуються.

OpenVPN добре піддається налаштуванню, але для роботи зі стороннім ПЗ буде потрібно деякий досвід.

SSTP теж добре налаштовується й при цьому можна розраховувати на підтримку від Microsoft.

SoftEther – це новий протокол, тому буде не так просто знайти яку-небудь інформацію про нього в інтернеті. Отже, процес налаштування трохи складніше.

Переможець: PPTP

Який VPN-протокол споживає найменше ресурсів?

Протокол PPTP вимагає дуже мало обчислювальної потужності через низький рівень шифрування.

L2TP/IPSec і IKEv2 використовують більше потужностей, тому що двічі інкапсулюють дані.

Продуктивність OpenVPN не так висока, однак при цьому протокол оптимізує споживання обчислювальної потужності й відмінно працює в нешвидких мережах.

SoftEther використовує більше обчислювальної потужності, тому що опирається на програмне рішення.

SSTP використовує мінімальні ресурси завдяки значній інтеграції в саму платформу.

Переможець: SSTP.

Хочете захистити свої особисті дані в мережі?

Використовуйте VPN для підвищення конфіденційності в інтернеті, захисту з'єднання й доступу до заблокованих веб-сайтам.

Опис кожного VPN-протоколу

Щоб правильно вибрати VPN-протокол, спочатку потрібно довідатися, що пропонує кожний з них.

PPTP

PPTP (Point-to-Point Tunnelling Protocol) був розроблений і створений компанією Microsoft ще в 1990-х роках. Завдяки доступності на всіх платформах, він дуже розповсюджений серед постачальників VPN-послуг. Найважливіша характеристика PPTP – його швидкість у порівнянні з іншими протоколами шифрування. Його легко настроїти, і при цьому в більшості платформ він іде як убудована функція.

Однак деякі експерти вважають, що даний протокол може бути менш безпечним, ніж інші, навіть незважаючи на те, що всі минулі проблеми безпеки були виправлені. Тому, якщо вас турбує ваша безпека, то для підключення варто вибрати інший VPN-протокол. Найчастіше його використовують ті, кому потрібно тільки одержати контент, обмежений для конкретного регіону тому що працює він дуже швидко. Якщо ваші основні потреби – швидкість і доступність, то PPTP буде відмінним вибором.

L2TP/IPSec

Протокол L2TP (Layer 2 Tunneling Protocol) – через свою високу продуктивність і набагато більше високого рівня безпеки – передбачалася як заміна протоколу PPTP. Цікаво те, що протокол L2TP сам по собі не підтримує яке-небудь шифрування, і для цих цілей використовує IPSec. Він також є убудованим протоколом у більшості сучасних ОС, що робить його налаштування такої ж простій, як і у випадку з PPTP.

Крім того, в L2TP/IPSec немає ніяких уразливостей, так що він являє більшу цінність із погляду безпеки й продуктивності. Однак його недолік у тім, що працює він трохи повільніше, ніж інші VPN-протоколи. Іноді він здатний упоратися з потужними фаєрволами.

OpenVPN

OpenVPN – один із самих популярних протоколів, які використовують практично всі VPN-сервіси у світі. Це відносно нова VPN технологія, у якій використовується комбінація інших технологій, таких як протоколи SSLv3 і OpenSSL. Це дозволило створити краще можливе VPN-рішення. Та сама бібліотека OpenSSL забезпечує шифрування багатьома іншим алгоритмам, включаючи AES, Camellia і Blowfish.

Серед переваг OpenVPN можна відзначити легкий процес налаштування, високий рівень безпеки, підтримку безлічі алгоритмів шифрування, а також гарну продуктивність проти фаєрволів і доступність за принципом open source. Але для роботи OpenVPN буде потрібно стороннє ПЗ, що може виявитися складним у налаштуванні. Хоча підтримка мобільних пристроїв тут і передбачена, вона поки що не настільки гарно, як підтримка настільних ПК. Що стосується швидкості в стандартному UDP-режимі, цей алгоритм повинен працювати швидше L2TP, але навряд чи буде швидше PPTP.

IKEv2

IKEv2 (Internet key exchange version 2) – це протокол VPN, що був розроблений компанією Microsoft у співробітництві з Cisco. Це протокол тунелювання на основі IPsec із широким спектром переваг. З погляду безпеки він прирівнюється або навіть перевершує протокол L2TP/IPsec, і при цьому в нього досить висока продуктивність.

Одне з основних переваг IKEv2 – підтримка протоколу MOBIKE, що робить його неймовірно надійним при мережах, що переміняються. Це, у свою чергу, робить протокол IKEv2 одним із кращих для мобільних користувачів, які перемикаються між Wi-Fi і стільниковою мережею або просто переміщаються від однієї точки доступу в інтернет до іншої. Ще однією особливістю є те, що при використанні з VPN Connect від Microsoft, протокол IKEv2 може автоматично відновлювати VPN-підключення після тимчасової втрати з'єднання.

Він сумісний з Windows і BlackBerry, а також може бути використаний з Linux і іншими платформами з відкритим вихідним кодом. І хоча він доступний на меншій кількості платформ у порівнянні з іншими VPN-протоколами, експерти вважають його досить гарним з погляду стабільності, безпеки й продуктивності.

SSTP

SSTP (Secure Socket Tunneling Protocol) теж розроблений Microsoft і тому заточено винятково під ПК із ОС Windows. Відповідно, його не можна перевірити на наявність бекдорів, і він навряд чи коли-небудь буде підтримувати пристрою Apple. SSTP дуже схожий на OpenVPN, тому як використовує той же протокол SSLv3.

Основні переваги SSTP – його високий рівень безпеки й здатність обходити навіть потужні фаєрволи. Якщо ви крутитесь у середовищі Windows, і вас не турбує ймовірність того, що Microsoft зберегла для себе секретні шляхи до ваших персональних даних, то SSTP, можна сказати, являє собою добре інтегроване VPN-рішення з гарним рівнем безпеки й простій налаштуванням.

SoftEther

SoftEther – відносно новий VPN-протокол, розроблений в 2013 році в якості open source заміни для VPN. Він може похвастатися гарною швидкістю й надійними мірами безпеки, хоча в силу новизни по ньому до цих складно шукати документацію. Він підтримує протоколи SSL-VPN і IPSec, EtherIP, OpenVPN і L2TP, і працює набагато швидше OpenVPN.

Крім значно кращої продуктивності в порівнянні з OpenVPN, SoftEther також пропонує безліч функцій, недоступних в OpenVPN. Наприклад, функцію динамічного DNS, фільтрацію пакетів, графічний інтерфейс керування, керування RPC по HTTPS, функції віртуального DHCP і NAT, а також генератор затримки, погрішності й втрати пакетів. Однак SoftEther розповсюджений не так, як і інші протоколи, використовувані для VPN-підключень.

Як видно, протоколи й стандарти мають різні характеристики; деякі пропонують високий рівень захисту, у той час як інші демонструють більшу продуктивність. Тут все залежить винятково від ваших потреб і завдань, тому що ви можете жертвувати продуктивністю заради одержання більшого рівня захисту й навпаки.

Розробка структурної схеми

Побудова єдиної захищеної корпоративної мережі для територіально розподілених об'єктів – складне комплексне завдання. При її рішенні доводиться враховувати безліч факторів і ризиків.

Більшість сучасних інформаційних систем носять розподілений характер і можуть функціонувати тільки при наявності високопродуктивної корпоративної мережі передачі даних, без якого сьогодні важко представити роботу комерційних компаній і державних організацій.

За даними дослідження ZK Research, більше 75% співробітників підприємств працюють поза головним офісом – на території філій, у відрядженнях або в домашніх умовах. Усім їм необхідний доступ до корпоративних застосунків і даних, у тому числі до таким критично важливим системам, як Oracle E-Business Suite, NetSuite, Sage ERP або

Microsoft Dynamics. Нерідко вони працюють і із хмарними застосунками – наприклад, з Salesforce.com, Google Apps і Microsoft Office 365.

Поєднуючи в єдину систему всі офіси й підрозділи підприємства, що часом перебувають на значній відстані від штаб-квартири, корпоративна мережа дозволяє надати персоналу можливість одночасної роботи з розподіленими або централізованими застосунками, базами даних і інших сервісів.

При цьому територіально розподілені мережі повинні забезпечувати безпека переданої інформації, мати необхідну продуктивність, бути зручними в адмініструванні й «прозорими» для користувачів і застосунків. Це припускає об'єднання віддалених офісів і філій у єдину інфокомунікаційну структуру й формування на її базі захищеного корпоративного робітничого середовища. Нерідко інфраструктурний рівень включає ще й бездротові сегменти мережі Wi-Fi, що забезпечують мобільність співробітників в офісі компанії

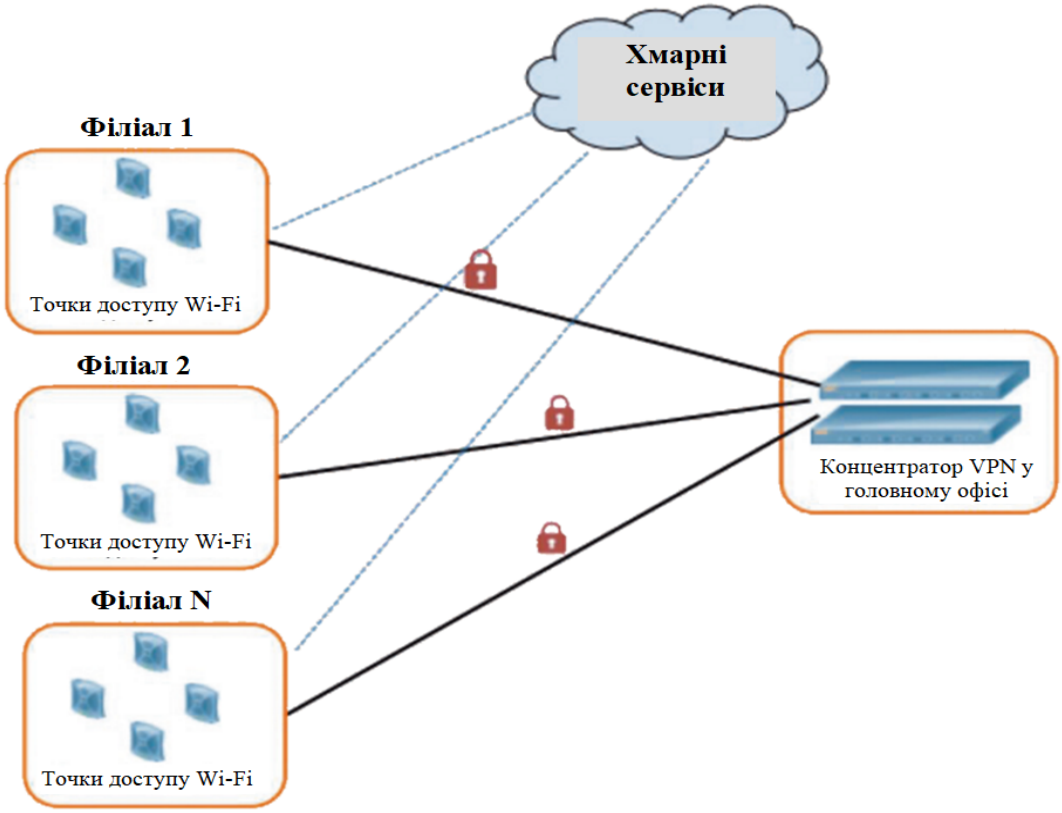


Рисунок 1 – Структурна схема системи

Розподілена корпоративна мережа з бездротовими сегментами у філіях. Централізоване керування дає адміністраторові мережі можливість управляти мережами філій і діагностувати несправності із центрального офісу. Більше дорога архітектура з контролерами WLAN у філіях дозволить ще й уніфікувати політикові безпеки в провідній і бездротовій мережах, спростити діагностику й усунення несправностей.

Для забезпечення захищеного віддаленого доступу до корпоративної мережі необхідно, щоб підключення здійснювалося тільки з використанням протоколів SSL VPN/IPSec при обов'язкової двофакторної автентифікації. Бажано також автоматично забезпечувати віддаленим користувачам захищений робочий простір, щоб при завершенні сеансу підключення на робочому місці не залишалося ніяких його слідів (тимчасові або скачанні файли, історія відвідування сторінок і ін. повинні бути віддалені).

IP VPN

У територіально розподіленій компанії для об'єднання розрізнених підрозділів у єдину корпоративну мережу можуть задіятися виділені канали зв'язку або загальнодоступні мережі передачі даних. Якщо для передачі даних, голосового трафіку й відео використовуються

виділені канали, передана по них інформація захищена від зовнішніх впливів, але таке рішення, по-перше, досить дорого, а по-друге, не завжди й не скрізь у підприємства є технічна можливість одержати у своє розпорядження виділений канал.

У таких організаціях для створення єдиної корпоративної мережі часто використовуються з'єднання VPN через Інтернет по IPSec, іноді – через операторські мережі MPLS. Подібна мережна інфраструктура захищається за допомогою автентифікації й керування доступом, тунелювання між площадками й шифрування. Територіально розподілена компанія може використовувати загальні мережі передачі даних.

Технологія віртуальних приватних мереж (Virtual Private Network, VPN) забезпечує безліч переваг при відносно невисокій вартості. VPN – логічна приватна мережа, організуєма поверх публічної. Подібно виділеним каналам, вона дозволяє створити захищене з'єднання між віддаленими площадками або локальними мережами.

Шлюзи безпеки здатні забезпечити захищений доступ з віддалених площадок через Інтернет до корпоративних ресурсів організації. IPSec VPN захищає з'єднання головного офісу з віддаленими філіями й партнерами компанії. Мобільні співробітники можуть використовувати для безпечної роботи з корпоративними ресурсами SSL або L2TP VPN, не застосовуючи програмних клієнтів VPN

L2 VPN реалізується із залученням сервісів Ethernet або на основі MPLS. У цьому випадку комутатори «упаковують» отримані від устаткування клієнта кадри Ethernet або IP MPLS і передають їх до місця призначення по «віртуальному каналі». За такою технологією будуються міські мережі Metro Ethernet або відповідно обласні мережі IP MPLS.

У випадку L3 VPN (IP VPN) віртуальну приватну мережу організує провайдер (MPLS VPN) або користувач (IPSec VPN). Якщо в підприємства безліч філій, то за допомогою технології Dynamic Multipoint VPN (DMVPN) можна обійтися всього двома концентраторами VPN.

Інтеграція сервісів

При організації VPN корпоративна мережа логічно відділена від публічних мереж, тобто трафік захищений від несанкціонованого доступу. При цьому компанія одержує повний контроль над її функціонуванням. По такій мережі можна передавати різні види трафіку з поділом по класах обслуговування.

Поряд з передачею даних віртуальні частки мережі можна використовувати для сервісів IP-телефонії й відео-конференц-зв'язку, гнучко змінювати пропускну здатність каналів залежно від потреб бізнесу, масштабувати мережну інфраструктуру, включаючи в єдину захищену приватну мережу нові об'єкти. Тому територіально розподілені мережі на основі VPN є основою для впровадження різних сервісів, таких як VoIP, ВКЗ, бізнес-застосунка.

За допомогою віртуальних приватних мереж можна об'єднати розподілені офіси в загальну мережу, створивши єдиний адресний простір локальної мережі і єдину нумерацію в системі корпоративної телефонії, тобто сформувати загальний інформаційний простір, доступне з будь-якої точки корпоративної мережі.

IPSec VPN – досить простий і розповсюджений спосіб створення захищеної мережної інфраструктури територіально розподілених компаній. Між пристроями створюються віртуальні тунелі, і весь трафік шифрується на встаткуванні замовника. У такий спосіб забезпечується незалежність від оператора зв'язку. Хоча рішення й відрізняється більше низькою вартістю в порівнянні з орендою каналів, у нього є свої недоліки: часто потрібне додаткове встаткування (або ПЗ), не завжди можна гарантувати якість сервісу.

Стратегії захисту

Вибір технології й варіанта підключення залежить від:

- виду переданого трафіку;
- структури організації і її бізнес-процесів;
- вимог до ІБ;
- тарифів оператора, послугами якого компанія збирається скористатися;

– і інших факторів.

Потрібно оцінити необхідну пропускну здатність і обсяг трафіку, вимоги до параметрів каналу зв'язку (включаючи надійність і ступінь захисту) для трафіку різного типу. Аналіз бізнес-процесів допомагає виявити, наскільки критичні для діяльності підприємства використовувані сервіси. Однак інформаційну безпеку варто проробляти не тільки для каналів зв'язку, але й для компанії в цілому.

Система безпеки опирається на безліч технологій, серед яких – шифрування трафіку, єдина система керування ІБ, засобу захисту бездротової частини мережі. Вибір технологічних, програмних і організаційних рішень для захисту комунікацій у територіально розподілених системах визначається архітектурою мережі, її масштабом, характером оброблюваної інформації, балансом технічних і фінансових можливостей. Конкретна реалізація захищених з'єднань між площадками вибирається на основі категоризації переданих даних з урахуванням їх критичності для бізнес-процесів компанії й технологічних особливостей, наприклад необхідності підтримки QoS.

До основних напрямків мережної безпеки ставляться керування доступом до ресурсів корпоративної інформаційної системи, захист її периметра, автентифікація транзакцій, моніторинг подій безпеки й ін. Раціональний захист повинна містити в собі шифрування даних, переданих при підключенні територіально рознесених підрозділів через зовнішні мережі, застосування засобів міжмережевого екранування й виявлення вторгнень для захисту периметра мережі, оперативний контроль за подіями ІБ. Вона будується з урахуванням характеристик інформації, параметрів інформаційної системи, оцінки ризиків і рівня різних погроз.

Спектр доступних сьогодні рішень для міжмережевого екранування й VPN – закордонних і вітчизняних – досить широкий і здатний задовольнити різноманітні вимоги до функціональності, продуктивності й ціні. Нерідко вендори пропонують інтегровані системи, що поєднують кілька функцій безпеки, наприклад функції міжмережевого екрана з VPN і IPS.

Реалізація конкретної стратегії захисту залежить від рівня зрілості процесів безпеки в організації. Залежно від критичності сервісу засобу безпеки можуть передбачати контроль доступу, захист даних, каналу й пристроїв, а також верифікацію останніх. Звичайно (по зростаючі) застосовуються наступні технології: багатофакторна автентифікація при організації доступу (не обов'язково забезпечується захист каналу), шифрування каналу (VPN), профілювання пристроїв, аналіз ризику кожного з'єднання, створення/контроль довіреного середовища на кінцевому пристрої.

Коли метою кіберзлочинців є велика організація з більшими інвестиціями в інформаційну безпеку, злом віддаленого (і найчастіше менш захищеного) сегмента мережі стає найбільш простим способом проникнення. Превентивні технології захисту на стороні віддалених сегментів – цілком переборний для них бар'єр. Вони можуть повторювати спроби атаки знову й знову, поки не досягнуть успіху, а одержавши доступ до віддаленого сегмента, будуть атакувати вже головний офіс / основні процеси з використанням отриманих легітимних прав. Тому компаніям, що володіють розвитий мережею філій, потрібно бути готовими не тільки протидіяти погрозам у віддаленому сегменті, але й мати засобу їхнього виявлення на ранніх етапах реалізації атак як реактивного (наприклад, пасток класу honeypot), так і проактивного характеру (системи виявлення вторгнень, системи захисту від таргетованих атак).

Поряд із захищеним віддаленим доступом до корпоративної мережі всі частіше потрібно забезпечувати безпека при роботі із хмарними сервісами. Коли компанія вирішує використовувати такі сервіси, вона покладається на компетенцію провайдеру. Однак передбачені технології захисту не вирішують проблем, зв'язаних зі своєчасним припиненням або правильним обігом із правами доступу до ресурсів. Якщо говорити про базові елементи захисту при використанні хмарних сервісів, то IT-адміністраторові необхідно вибудувати процес керування доступом (Identity Management), що дозволить вчасно блокувати обіг

співробітника до зовнішніх сервісів при зміні його статусу (перехід в інший відділ, що стоїть звільнення). Крім цього, такі процеси повинні враховувати й зміну IT-адміністратора.

Для ефективної протидії сучасним погрозам в умовах територіально розподіленої корпоративної мережі повинні бути дотримані наступні вимоги:

– централізоване керування політикою безпеки всіх елементів системи захисту.

– кореляція даних на основі вступників подій і гнучка зміна правил на пристроях відповідно до тих, що змінюються, погроз.

– безперервне відновлення стану сервісних модулів на пристроях безпеки, таких як Web-фільтрація, системи виявлення вторгнень, контроль трафіку застосунків, антиспам, бази IP-репутації й інших;

– забезпечення відказостійкості ключових елементів забезпечення безпеки.

– реалізація політик (Single Sign On і Identity Based Policy) для контролю дій всіх користувачів мережі.

Безсумнівно, для організації безпечної роботи в корпоративній мережі потрібний комплексний підхід. Різні технічні рішення – міжмережеві екрани, антивірусні й антиспам-системи, VPN і інші – необхідно доповнювати організаційними мірами. Це особливо актуально, коли підприємство має територіально віддалені філії або потрібно створити умови для безпечної роботи мобільних співробітників, що наприклад перебувають у відрядженнях. У цьому випадку дуже важливо не тільки наявність надійного й захищеного каналу зв'язку між співробітником і корпоративною мережею, але й можливість однозначно ідентифікувати користувача, щоб надати йому належні права доступу до інформації. Необхідно відзначити важливість автентифікації саме користувачів, а не пристроїв (ноутбуків, смартфонів), що підключаються до корпоративної мережі, тому що у випадку втрати або крадіжки встаткування зловмисник може одержати доступ у мережу підприємства.

Аналогічні завдання виникають і при забезпеченні взаємодії між територіально розподіленими філіями. Дуже важливе використання надійних механізмів автентифікації як при підключенні до корпоративної мережі, так і при доступі до різних інформаційних систем, порталам і сервісам, що працюють у ній. Одним з таких механізмів є використання сертифікатів відкритого ключа, випущених корпоративним центром, що засвідчує. Централізована система керування засобами автентифікації й самим доступом до корпоративних ресурсів і систем дозволяє оперативно реагувати на випадки виявлення погроз або виникнення інцидентів.

Віддалена підтримка й адміністрування

У рамках виконання своїх обов'язків системним адміністраторам часто потрібно підключатися до віддалених комп'ютерів для усунення виниклих неполадок або установки нового ПЗ. Компанії, що має кілька філій, співробітники яких не завжди мають потрібну кваліфікацію, подібна можливість украй необхідна. Її надають спеціальні утиліти, наприклад програма Radmin. Вона використовується в розподілених корпоративних мережах для підтримки користувачів, дозволяючи вирішувати технічні проблеми співробітників, що навіть перебувають в інших містах.

Для авторизації користувачів у програмі може бути обрана або система безпеки Windows з підтримкою Active Directory і протоколу Kerberos, або власна система с індивідуальними правами доступу для кожного користувача й захищеної автентифікацією за іменем й паролем. У першому випадку в адміністраторів домена є можливість застосовувати звичні засоби призначення прав. Системний адміністратор може дати дозвіл на підключення в кожному з режимів – «Повний контроль», «Перегляд», Telnet, «Обмін файлами» або «Переадресація» – будь-якому користувачеві або групі користувачів. ПЗ Radmin сумісно з іншими системами мережної безпеки. Для роботи програми досить підключення до одного порту TCP, номер якого можна задати в налаштуваннях.

Щоб ніхто не міг одержати несанкціонованого доступу до віддаленого комп'ютера, в Radmin можна настроїти IP-фільтрацію, а також заборонити підключення до екрана без явного схвалення його користувача. Крім того, в Radmin ведеться протокол з'єднань, всі дії

записуються в журнал. Ця інформація може придатися для аудита підключень до віддаленого комп'ютера й для виявлення потенційно небезпечного поводження, наприклад спроб підібрати пароль або з'єднань у неробочий час.

Radmin надійно захищає всі передані дані. За 16-літню історію існування продукту в ньому не було знайдено ні однієї уразливості, у той час як в інших подібних рішеннях число уразливостей виміряється десятками. Radmin активно використовується для роботи не тільки в захищених корпоративних системах, але й у такій потенційно ненадійній мережі, як Інтернет. І ніяких проблем з безпекою не виявлено.

Централізований моніторинг і керування

Наскільки важливі в цьому контексті функції централізованого керування в режимі реального часу? Моніторинг і виявлення погроз IT-безпеки в реальному часі вимагають постійного збору інформації про події, що відбуваються в розподілених сегментах мережі. Однак у віддалених підрозділах не завжди є фахівці служби підтримки, а тим більше співробітники, що відповідають винятково за адміністрування засобів захисту. У такому випадку потрібно не тільки централізація, але й можливість ієрархічного керування. Наприклад, поширення глобальних критичних політик, сформованих у головному офісі, при одночасному локальному адмініструванні унікальних правил для розподілених сегментів.

Створення єдиних центрів керування, безумовно, необхідно, тому що допомагає виявляти ризики й, відповідно, мінімізувати наслідку. Однак адміністрування таких центрів у режимі реального часу вимагає виділення додаткового фінансування. Все повинне бути відповідно до, і якщо при оцінці ризиків установлюється висока ймовірність того, що передбачувана атака на підприємство може привести до масштабного збитку, то системи централізованого керування повинні обов'язково функціонувати в режимі реального часу.

У групі засобів моніторингу можна виділити рішення для керування подіями й даними безпеки (Security Information & Event Management, SEIM) з кореляцією подій, що дозволяють контролювати як самі події безпеки, так і їхній взаємозв'язок. Журнали подій аналізуються із застосуванням методів, аналогічних аналізу Вольших Даних. Швидко розвиваються й засобу відстеження внутрішніх погроз і захисту від витоків інформації (DLP). Еволюціонують методи автентифікації й рішення PKI. В імпортні продукти вбудовуються вітчизняні криптоалгоритми й движки.

Без централізованого керування неможливо побудувати ефективну систему захисту в умовах розподіленої мережі. Сучасні засоби керування дозволяють координувати рішення від різних виробників, дотримуючи принципів відповідності загальної корпоративної політики безпеки. Прикладом є технологія SDN. Вендори активно працюють у даному напрямку: наприклад, компанія Fortinet представила нову систему безпеки програмно обумовлених мереж (Software-Defined Network Security, SDNS).

Ефективні інвестиції в ІБ вимагають комплексної оцінки ризиків і погроз. Потрібно брати до уваги майбутній розвиток захищеної телекомунікаційної інфраструктури, інакше неминучі додаткові витрати на модернізацію системи.

Висновок. У статті розглянуто та проаналізовано програмне забезпечення, яке призначено для системи захисту корпоративної мережі від кіберзагроз. В межах України в недостатній мірі представлені вітчизняні розробки в цій області. У роботі наведені теоретичне узагальнення й рішення наукового завдання дослідження методів захисту корпоративної мережі від кіберзагроз. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем захисту корпоративної мережі від кіберзагроз; Досліджена система захисту корпоративної мережі від кіберзагроз; На основі отриманих результатів досліджень створена програмна реалізація системи захисту корпоративної мережі від кіберзагроз. Розроблені під час виконання роботи алгоритми дозволяють успішно вирішувати завдання захисту корпоративної мережі від кіберзагроз. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки. Розроблене

програмне забезпечення має простий, дружній та зручний інтерфейс користувача, що забезпечує легкість у освоєнні роботи програмного продукту, зручність у використанні, і не потребує особливих спеціальних знань. При створені програмного забезпечення було використано об'єктно-орієнтований підхід, що відповідає сучасним тенденціям у галузі розробки комерційних програмних систем. Програма реалізована на мові високого рівня Embarcadero Delphi 10.2 Tokyo. Дана мова програмування дозволяє найбільш ефективно обробляти дані. Це дозволило мінімізувати строк розробки програмного забезпечення, і, як слід, зменшити витрати на його розробку. Запропоноване програмне забезпечення ділиться на загальне програмне забезпечення, що поставляється із засобами обчислювальної техніки й спеціальне програмне забезпечення, що спеціально розроблене для даної конкретної системи й включає програми, що реалізують її функції. Для підвищення рівня безпеки запропоновано застосовувати алгоритм Madryga. В цілому створене програмне забезпечення підтверджує правильність використаних проектних рішень та повністю відповідає вимогам технічного завдання. Створене програмне забезпечення має потенційну можливість для подальшого вдосконалення і застосування у різних галузях.

Список літератури

1. Смирнов С. А. Алгоритмы формирования множества маршрутов передачи метаданных в облачные антивирусные системы / А. А. Смирнов, С. А. Смирнов, А. К. Дидык // Актуальні питання забезпечення кібернетичної безпеки та захисту інформації: зб. наук. праць II Міжнар. наук.-практ. конф., м. Київ, 24-27 лютого 2016 р. – К.: Європейський університет, 2016. – С. 140-142.
2. Смирнов С. А. Разработка и реализация метода безопасной маршрутизации метаданных в облачные антивирусные системы / А. А. Смирнов, С. А. Смирнов, А. К. Дидык // Securitea informationala 2015-2016: Conferenta internationala (editia a XII-a), Chisinau, Moldova, 3 martie 2016. – Chisinau: ADSEM, 2016. – С. 90-96.
3. Смирнов С. А. Алгоритм формирования базового множества маршрутов передачи метаданных в облачные антивирусные системы / А. А. Смирнов, С. А. Смирнов, А. К. Дидык // Інформатика та системні науки (ІСН-2016): зб. тез VII всеукр. наук.-практ. конф., м. Полтава, 10-12 березня 2016 р. – Полтава: ПУЕТ, 2016. – С. 261-263.
4. Смирнов С. А. Система обработки и формирования начального состояния маршрутизации метаданных в облачные антивирусные системы / А. А. Смирнов, С. А. Смирнов, А. К. Дидык // Проблеми кібербезпеки інформаційно-телекомунікаційних систем: зб. тез наук.-практ. конф., м. Київ, 10-11 березня 2016 р. – К.: КНУ ім. Тараса Шевченка, 2016. – С. 81-82.
5. Смирнов С. А. Алгоритм безопасной маршрутизации на базовом множестве путей передачи метаданных в программный сервер облачной антивирусной системы / А. А. Смирнов, С. А. Смирнов, А. К. Дидык // Інформаційна безпека та комп'ютерні технології (IS&CT): зб. тез міжнар. наук.-практ. конф., м. Кіровоград, 24-25 березня 2016 р. – Кіровоград: КНТУ, 2016. – С. 73.
6. Смирнов С. А. Исследование способа контроля линий связи телекоммуникационной системы для облачных антивирусов / А. А. Смирнов, С. А. Смирнов, А. К. Дидык // Збірник тез першої міжнародної науково-практичної конференції «Проблеми науково-технічного та правового забезпечення кібербезпеки у сучасному світі» (ПНПЗК-2016), м. Харків, 30 березня – 1 квітня 2016 р. – Х.: НТУ «ХПІ», 2016. – С. 14.
7. Смирнов С. А. Разработка способа контроля линий связи телекоммуникационной системы для облачных антивирусов / А. А. Смирнов, С. А. Смирнов, А. К. Дидык // Матеріали XVIII міжнародного науково-практичного семінару «Комбінаторні конфігурації та їх застосування» (м. Кіровоград, 15-16 квітня 2016 р.). – Кіровоград: КНТУ, 2016. – С. 182-186.
8. Смирнов С. А. Разработка и исследование способа контроля линий связи телекоммуникационных сетей для облачных антивирусных систем / А. А. Смирнов, С. А. Смирнов, А. К. Дидык // Проблеми і перспективи розвитку ІТ-індустрії: VIII міжнар. наук.-практ. конф., м. Харків, 28-29 квітня 2016 р.: зб. тез. – Х.: ХНЕУ, 2016. – С. 48.
9. Смирнов С. А. Модель системы нейросетевых экспертов безопасной маршрутизации для облачных антивирусных систем / А. А. Смирнов, С. А. Смирнов, А. К. Дидык // Інформаційна та економічна безпека (INFECO-2016): зб. тез III міжнар. наук.-практ. конф., м. Харків, 28-30 кві. 2016 р. – Х.: ХНМІ ДВНЗ «УБС», 2016. – С. 178-182.
10. Смирнов С. А. Метод безопасной маршрутизации метаданных в облачные антивирусные системы / А. А. Смирнов, С. А. Смирнов, А. К. Дидык // Сборник тезисов XII международной конференции «Стратегия качества в промышленности и образовании» (г. Варна, Болгария, 30 мая – 02 июня 2016 г.). – Варна: ТУВ, 2016. – С. 581-585.

УДК 004

В. Маслєнко, магістр гр. КІ-18МЗ-1,4
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ ЗАХИСТУ КОРПОРАТИВНИХ ДОДАТКІВ, ЯКІ РОЗРОБЛЯЮТЬСЯ ЗА ДОПОМОГОЮ МЕТОДОЛОГІЇ AGILE

У статті розроблено програмне забезпечення, яке призначено для системи захисту корпоративних додатків, які розробляються за допомогою методології Agile. Метою розробки є дослідження та програмна реалізація системи захисту корпоративних додатків, які розробляються за допомогою методології Agile. Об'єктом дослідження є процес захисту корпоративних додатків, які розробляються за допомогою методології Agile. Предметом дослідження є методи захисту корпоративних додатків, які розробляються за допомогою методології Agile. Методи дослідження базуються на методах захисту інформації, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи захисту корпоративних додатків, які розробляються за допомогою методології Agile.
комп'ютерна інженерія, захист інформації, Agile

Постановка проблеми. З появою в бізнес-лексиконі модного слова «эджайл» у захисників додатків додалося головного болю. Мало того, що й раніше об'єкти захисту – корпоративні додатки – несли в собі рукотворні уразливості, так тепер вони ще й створюються швидко, і живуть недовго.

При класичному підході кожна зміна вимагає перевірки на відсутність нових уразливостей, а інфраструктуру й засоби захисту необхідно адаптувати до нових вимог відносно функціональності й безпеки.

Зміни – це не тільки нові функції з іншим програмним кодом. Це й додавання товару на вітрину електронного магазина, і перероблена форма анкети-заяви, яку треба завантажувати, і зміна форми уведення й т.п.

За правилами, при будь-якій зміні системи треба запускати режим сканування об'єкта й, залежно від виявлених вад, або повертати його на доробку й виправлення, або переналаштувати системи захисту, щоб закрити уразливості налаштуваннями або віртуальними патчами.

Але коли об'єкт захисту міняється сотні разів у день (нормальний режим для, наприклад, інтернет-банку), ці правила перестають бути ефективними: сканування й переналаштування тривають довше, ніж інтервал між змінами. Якщо додержуватися цих правил, системи захисту будуть постійно перебувати в режимі самонавчання й переналаштування й не зможуть ефективно забезпечувати безпеку.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи захисту корпоративних додатків, які розробляються за допомогою методології Agile.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи захисту корпоративних додатків, які розробляються за допомогою методології Agile.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем захисту корпоративних додатків, які розробляються за допомогою методології Agile.

– Дослідження системи захисту корпоративних додатків, які розробляються за допомогою методології Agile.

– Програмна реалізація системи захисту корпоративних додатків, які розробляються за допомогою методології Agile.

Об'єктом дослідження є процес захисту корпоративних додатків, які розробляються за допомогою методології Agile.

Предметом дослідження є методи захисту корпоративних додатків, які розробляються за допомогою методології Agile.

Методи дослідження базуються на методах захисту інформації, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Незважаючи на цю очевидну вимогу, сьогодні на ринку засобів захисту з'являється усе більше систем, орієнтованих на рішення приватних завдань, у тому числі покликаних робити протидію внутрішнім IT-загрозам. Однак, цей ефект (як ми покажемо далі) порою може досягатися за рахунок зниження ефективності протидії зовнішнім IT-загрозам, що, на наш погляд, неприпустимо.

Для ілюстрації сказаного будемо розглядати питання реалізації лише одного механізму захисту (правда, відзначимо, ключового в частині рішення завдань протидії внутрішнім IT-загрозам) – механізму контролю доступу до ресурсів.

Призначення механізму контролю доступу до ресурсів

Ключовим механізмом захисту інформації є контроль доступу до ресурсів, заснований на завданні й реалізації правил розмежування доступу до ресурсів для користувачів. Правила доступу, що задаються, завжди можуть бути представлені відповідною моделлю (або матрицею доступу).

Нехай множині $C = \{C_1,\ldots,C_к\}$ і $O = \{O_1,\ldots,O_k\}$ – відповідно лінійно впорядковані множині суб'єктів і об'єктів доступу. Як суб'єкт доступу C_i, $i = 1,\ldots,k$ розглядається як окремий суб'єкт, так і група суб'єктів, що володіють однаковими правами доступу (помітимо, що на практиці це можуть бути як різні користувачі, так і той самий користувач, що володіє різними правами доступу при різних режимах обробки інформації), відповідно, як об'єкт доступу O_i, $i = 1,\ldots,k$ може також розглядатися як окремий об'єкт, так і група об'єктів, характеризуемих однаковими правами доступу до них.

Нехай $S = \{0, Чт, Зп\}$ – множин прав доступу, де «0» позначає відсутність доступу суб'єкта до об'єкта, «Чт» – дозвіл доступу для читання об'єкта, «Зп» – дозвіл доступу для запису в об'єкт.

Канонічну модель контролю доступу (модель контролю доступу, що реалізує базові вимоги до механізму захисту) можна представити матрицею доступу D, що має наступний вид:

$$D = \begin{array}{c} \\ O_1 \\ O_2 \\ \cdot \\ \cdot \\ \cdot \\ O_{k-1} \\ O_k \end{array} \begin{array}{c} \begin{array}{cccc} C_1 & C_2\ldots & C_{k-1} & C_k \end{array} \\ \begin{bmatrix} Зп/Чт & 0 & 0 & 0 \\ 0 & Зп/Чт & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & Зп/Чт & 0 \\ 0 & 0 & 0 & Зп/Чт \end{bmatrix} \end{array}$$

Під канонічною моделлю контролю доступу для лінійно впорядкованих множин суб'єктів (груп суб'єктів) і об'єктів (груп об'єктів) доступу розуміється модель, описувана матрицею доступу, елементи головної діагоналі якої «Зп/Чт» задають право повного доступу суб'єктів до об'єктів, інші елементи «0» задають заборона доступу суб'єктів до об'єктів.

Помітимо, що канонічна модель контролю доступу описує режим ізольованої обробки інформації, при якому об'єкти не можуть служити каналами взаємодії суб'єктів.

Сьогодні при реалізації приватних рішень по протидії внутрішнім IT-загрозам широко використовується повноважний контроль доступу. Його практичне використання в даних додатках обумовлене тим, що в корпоративних системах, як правило, на тому самому комп'ютері обробляється різна за рівнем конфіденційності інформація, що дозволяє її категоризувати («відкрита», «конфіденційна», «строго конфіденційна» і т.д.), при цьому необхідно забезпечити різні режими обробки інформації різних категорій на основі завдання відповідних повноважень суб'єктам доступу (звідки й назва) до категоризуваних об'єктів.

Основу повноважного контролю доступу становить спосіб формалізації понять «група користувачів» і «група об'єктів», на підставі шкали повноважень, що вводиться. Найбільше широко на практиці використовується спосіб ієрархічної формалізації відносини повноважень, що складає в наступному. Ієрархічна шкала повноважень уводиться на основі категоризування даних (відкриті, конфіденційні, строго конфіденційні й т.д.) і прав допуску до даних користувачів (за аналогією з поняттям «форми допуску»). Будемо вважати, що чим вище повноваження суб'єкта й категорія об'єкта, тим відповідно, менше їхній порядковий номер у лінійно повноважно впорядкованих множинах суб'єктів і об'єктів – $C = \{C_1,\ldots,C_к\}$ і $O = \{O_1,\ldots,O_k\}$).

Відповідна формалізація правил доступу суб'єктів до об'єктів при цьому, як правило, зводиться до наступного:

– суб'єкт має право доступу «Зп/Чт» до об'єкта в тому випадку, якщо повноваження суб'єкта й категорія об'єкта збігаються;

– суб'єкт має право доступу «Чт» до об'єкта в тому випадку, якщо повноваження суб'єкта вище, ніж категорія об'єкта;

– суб'єкт не має прав доступу до об'єкта в тому випадку, якщо повноваження суб'єкта нижче, ніж категорія об'єкта.

Матриця доступу D, що описує повноважну модель контролю доступу, має такий вигляд:

$$D = \begin{array}{c} \\ O_1 \\ O_2 \\ \cdot \\ \cdot \\ \cdot \\ O_{k-1} \\ O_k \end{array} \begin{array}{c} \begin{array}{cccc} C_1 & C_2\ldots & C_{k-1} & C_k \end{array} \\ \left[\begin{array}{cccc} Зп/Чт & 0 & 0 & 0 \\ Чт & Зп/Чт & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots \\ Чт & Чт & Зп/Чт & 0 \\ Чт & Чт & Чт & Зп/Чт \end{array}\right] \end{array}$$

Таким чином, основне завдання, розв'язуване при реалізації даного способу контролю доступу, складається в запобіганні можливості зниження категорії інформації при її обробці. Іноді додатково вводиться правило, що дозволяє запис інформації більше низької категорії в об'єкти більше високої категорії, що також не суперечить ідеї протидії зниженню категорії інформації; матриця доступу D, що описує повноважну модель контролю доступу, при цьому має такий вигляд:

$$D = \begin{array}{c} \\ O_1 \\ O_2 \\ . \\ . \\ . \\ O_{k-1} \\ O_k \end{array} \begin{array}{c} \begin{array}{cccc} C_1 & C_2 \ldots & C_{k-1} & C_k \end{array} \\ \left[\begin{array}{cccc} Зп/Чт & Зп & Зп & Зп \\ Чт & Зп/Чт & Зп & Зп \\ & & & \\ & & & \\ Чт & Чт & Зп/Чт & Зп \\ Чт & Чт & Чт & Зп/Чт \end{array}\right] \end{array}$$

Можливість роботи того самого користувача з даними різних категорій більшістю відомих реалізацій повноважного контролю доступу забезпечується тим, що в системі реалізуються динамічні повноваження користувача, змінювані стосовно до тому, з документом якої категорії користувач працює. Коректність реалізації повноважного контролю тут забезпечується тим, що дозволяється змінювати категорію лише убік її підвищення (C_k C_{k-1}, …C_1) – після читання відкритого документа користувачеві дозволяється зберігати дані в об'єкт категорії «відкрито», після читання конфіденційного документа користувачеві дозволяється зберігати дані в об'єкт категорії «конфіденційно», причому всі відкриті раніше документи категорії «відкрите» також дозволяється зберігати тільки в об'єкт категорії «конфіденційно».

У порядку зауваження відзначимо, що саме це рішення вже істотно знижує ефективність захисту інформації, не дозволяючи забезпечити різні режими обробки інформації різних категорій. Пояснимо сказане, при цьому не будемо забувати, що основу розмежувальної політики доступу до ресурсів в ОС Windows становить призначення атрибутів доступу об'єктам і привілеїв користувачам. Серед цих привілеїв є дуже важливі, наприклад, дозволити тільки локальний вхід у систему й ін. Привілеї призначаються облікового запису. При розглянутому ж підході до рішення завдання (повноважний контроль доступу), доступ до інформації різних категорій здійснюється під однією й тим же обліковим записом, що унеможливлює при такому рішень призначати різні привілеї користувачеві при обробці інформації різної категорії. На наш погляд, уже цього досить, щоб визнати подібне рішення не самим удалим. Однак у статті мова йтиме про іншому.

Завдання антивірусного захисту в корпоративних додатках

Класично завдання захисту інформації складається не тільки в захисті від порушення її конфіденційності, але й у забезпеченні її доступності й цілісності. А в цій частині особлива увага варто звернути на протидію можливому її «зараженню» макровірусами, що є вже завданням протидії зовнішнім IT-загрозам.

Проілюструємо, у чому складається особливість розглянутих додатків (обробка інформації на підприємстві).

– Обробка категоризованої інформації (наприклад, «конфіденційно» і «відкрите») апріорі припускає, що в першу чергу об'єктом захисту є інформація більше високих категорій (зокрема, у першу чергу варто захищати конфіденційну інформацію, робота з відкритою інформацією в даних додатках є опціональною, і її захист не настільки важливий).

– Обробка категоризованої інформації (наприклад, «конфіденційно» і «відкрите») апріорі припускає різні режими створення, обробки й зберігання інформації різних категорій, причому, чим вище категорія інформації, тим більше тверді обмеження накладаються на її обробку (зокрема, конфіденційну інформацію, як правило, дозволяється створювати тільки на обчислювальних засобах підприємства, причому певним набором додатків, зберігання й обмін даною інформацією з мережі або з використанням мобільних накопичувачів також здійснюється між обчислювальними засобами корпоративної мережі, які повинні бути

захищені, що вимагає обробка конфіденційних даних, відкрита ж інформація може надходити з неперевірених джерел, що не припускає реалізації яких-небудь регламентів по її створенню, обробці й зберіганню).

– Як наслідок, імовірність того, що «заражено» макровірусом відкритий документ на порядки вище, ніж конфіденційний, відповідно, чим вище категорія документа (жорсткіше регламенти на режими його обробки), тим менше ймовірність того, що документ «заражений» макровірусом.

Із усього сказаного можемо зробити дуже важливий висновок: чим нижче категорія документа, тим менш він має потребу в захисті від «зараження», що, у тому числі, позначається на реалізованих режимах його обробки, як наслідок, тим більшою ймовірністю бути «зараженим» він характеризується.

З обліком же того, що на тому самому комп'ютері обробляється як відкрита (яка має більшу ймовірність «зараження»), так і конфіденційна (яку необхідно захищати від «зараження») інформація, може бути сформульоване завдання антивірусного захисту в наступній постановці: забезпечити захист конфіденційних даних від макровірусів, якими з великою ймовірністю можуть бути «заражені» відкриті документи, тобто запобігти поширенню вірусу на конфіденційні дані. У загальному ж випадку (при наявності декількох категорій конфіденційності) завдання може бути сформульована в такий спосіб: запобігти поширенню вірусу на дані більше високої категорії конфіденційності.

Модель імовірнісного контролю доступу до ресурсів

Як і раніше, будемо вважати, що чим вище повноваження суб'єкта й категорія об'єкта, тим відповідно, менше їхній порядковий номер у лінійно повноважно впорядкованих множинах суб'єктів і об'єктів – $C = \{C_1,\ldots,C_к\}$ і $O = \{O_1,\ldots,O_k\}$).

Позначимо ж через P_i імовірність того, що документ і-й категорії «заражений» макровірусом, при цьому (як було сказано вище) апріорі маємо:

$$P_1 < P_2 < \ldots < P_k \ldots$$

Беручи до уваги той факт, що макровірус починає діяти (що може нести в собі загрозу «зараження») лише після прочитання його відповідним додатком і що запобігати треба можливість «зараження» документа більше високої категорії макровірусом з документа більше низької категорії (після його прочитання додатком), одержуємо наступну матрицю доступу F, що описує імовірнісну модель контролю доступу, реалізовану для антивірусної протидії:

$$F = \begin{array}{c} \\ O_1\,(P_1) \\ O_2\,(P_2) \\ \vdots \\ O_{k-1}(P_{k-1}) \\ O_k\,(P_k) \end{array} \begin{array}{c} \begin{array}{cccc} C_1 & C_2 \ldots . & C_{k-1} & C_k \end{array} \\ \left[\begin{array}{cccc} \text{Зп/Чт} & \text{Чт} & \text{Чт} & \text{Чт} \\ \text{Зп} & \text{Зп/Чт} & \text{Чт} & \text{Чт} \\ \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots \\ \text{Зп} & \text{Зп} & \text{Зп/Чт} & \text{Чт} \\ \text{Зп} & \text{Зп} & \text{Зп} & \text{Зп/Чт} \end{array}\right] \end{array}$$

Бачимо, що при реалізації даної моделі контролю доступу дозволяється запис документів, що мають меншу ймовірність зараження макровірусом в об'єкти, документи в які мають більшу ймовірність зараження макровірусом – зворотне заборонено, тобто запобігає підвищення ймовірності «зараження» документів більше високої категорії конфіденційності, за рахунок того, що одночасно з ними на тому самому комп'ютері можуть створюватися, оброблятися й зберігатися документи більше низької категорії, імовірність «зараження» макровірусом яких вище.

Бачимо, що при реалізації даної схеми ймовірність «зараження» документа більше високої категорії, наприклад, O_1 (P_1) не змінюється у зв'язку з тим, що на тім же комп'ютері обробляється інформація більше низької категорії, наприклад, O_k (P_k). При цьому будемо розуміти, що режими обробки інформації різних категорій можуть кардинально розрізнятися (наприклад, при обробці на одному комп'ютері відкритої O_k і конфіденційної інформації O_1, маємо: $P_k >> P_1$, причому залежно від реалізованих правил і організаційних заходів щодо обробки конфіденційних даних це відношення може становити сотні, тисячі й більше раз, тобто саме в стільки разів можна знизити ймовірність «зараження» конфіденційних даних макровірусами, що зберігаються у відкритих даних, для яких порию, $P_k = 1$).

Недоліки приватного рішення. Комплексний підхід до реалізації контролю доступу до ресурсів у корпоративних додатках

Зрівняємо матриці D і F. Бачимо, що вони повністю суперечать один одному, тобто вимоги до реалізації повноважного контролю доступу при рішенні альтернативних завдань захисту інформації не те щоб були різні – вони суперечливі.

З погляду протидії зовнішнім IT-загрозам (у частині антивірусного захисту) практичне використання механізмів повноважного контролю доступу неприпустимо. Це обумовлюється тим, що, як видно із проведеного дослідження, при реалізації приватного рішення, заснованого на використанні повноважного контролю доступу, кардинально знижується ефективність протидії зовнішнім IT-загрозам.

У порядку зауваження відзначимо, що підвищення ймовірності вірусного впливу на конфіденційні дані – це не єдина причина зниження ефективності протидії зовнішнім IT-загрозам при реалізації повноважного контролю доступу. У цьому випадку підвищується й імовірність успішної мережної атаки, тому що мережні служби в цьому випадку запускаються під обліковим записом, що має доступ до конфіденційної інформації, і ін.

Колись розглянемо, яку інформацію ми категоризуэм, стосовно до рішення завдання антивірусного захисту. Природно, що якісна відмінність в обробці має відкрита інформація й конфіденційна інформація, тобто ми можемо виділити дві основні категорії: «відкрите» і «конфіденційно». При цьому обробка конфіденційної інформації різних категорій, у частині ймовірності бути вихідно «зараженої» макровірусом, уже відрізняється не настільки істотно. З обліком сказаного на практиці має сенс розглядати насамперед наступне відношення ймовірностей того, що документ і-й категорії «заражений» макровірусом, позначивши категорію «відкрите», як k, маємо:

$$P_1 = P_2 = \ldots = P_{k-1} << P_k \ldots$$

Природно, що якщо ми не можемо дозволити ні читання, ні запис (тому що ці вимоги суперечливі в матрицях доступу), те залишається лише одне рішення, пов'язане з повною забороною доступу. З обліком сказаного одержуємо модель повноважного контролю доступу, реалізація якої дозволяє вирішувати розглянуті альтернативні завдання в комплексі, описувану матрицею доступу D(F):

$$D(F) = \begin{array}{c} \\ O_1 \\ O_2 \\ . \\ . \\ . \\ O_{k-1} \\ O_k \end{array} \begin{array}{c} \begin{array}{cccc} C_1 & C_2 \ldots . & C_{k-1} & C_k \end{array} \\ \begin{bmatrix} Зп/Чт & 0 & 0 & 0 \\ Чт & Зп/Чт & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots \\ Чт & Чт & Зп/Чт & 0 \\ 0 & 0 & 0 & Зп/Чт \end{bmatrix} \end{array}$$

Помітимо, що при такому підході до реалізації повноважного контролю доступу обробка відкритих даних по суті повністю ізолюється від обробки конфіденційних даних. Результатом такого рішення, що ніяк не суперечить ідеї обробки даних на основі повноважень користувачів і категорій об'єктів, є те, що підвищення ймовірності «зараження» макровірусом відкритих даних ніяк не позначається на ймовірності «зараження» макровірусом конфіденційних даних, що визначається умовою:

$$P_1 = P_2 = \ldots = P_{k-1} << P_k...$$

Важливим тут є той момент, що якщо на ймовірність «зараження» макровірусом відкритих даних вплинути практично неможливо, крім як зменшити її значення, за рахунок застосування спеціалізованих антивірусних засобів захисту (що, з одного боку, не дасть рішення в загальному виді, тому що сигнатурний аналіз дозволяє знаходити тільки відомі макровіруси, з іншого боку, у даних додатках виглядає трохи дивним – захищаємо відкриті дані, загалом кажучи не дуже й нужденні в захисті, щоб в остаточному підсумку вберегти від «зараження» конфіденційні дані), те ймовірність «зараження» макровірусом конфіденційних даних можна істотно знизити (на порядки – у сотні, у тисячі, а може бути, і більше раз, реалізувавши відповідні організаційні заходи щодо їхньої обробки (які й так апріорі повинні бути реалізовані, але вже з метою протидії зниженню їхньої категорії)).

Якщо під окремим обліковим записом реалізується доступ у зовнішню мережу, причому під цим обліковим записом не дозволений доступ до конфіденційних даних, то значно знижується й імовірність несанкціонованого доступу до конфіденційної інформації й з мережі.

Матриця D(F) ілюструє той факт, що при обробці на комп'ютері інформації тільки двох категорій («відкритий» і «конфіденційно» – найпоширеніший випадок), з погляду рішення завдання захисту інформації в комплексі використання повноважного контролю доступу неприпустимо (а це адже найпоширеніший випадок категоризування інформації на практиці).

У порядку зауваження відзначимо, що в загальному випадку, використовуючи розглянутий підхід (забороняючи відповідні права доступу), можна формувати різні правила контролю доступу (різні варіанти захисту від «зараження» макровірусом конфіденційних даних). Один із прикладів відповідної матриці (ізолюється обробка даних, найвищої категорії) доступу представлений нижче:

$$D(F) = \begin{array}{c} \\ O_1 \\ O_2 \\ . \\ . \\ . \\ O_{k-1} \\ O_k \end{array} \begin{array}{c} \begin{array}{cccc} C_1 & C_2 \ldots . & C_{k-1} & C_k \end{array} \\ \begin{bmatrix} Зп/Чт & 0 & 0 & 0 \\ 0 & Зп/Чт & 0 & 0 \\ & \cdots\cdots\cdots & & \\ & \cdots\cdots\cdots & & \\ 0 & Чт & Зп/Чт & 0 \\ 0 & Чт & Чт & Зп/Чт \end{bmatrix} \end{array}$$

У порядку зауваження відзначимо, що за умови:

$$P_1 << P_2 << \ldots << P_{k-1} << P_k,$$

повинна бути реалізована канонічна модель контролю доступу.

Бачимо, що при реалізації комплексного підходу до рішення вже не доцільна яка-небудь жорстко задана формалізація відносин на основі міток безпеки (або категорій і повноважень), у цьому випадку доцільне завдання правил розмежування доступу суб'єктів до

об'єктів на основі матриці доступу, що дозволяє реалізувати необхідні для конкретних умов використання засобу захисту інформації правила розмежування доступу, що забезпечують ефективну протидію як внутрішнім, так і зовнішнім ІТ-загрозам.

На закінчення відзначимо, що засіб захисту повинне вирішувати в комплексі необхідний набір завдань захисту, актуальних для конкретного додатка, зокрема, стосовно до захисту конфіденційної інформації – забезпечувати протидія як внутрішнім, так і зовнішнім ІТ-загрозам.

Реалізація ж приватних рішень не повинна знижувати результуючої ефективності захисту інформації, що можливо через те, що рішення для альтернативних типів загроз можуть взаємно виключати один одного, внаслідок чого реалізація приватного рішення може приводити до підвищення ефективності протидії одній групі загроз за рахунок зниження ефективності протидії іншій групі загроз.

Розробка структурної схеми

Agile

Гнучка методологія розробки (англ. Agile software development, agile-методи) – серія підходів до розробки програмного забезпечення, орієнтованих на використання ітеративної розробки, динамічне формування вимог і забезпечення їхньої реалізації в результаті постійної взаємодії усередині робочих груп, що самоорганізуються, що складаються з фахівців різного профілю [1]. Існує кілька методик, що відносяться до класу гнучких методологій розробки, зокрема екстремальне програмування, DSDM, Scrum, FDD.

Застосовується як ефективна практика організації праці невеликих груп (які роблять однорідну творчу роботу) в об'єднанні з керуванням ними комбінованим (ліберальним і демократичним) методом.

Більшість гнучких методологій націлені на мінімізацію ризиків шляхом відомості розробки до серії коротких циклів, називаних ітераціями, які звичайно тривають дві-три тижні. Кожна ітерація сама по собі виглядає як програмний проект у мініатюрі й включає всі завдання, необхідні для видачі міні-приросту по функціональності: планування, аналіз вимог, проектування, програмування, тестування й документування. Хоча окрема ітерація, як правило, недостатня для випуску нової версії продукту, мається на увазі, що гнучкий програмний проект готовий до випуску наприкінці кожної ітерації. По закінченні кожної ітерації команда виконує переоцінку пріоритетів розробки.

Agile-методи наголошують на безпосереднє спілкування віч-на-віч. Більшість agile-команд розташовані в одному офісі, іноді називаному англ. bullpen. Як мінімум, вона включає й «замовників» (англ. product owner – замовник або його повноважний представник, що визначає вимоги до продукту; цю роль може виконувати менеджер проекту, бізнес-аналітик або клієнт). Офіс може також включати тестувальників, дизайнерів інтерфейсу, технічних письменників і менеджерів.

Основною метрикою agile-методів є робочий продукт. Віддаючи перевагу безпосередньому спілкуванню, agile-методи зменшують обсяг письмової документації в порівнянні з іншими методами. Це привело до критики цих методів як недисциплінованих.

У лютому 2001 у штаті Юта США був випущений «Маніфест гнучкої методології розробки програмного забезпечення» (англ. Agile Manifesto). Він був альтернативою керованим документацією «великоваговим» практикам розробки програмного забезпечення, таким як «метод водоспаду», що був золотим стандартом розробки в той час. Даний маніфест був схвалений і підписаний представниками методологій: екстремального програмування, Crystal Clear [en], DSDM, Feature driven development, Scrum, Adaptive software development [en], Pragmatic Programming. Гнучка методологія розробки використовувалася багатьма компаніями й до прийняття маніфесту, однак входження Agile-Розробки в маси відбулося саме після цієї події.

Agile – сімейство процесів розробки, а не єдиний підхід у розробці програмного забезпечення, і визначається Agile Manifesto [2]. Agile не включає практик, а визначає цінності й принципи, якими керуються команди.

Agile Manifesto розроблений і прийнятий 11-13 лютого 2001 року на лижному курорті The Lodge at Snowbird у горах Юти. Agile Manifesto містить 4 основні ідеї й 12 принципів. Примітно, що Agile Manifesto не містить практичних рад.

Основні ідеї:

– люди й взаємодія важливіше процесів і інструментів;
– працюючий продукт важливіше вичерпної документації;
– співробітництво із замовником важливіше узгодження умов контракту;
– готовність до змін важливіше проходження первісному плану.

Принципи, які роз'ясняє Agile Manifesto [3]:

– задоволення клієнта за рахунок ранньої й безперебійної поставки коштовного програмного забезпечення;
– вітання змін вимог навіть наприкінці розробки (це може підвищити конкурентоспроможність отриманого продукту);
– часта поставка робочого програмного забезпечення (щомісяця або тиждень або ще частіше);
– тісне, щоденне спілкування замовника з розроблювачами протягом усього проекту;
– проектом займаються мотивовані особистості, які забезпечені потрібними умовами роботи, підтримкою й довірою;
– метод передачі, що рекомендується, інформації – особиста розмова (віч-на-віч);
– працююче програмне забезпечення – кращий вимірник прогресу;
– спонсори, розроблювачі й користувачі повинні мати можливість підтримувати постійний темп на невизначений строк;
– постійна увага поліпшенню технічної майстерності й зручному дизайну;
– простота – мистецтво не робити зайвої роботи;
– кращі технічні вимоги, дизайн і архітектура виходять у самоорганізованої команди;
– постійна адаптація до обставин, що змінюються. Команда повинна систематично аналізувати можливі способи поліпшення ефективності й відповідно коректувати стиль своєї роботи. [4]

Один з повторюваних пунктів критики: при agile-підході часто зневажають створенням плану («дорожньої карти») розвитку продукту, так само як і керуванням вимогами, у процесі якого й формується така «карта». Гнучкий підхід до керування вимогами не має на увазі далеко, що йдуть планів (по суті, керування вимогами просто не існує в даній методології), а має на увазі можливість замовника раптом і зненацька наприкінці кожної ітерації виставляти нові вимоги, що часто суперечать архітектурі вже створеного й поставляти^ся продукта, що. Таке іноді приводить до катастрофічного «авралам» з масовим рефакторингом і переробками практично на кожній черговій ітерації.

Крім того, уважається, що робота в agile мотивує розроблювачів вирішувати всі завдання, що надійшли, найпростішим і найшвидшим можливим способом, при цьому найчастіше не обертаючи уваги на правильність коду з погляду вимог нижчележачої платформи (підхід – «працює, і добре», при цьому не враховується, що може перестати працювати при найменшій зміні або ж дати важкі до відтворення дефекти після реального впровадження в клієнта). Це приводить до зниження якості продукту й нагромадженню дефектів.

Існують методології, які дотримуються цінностей і принципів заявлених в Agile Manifesto, деякі з них:

– Agile Modeling (англ.) – набір понять, принципів і прийомів (практик), що дозволяють швидко й просто виконувати моделювання й документування в проектах розробки програмного забезпечення. Не містить у собі детальну інструкцію із проектування, не містить описів, як будувати діаграми на UML. Основна мета: ефективне моделювання й документування; але не охоплює програмування й тестування, не включає питання

керування проектом, розгортання й супроводи системи. Однак містить у собі перевірку моделі кодом [5].

– Agile Unified Process (англ.) (AUP) спрощена версія IBM Rational Unified Process (RUP), розроблена Скоттом Амблером, що описує просте й зрозуміле наближення (модель) для створення програмного забезпечення для бізнес-додатків.

– Agile Data Method (англ.) – група ітеративних методів розробки програмного забезпечення, у яких вимоги й рішення досягаються в рамках співробітництва різних крос-функціональних команд.

– DSDM заснований на концепції швидкої розробки додатків (Rapid Application Development, RAD). Являє собою ітеративний і інкрементний підхід, що надає особливого значення тривалій участі в процесі користувача/споживача.

– Essential Unified Process (англ.) (EssUP).

– Екстремальне програмування (англ. Extreme programming, XP).

– Feature driven development (FDD) – функціонально-орієнтирована розробка. Використовуване в FDD поняття функції або властивості (англ. feature) системи досить близько до поняття прецеденту використання, використовуваній в RUP, істотна відмінність – це додаткове обмеження: «кожна функція повинна допускати реалізацію не більш, ніж за два тижні». Тобто якщо сценарій використання досить малий, його можна вважати функцією. Якщо ж великий, то його треба розбити на трохи щодо незалежних функцій.

– Getting Real – ітеративний підхід без функціональних специфікацій, що використовується для веб-додатків. У даному методі спершу розробляється інтерфейс програми, а потім її функціональна частина.

– OpenUP – це ітеративно-інкрементальний метод розробки програмного забезпечення. Позиціонується як легкий і гнучкий варіант RUP. OpenUP ділить життєвий цикл проекту на чотири фази: початкова фаза, фази уточнення, конструювання й передачі. Життєвий цикл проекту забезпечує надання зацікавленим особам і членам колективу крапок ознайомлення й прийняття рішень протягом усього проекту. Це дозволяє ефективно контролювати ситуацію й вчасно ухвалювати рішення щодо прийнятності результатів. План проекту визначає життєвий цикл, а кінцевим результатом є остаточний додаток.

– Scrum установлює правила керування процесом розробки й дозволяє використовувати вже існуючі практики кодування, коректуючи вимоги або вносячи тактичні зміни. Використання цієї методології дає можливість виявляти й усувати відхилення від бажаного результату на більше ранніх етапах розробки програмного продукту.

– Ощадлива розробка програмного забезпечення (англ. lean software development) використовує підходи з концепції ощадливого виробництва.

Розроблене програмне забезпечення представляє із себе набір компонентів призначених для забезпечення політики безпеки як у вже існуючих, так і в створюваних мережних корпоративних додатках, які розробляються за допомогою методології Agile.

Розроблене програмне забезпечення дозволяє забезпечити захист переданої по мережі інформації, строгу взаємну автентифікацію користувачів і серверів, гнучке розмежування доступу. Для реалізації цих функцій у системі використовуються SSL/TLS протоколи й X.509 цифрові сертифікати, тобто універсальні, що стали стандартом де-факто, механізми, підтримувані практично всіма розповсюдженими Веб-агентами.

За допомогою розробленого програмного забезпечення легко забезпечуються вимоги по інформаційній безпеці, запропоновані різними Інтернет додатками, такими як:

– сервера платіжних систем;

– інтернет-магазини;

– багатопрофільні корпоративні Веб-сервера, що містять інформацію з різним рівнем конфіденційності;

– B2B системи;

– системи захищеного документообігу;

– системи обміну електронною поштою;

– й багато які інші.

На рисунку 1 представлена структурна схема розробленої системи. Для поняття роботи системи введені наступні позначення:

– ЕЦП – електроний цифровий підпис;
– УЦ – удостовірюючий центр.
– ЦС – цифровий сертифікат;
– PKI – інфраструктура відкритих ключів;
– DVCS – Data Validation and Certification Server Protocols – протокол підтвердження даних та сертифікації серверу;
– OCSP – Online Certificate Status Protocol – онлайн протокол статусу сертфікату;
– TSP – Time-Stamp Protocol – протокол часових міток;
– TLS – криптографічний протокол, що забезпечує захищену передачу даних між вузлами в мережі Інтернет;
– RFC – документ, у якому описується той або інший стандарт.

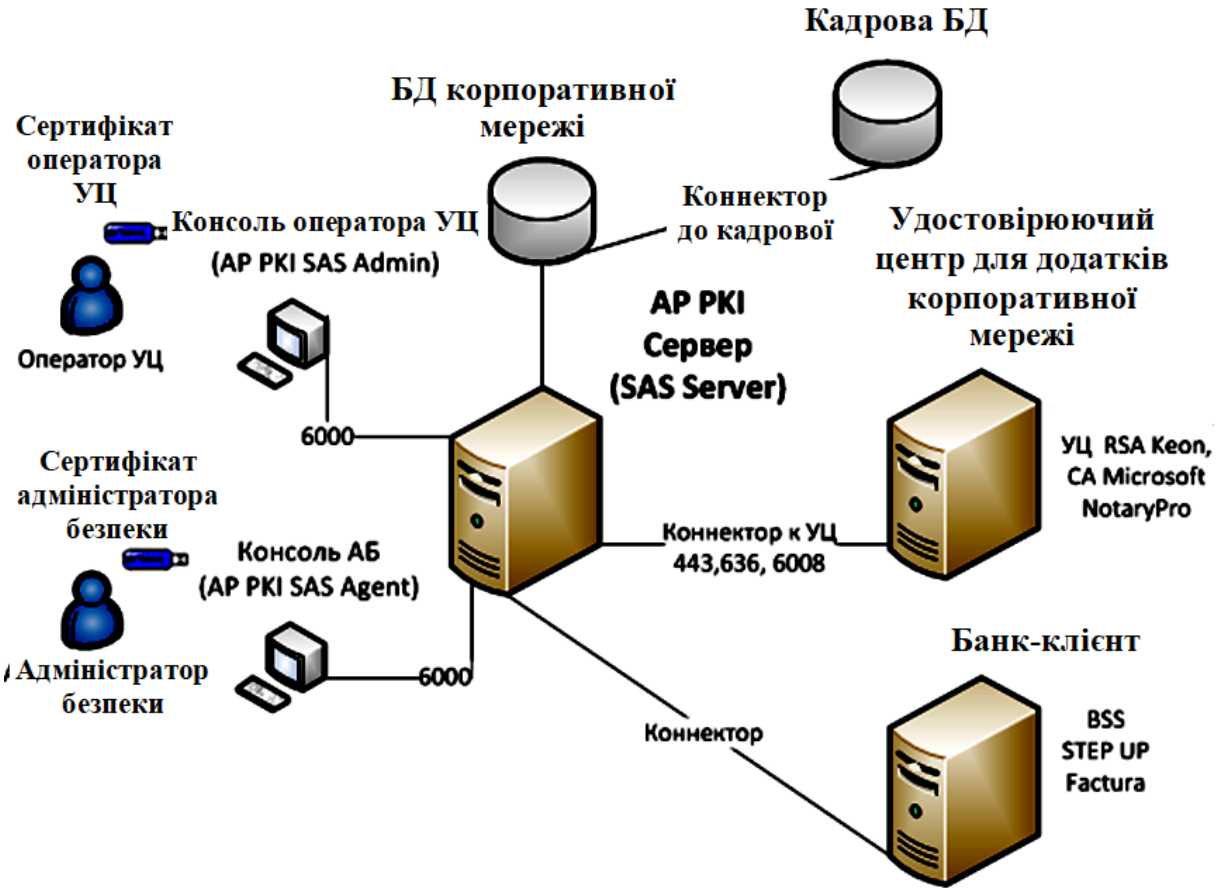


Рисунок 1 – Структурна схема системи

Розглянемо більш детально складові структурної схеми, та принцип роботи системи.

Удостовірюючий центр для додатків корпоративної мережі

Удостовірюючий центр для додатків корпоративної мережі (удостовірюючий центр – УЦ) є повністю вітчизняною розробкою:

– відповідає вимогам Доктрини інформаційної безпеки в плані заміщення імпортних технічних і програмних засобів у українських інформаційних системах;
– завдяки відомості всіх криптографічних процедур в ізольований криптографічний PKSC#11 токен, в УЦ можуть використовуватися як вітчизняні криптографічні алгоритми, так і закордонні;

– використовувані вітчизняні криптографічні механізми й протоколи опираються на інтернет драфти, розроблені вітчизняними компаніями, а отже, рішення сумісні з рішеннями інших вітчизняних виробників;

– технічна реалізація заснована на сучасних керівних документах, стандартах і міжнародних рекомендаціях, що дозволяє:

1) в одному технічному рішенні підтримувати невиразно велике число зовсім ізольованих, у тому числі з різними криптографічними алгоритмами, видавців;

2) підтримуються механізми кросування видавців (аж до рівня мостового УЦ), у тому числі й зовнішніх, для утворення єдиних зон обігу захищених документів;

3) для систем наближених до On-line передбачене поширення відновлень списків відкликаних сертифікатів (delta CRL);

4) компоненти самого УЦ для побудови ланцюжків сертифікації використовують внутрішній сервіс OCSP, що може бути оформлений як корпоративний зі складу служби "електронного нотаріату";

5) до складу системи входить власна служба роздачі міток часу, з механізмами підстроювання під зовнішні еталони;

6) відповідно до RFC 3039 Internet X.509 Public Key Infrastructure. Qualified Certificate Profile у сертифікат може бути введений серійний номер імені, тим самим вирішена "колізія імен" – проблема «однофамільців»;

7) реєстр крім самого сертифіката користувача може містити додаткову інформацію про суб'єкта, включаючи графічні елементи (фотографії, відбитки пальців і т.п.);

8) всі інформаційні блоки при транспортуванні й зберіганні захищені електронними цифровими підписами, що забезпечує цілісність, авторство й невідрікаємість і спрощує процедури розбору конфліктних ситуацій.

Удостовірюючий центр для додатків корпоративної мережі (УЦ) є основою комп’ютерних систем захищеного документообігу на технології відкритого розподілу ключів (Public Key Infrastructure (PKI)). Технічна реалізація Центра, що засвідчує, відповідає вимогам Закону України "Про електронний цифровий підпис" за умови використання в ЦУ сертифікованих ДСТЗІ СБУ засобів електронного цифрового підпису. УЦ, може виступати як ключовий компонентом для різного типу прикладних захищених систем корпоративного рівня (захищений документообіг, Інтернет-банкінг, білінгові системи, електронна комерція (B2C, B2B), Інтернет процесінг і.т.п.).

Сертифікат X.509 v3

Сертифікат X.509 v3 визначається в такий спосіб. Для обчислення підпису дані, які повинні бути підписані, представляються з використанням ASN.1 однозначних правил подання (DER).

```
Certificate ::= SEQUENCE {
   tbsCertificate     TBSCertificate,
   signatureAlgorithm AlgorithmIdentifier,
   signatureValue     BIT STRING
}
TBSCertificate ::= SEQUENCE {
   version [0] EXPLICIT Version DEFAULT v1,
   serialNumber CertificateSerialNumber,
   signature AlgorithmIdentifier,
   issuer Name,
   validity Validity,
   subject Name,
   subjectPublicKeyInfo SubjectPublicKeyInfo,
   issuerUniqueID [1] IMPLICIT
      UniqueIdentifier OPTIONAL,
   ---і якщо є присутнім, версія повинна
```

```
    ---і бути v2 або v3
    subjectUniqueID [2] IMPLICIT
       UniqueIdentifier OPTIONAL,
    ---і якщо є присутнім, версія повинна бути
    ---і v2 або v3
    extensions [3] EXPLICIT Extensions OPTIONAL
    ---і якщо є присутнім, версія повинна бути v3
}
Version ::= INTEGER { v1(0), v2(1), v3(2) }
CertificateSerialNumber ::= INTEGER
Validity ::= SEQUENCE {
   notBefore Time,
   notAfter  Time
}
Time ::= CHOICE {
   utcTime     UTCTime,
   generalTime GeneralizedTime
}
UniqueIdentifier ::= BIT STRING
SubjectPublicKeyInfo ::= SEQUENCE {
   algorithm        AlgorithmIdentifier,
   subjectPublicKey BIT STRING
}
Extensions ::= SEQUENCE SIZE (1..MAX) OF Extension
Extension ::= SEQUENCE  {
     extnID    OBJECT IDENTIFIER,
     critical  BOOLEAN DEFAULT FALSE,
     extnValue OCTET STRING
}
```

Поля сертифіката. Сертифікат є послідовність трьох обов'язкових полів: tbsCertificate, signatureAlgorithm і signatureValue.

– tbsCertificate. Поле містить імена суб'єкта й випускаючого, відкритий ключ, пов'язаний із суб'єктом, період дійсності й іншу пов'язану із цим сертифікатом інформацію. Поля докладно описані далі; tbsCertificate звичайно включають розширення, які теж будуть описані нижче.

– signatureAlgorithm. Поле signatureAlgorithm містить ідентифікатор криптографічного алгоритму, використовуваного УЦ для підписування даного сертифіката. Існують стандартні алгоритми, які повинні підтримуватися всіма реалізаціями, але конкретна реалізація може підтримувати й інші алгоритми.

Ідентифікатор алгоритму визначається наступної ASN.1-структурою:

```
AlgorithmIdentifier ::= SEQUENCE  {
  algorithm  OBJECT IDENTIFIER,
  parameters ANY DEFINED BY algorithm OPTIONAL
}
```

Ідентифікатор алгоритму використовується для визначення криптографічного алгоритму. Компонент OBJECT IDENTIFIER ідентифікує алгоритм (такий як DSA з SHA-1). Компоненти поля параметрів змінюються відповідно до зазначеного алгоритму. Поле повинне містити той же самий ідентифікатор алгоритму, що й поле підпису в tbsCertificate.

– signatureValue. Поле signatureValue містить цифровий підпис, обчислений для поля tbsCertificate, записаному в DER-поданні ASN.1. Це означає, що поле tbsCertificate, представлене як ASN.1 DER, використовується як вхід у функцію підпису. Отримане значення підпису представлене як BIT STRING і включено в поле підпису. Деталі даного

процесу можуть відрізнятися для кожного конкретного алгоритму підпису. Створенням даного підпису УЦ підтверджує дійсність інформації в поле tbsCertificate. Зокрема, УЦ підтверджує зв'язок між матеріалом відкритого ключа й суб'єктом сертифіката.

– TBSCertificate. Послідовність TBSCertificate містить інформацію, пов'язану із суб'єктом сертифіката й УЦ, що випустив сертифікат. Кожний TBSCertificate містить імена суб'єкта й випускаючого, відкритий ключ, пов'язаний із суб'єктом, період дійсності, номер версії й серійний номер сертифіката; деякі поля можуть (але це не обов'язково) містити унікальний ідентифікатор. Розглянемо синтаксис і семантику таких полів. TBSCertificate звичайно включає розширення. Розглянемо також найбільше часто використовувані в Internet розширення.

– Version. Дане поле описує версію подання сертифіката. Якщо використовуються розширення, то версія повинна бути 3 (значення – 2). Якщо розширення не зазначені, але UniqueIdentifier представлений, версія може бути 2 (значення – 1); але версія може бути й 3. Якщо представлені тільки базові поля, версія може бути 1 (значення в сертифікаті опущене як значення за замовчуванням); але версія може бути 2 або 3. Реалізації повинні бути готові приймати будь-яку версію сертифіката. Як мінімум конформні реалізації повинні розпізнавати версію 3 сертифікатів.

– Serial number. Серійний номер повинен бути позитивним цілим, призначуваним УЦ для кожного сертифіката. Він повинен бути унікальним для кожного сертифіката, випущеного даним УЦ. Таким чином, ім'я що выпустили й серійний номер однозначно визначають сертифікат. Cas повинні забезпечувати, щоб серійні номери були ненегативними цілими. Уважається, що серійні номери можуть мати довжину до 20 октетів.

– Signature. Дане поле містить ідентифікатор алгоритму, використовуваного УЦ для підписування сертифіката.

– Дане поле повинне містити той же самий ідентифікатор алгоритму, що й поле signatureAlgorithm в Certificate. Зміст необов'язкового поля параметрів залежить від конкретного алгоритму.

– Issuer. Поле issuer ідентифікує того, хто підписав і випустив сертифікат. Поле issuer повинне містити непусте унікальне ім'я (DN). Ім'я визначається у відповідності з наступної ASN.1 структурою:

```
Name ::= CHOICE { RDNSequence }
RDNSequence ::= SEQUENCE OF
   RelativeDistinguishedName
RelativeDistinguishedName ::=
   SET OF AttributeTypeAndValue
AttributeTypeAndValue ::= SEQUENCE {
   type   AttributeType,
   value  AttributeValue
}
AttributeType ::= OBJECT IDENTIFIER
AttributeValue ::= ANY DEFINED BY
   AttributeType
```

Ім'я описує ієрархічне ім'я, що складається з атрибутів, таких, наприклад, як назва країни, і відповідних значень, таких як RU. Тип компонента AttributeValue визначається значенням AttributeType. Стандарт X.509 не обмежує набір типів атрибутів, які можуть з'явитися в ім'ї. Проте, стандартом рекомендується підтримувати наступні типи атрибутів в іменах випускаючі й суб'єкта:

– Країна.
– Організація.
– Організаційна одиниця.
– Позначення унікального імені.
– Назва штату або регіону.

– Загальноприйняте ім'я (наприклад, Іванов Іван).
– Серійний номер.

Додатково можуть бути присутнім деякі інші типи атрибутів в іменах випускаючі й суб'єкта, наприклад:

– Локалізація.
– Заголовок.
– По батькові.
– Призначене ім'я.
– Ініціали.
– Псевдонім.
– Спеціальна назва (наприклад, "Jr.", " 3-ій" або "IV").

Також може бути присутнім атрибут domainComponent. DNS надає собою ієрархічну систему позначення ресурсів. Даний атрибут надає зручний механізм для організацій, які хочуть використовувати унікальні DN імена паралельно зі своїми DNS-Іменами. Це не заміняє dNSName компонент альтернативного поля ім'я. Стандарт не вимагає конвертувати такі імена в DNS-Імена.

Сторона, що перевіряє, повинна обробляти поля унікального ім'я випускаючого й унікального ім'я суб'єкта для одержання ланцюжка імен при перевірці *дійсності сертифікаційного* шляху. Ланцюжок імен виходить у випадку відповідності унікального ім'я випускаючого в першому сертифікаті ім'я суб'єкта в сертифікаті УЦ.

Служба "Електронного нотаріату"

"Електронний нотаріус" (ЕН) може бути як додатковим сервісом в комп’ютерній системі, що виконує функції Центра, що засвідчує (УЦ) сертифікатів ключів підпису в якості стандартизованого RFC 3029 Internet X.509 Public Key Infrastructure Data Validation and Certification Server Protocols (DVCS). RFC 2560 Online Certificate Status Protocol – OCSP. RFC 3161 Time-Stamp Protocol (TSP)) технічного рішення «Про Електронний цифровий підпис», так і як самостійний програмний комплекс, і реалізовувати разову або абонентську послугу з перевірки й сертифікації інформації, перевірки сертифікатів і виробленню квитанції, що містять «штамп» часу. В ЕН зведені служби, технічна реалізація яких стандартизована міжнародними рекомендаціями, по фактах усіляких перевірок, підтверджень і вироблення «штампа часу» для зовнішніх компонентів інфраструктури відкритих ключів.

"Електронний нотаріус" виконує наступні функції:

– Посвідчення факту володіння інформацією з або без її подання сервісу.
– Перевірка дійсності ЕЦП.
– Перевірка дійсності сертифіката відкритого ключа (для компонентів DVCS або OCSP).
– Вироблення квитанції, що містить «штамп» часу (TSP).

Задачі, у рішенні яких, може бути використана Служба "Електронного нотаріату":

1. Створення єдиного домена захищеного електронного документообігу, у тому числі побудованому на несумісних між собою засобах криптографічного захисту інформації, але маючих сертифікат ДСТЗІ СБУ на засоби криптографічного захисту інформації для гетерогенних програмно-апаратних платформ.
2. Одержання штампа «дійсного часу для даної PKI системи» на завіреному електронному документі. Досить важливо (для попередження шахрайських дій або колізій) при завіренні електронного документа коректно вказувати дату підписання, однак проставляння дійсної дати цілком є відповідальністю підписується стороны, що. ЕН у цьому випадку є «третьою» стороною – довіреному арбітром, що фіксує факт наявності дійсної ЕЦП на конкретний момент часу. Даний сервіс іноді називають Time Stamping. Наявність «третьої» незалежної сторони може виявитися корисною щоб зафіксувати певний етап у технологічному ланцюжку документообігу (якийсь документ пройшов яку те стадію свого формування), наприклад, на конкретний момент часу податкова декларація завірена й

доставлена від платника податків в інспекцію. У більше широкому змісті ЕН може бути використаний абстрактною прикладною системою як джерело TSP міток «еталонного часу».

3. Тривале архівне зберігання електронних документів. ЕЦП на електронному документі має «строк життя», що, зокрема визначається «строком життя» персонального сертифіката, який бере участь у формуванні ЕЦП. Через багато причин цей час досить обмежений, що не дозволяє будувати повноцінну систему документообігу, включаючи такий важливий компонент як архівне зберігання. Наявність DVC квитанцій по перевірці ЕЦП дозволяє робити висновки про дійсність ЕЦП уже після витікання часу дійсності сертифіката, що брав участь у виробленні даної ЕЦП. Дана властивість пояснюється тим, що сертифікат ЕН (DVCS), яким завірена квитанція, більш тривала й існують механізми пролонгації квитанцій (випуск квитанції на квитанцію).

4. Організація перевірки ЕЦП «третьою» стороною для користувачів дозволяє перевести сам факт перевірки із площини криптографічних обчислень на сертифікованих серверах захисту інформації в площину організації довіреної доставки квитанцій із сервера ЕН, що в багатьох випадках значно технологічніше. Ступінь «доручення» доставки квитанцій не регламентується законом «Про ЕЦП» і цілком визначається специфікою комп'ютерної системи, у якій використовуються завірені документи. Способів доставки досить багато: від доставки квитанції кур'єрською службою, підтвердженням по телефоні, порівнянням самих файлів – квитанцій отриманих по мережі й з репозиторія ЕН (DVCS), до організації захищених сегментів мережі, на підтвердження що мають, наприклад, атестат ДСТЗІ СБУ.

5. Покладання на сервіс ЕН функцію перевірки дійсності якогось цифрового сертифіката істотно спрощує комп'ютерну систему, у якій циркулюють завірені електронні документи. Сама по собі процедура перевірки сертифіката досить трудомістка, необхідно побудувати ланцюжок перевірки кінцевого сертифіката з перевіркою всіх проміжних кореневих сертифікатів, визначити місце розповсюдження, одержати й обробити списки відкликаних сертифікатів і т.п.

6. Даний сервіс може бути досить корисний для комп'ютерних систем (КС), у яких використовується факт володіння користувачем якоюсь інформацією без її опублікування. Наприклад, КС проведення різних тендерів, регламент яких визначає, що до певного строку ніхто не повинен мати доступ до конкурсного матеріалу (за винятком коротких анотацій) і тільки по настанню часу початку конкурсу «конверти» повинні бути розкриті. Для таких систем учасники представляють квитанції на істинність ЕЦП конкурсного матеріалу без фактичної передачі самого матеріалу до моменту настання конкурсу. Істинність представленого в наслідку матеріалу підтверджено ЕЦП зі складу DVC квитанції. У цьому випадку захист конкурсного матеріалу покладає на самих конкурсантів – самих зацікавлених у захисті даних осіб і повністю знімає ризик шахрайства в системі.

Служба атрибутування (реалізація заснована на RFC 3281) вирішує дві задачі:

– Дозволяє здійснити криптографічний зв'язок сертифіката ключа підпису з додатковою інформацією, захищеної ЕЦП, що визначає роль власника сертифіката в КС, наприклад, для цілей розмежування доступу, розміщення персональної інформації, розміщення інформації уточнюючого повноваження й т.п.

– Дозволяє здійснити криптографічний зв'язок між абстрактним блоком даних і додатковою інформацією (метаданими), наприклад, такий атрибутний контейнер можна асоціювати з електронним документом разом з метаданими при міжсистемному (міжвідомчому) інформаційному обміні. Додатково, використовувана технологія дозволяє (ЕЦП у вигляді CMS або PKCS#7, або «підпис із розширеними даними для перевірки» по ETSI TS 101 733 не може це забезпечити) ввести поняття строку дійсності документа, включаючи механізми екстреного визнання розміщеної в контейнері інформації недійсною. Дана унікальна властивість може бути використана при випуску електронних дозволів, наприклад, імпортно-карантинні дозволи, ліцензії (у тому числі й на програмне забезпечення) і т.п.

Висновок. У статті розглянуто та проаналізовано програмне забезпечення, яке призначено для операційної системи захисту корпоративних додатків, які розробляються за допомогою методології Agile. В межах України в недостатній мірі представлені вітчизняні розробки в цій області. У роботі наведені теоретичне узагальнення й рішення наукового завдання дослідження методів захисту корпоративних додатків, які розробляються за допомогою методології Agile. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем захисту корпоративних додатків, які розробляються за допомогою методології Agile; Досліджена система захисту корпоративних додатків, які розробляються за допомогою методології Agile; На основі отриманих результатів досліджень створена програмна реалізація системи захисту корпоративних додатків, які розробляються за допомогою методології Agile. Розроблені під час виконання роботи алгоритми дозволяють успішно вирішувати завдання захисту корпоративних додатків, які розробляються за допомогою методології Agile. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки. Розроблене програмне забезпечення має простий, дружній та зручний інтерфейс користувача, що забезпечує легкість у освоєнні роботи програмного продукту, зручність у використанні, і не потребує особливих спеціальних знань. При створені програмного забезпечення було використано об'єктно-орієнтований підхід, що відповідає сучасним тенденціям у галузі розробки комерційних програмних систем. Програма реалізована на мові високого рівня Visual C++. Дана мова програмування дозволяє найбільш ефективно обробляти дані. Це дозволило мінімізувати строк розробки програмного забезпечення, і, як слід, зменшити витрати на його розробку. Запропоноване програмне забезпечення ділиться на загальне програмне забезпечення, що поставляється із засобами обчислювальної техніки й спеціальне програмне забезпечення, що спеціально розроблене для даної конкретної системи й включає програми, що реалізують її функції. Для підвищення рівня безпеки запропоновано застосовувати алгоритм ДСТУ 28147:2009. В цілому створене програмне забезпечення підтверджує правильність використаних проектних рішень та повністю відповідає вимогам технічного завдання. Створене програмне забезпечення має потенційну можливість для подальшого вдосконалення і застосування у різних галузях.

Список літератури

1. Майк Кон. Scrum: гибкая разработка ПО = Succeeding with Agile: Software Development Using Scrum (Addison-Wesley Signature Series). – М.: «Вильямс», 2011. – С. 576. – ISBN 978-5-8459-1731-7.
2. Роберт С. Мартин, Джеймс В. Ньюкирк, Роберт С. Косс. Быстрая разработка программ. Принципы, примеры, практика = Agile software development. Principles, Patterns, and Practices. – Вильямс, 2004. – 752 с. – ISBN 0-13-597444-5.
3. James A. Highsmith. Agile Software Development Ecosystems. – Addison-Wesley Professional, 2002. – ISBN 978-0-201-76043-9.
4. В. Столлингс. Криптография и защита сетей: принципы и практика (2-е издание). / Пер. с англ. – М.: Издательский дом «Вильямс», 2001.
5. Баричев С. Г., Гончаров В. В., Серов Р. Е. Основы современной криптографии. – М.: Горячая линия – Телеком, 2001.
6. Смирнов А.А. Системы обнаружения и предотвращения вторжений для защиты компьютерных сетей от вредоносного программного обеспечения / Д.А. Даниленко, А.А. Смирнов, И.Г. Кирилов // Збірник тез доповідей науково-практичної конференції «Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку». м. Харків. 21-22 березня 2012 р. – Харків. АВВ МВС. – 2012. – С. 70-71.
7. Смірнов О.А. Дослідження методів виявлення вторгнень в телекомунікаційні мережі для підвищення інформаційної безпеки // Д.О. Даниленко // Збірник тез науково-практичної конференції «Захист інформації в інформаційно-комунікаційних системах». м. Київ. 24-27 квітня 2012 р. – Київ: НАУ. – 2012. – С. 22-25.
8. Смирнов А.А. Исследование систем обнаружения и предотвращения вторжений для защиты телекоммуникационных сетей от вредоносного программного обеспечения / Д.А. Даниленко // Збірник тез

доповідей VIII наукової конференції «Новітні технології – для захисту повітряного простору». Харків. 18-19 квітня 2012 р. – м. Харків. ХУПС. – 2012. – С. 45.
9. Смирнов А.А. Исследование методов сигнатурного обнаружения вредоносного программного обеспечения в телекоммуникационных системах и сетях // Д.А. Даниленко // Збірник тез XIII міжнародного науково-практичного семінару «Комбінаторні конфігурації та їх застосування». м. Кіровоград. 13-14 квітня 2012 р. – Кіровоград: КНТУ. – 2012. – С. 43-45.
10. Смирнов А.А. Исследование методов проактивной защиты от вредоносного программного обеспечения в телекоммуникационных системах и сетях / Д.А. Даниленко // Збірник тез V міжнародної науково-практичної конференції «інтегровані інтелектуальні робототехнічні комплекси» (ІПРТК-2012). м. Київ. 15-16 травня 2012 р. – Київ: НАУ. – 2012. – С. 314-315.

УДК 657

О. Медведенко, магістр гр. ООУД-18М-1,9
Центральноукраїнський національний технічний університет

НОРМАТИВНА РЕГЛАМЕНТАЦІЯ ВІДОБРАЖЕННЯ В ОБЛІКУ ТА ЗВІТНОСТІ ВИРОБНИЦТВА ПРОДУКЦІЇ ТВАРИННИЦТВА

У статті розглядаються методологічні аспекти та нормативна регламентація обліку виробництва продукції тваринництва. Виокремлено основні об'єкти облікового спостереження виробництва продукції тваринництва та проблемні аспекти відображення їх в обліку та звітності.
тваринництво, витрати на виробництво, біологічні активи, сільськогосподарська продукція, собівартість, оцінка, сільськогосподарське підприємство.

Постановка проблеми та її актуальність. Як правило, метою діяльності будь-якого підприємства є отримання прибутку. У виробництві прибуток отримують за рахунок виробництва та продажу продукції. В аграрній сфері – сільськогосподарської продукції та біологічних активів.

Виробництво продукції тваринництва є одним з основних видів господарської діяльності багатьох аграрних підприємств.

З огляду на значну роль біологічних активів та продукції тваринництва у забезпеченні населення цінними продуктами харчування та виробничого процесу аграрних підприємств, організація їхнього обліку відповідно до потреб управління є важливим напрямом удосконалення облікової системи. Особливої гостроти ця проблема набула після впровадження П(С)БО 30 «Біологічні активи», який змінив традиційні засади організації та ведення бухгалтерського обліку в сільському господарстві і визначив нові вимоги до облікової інформації.

Аналіз останніх досліджень і публікацій. Різні аспекти обліку витрат виробництва й виходу продукції тваринництва досліджували відомі вітчизняні науковці, серед яких Дем'яненко М.Я., Кірейцев Г.Г., Лінник В.Г., Маренич Т.Г., Моссаковський В.Б., Нападовська Л.В., Садовська І.Б., Саблук П.Т. та інші науковці.

Проте організаційні аспекти обліку у тваринництві та їх нормативна регламентація залишаються дискусійними. Потребує удосконалення на практиці методика оцінки поточних біологічних активів та організаційно- методологічні підходи і положення щодо побудови та ведення первинного, зведеного, аналітичного та синтетичного обліку даних активів.

Метою статті є дослідження нормативної регламентації відображення в обліку та звітності виробництва продукції тваринництва та надання пропозицій щодо її вдосконалення.

Виклад основного матеріалу. Функціонування в аграрному секторі різних організаційно-правових форм підприємницької діяльності вимагає нових підходів до

організації бухгалтерського обліку. В аграрному секторі специфічними об'єктами обліку є земля, біологічні активи і біологічні перетворення, сільськогосподарська продукція тощо.

Щоб правильно і раціонально організувати облік виробництва продукції тваринництва, необхідно мати: досконалу законодавчо-нормативну базу; галузеві стандарти і методичні рекомендації з обліку біологічних активів, витрат і доходів та визначення фінансових результатів.

Сільськогосподарські підприємства для обліку витрат на виробництво продукції тваринництва повинні керуватися загальними нормативними документами з бухгалтерського обліку, а саме: Законом про бухгалтерський облік та фінансову звітність в Україні [1], П(С)БО 16 «Витрати» [2], Інструкцією про застосування Плану рахунків бухгалтерського обліку № 291 [3].

Водночас порядок бухгалтерського обліку в сільському господарстві регламентовано П(С)БО 30 «Біологічні активи» [4] та Методичними рекомендаціями з бухгалтерського обліку біологічних активів № 1315 [5], а також Методичними рекомендаціями з планування, обліку і калькулювання собівартості продукції (робіт, послуг) сільськогосподарських підприємств № 132 [6]. Щоправда, керуватися Методичними рекомендаціями № 132 необхідно тільки в частині, що не суперечить П(С)БО.

Специфічні питання обліку, документообігу в галузі тваринництва регламентовано відповідними нормативними документами. У таблиці 1 наведено огляд таких нормативних документів.

Таблиця 1 – Огляд нормативних документів щодо обліку в галузі тваринництва

№ з/п	Нормативний документ	Характеристика
1	П(С) БО 30 [4]	Це основний нормативний документ з бухгалтерського обліку для сільськогосподарських підприємств. У Положенні зазначено, як визнати та оцінити біологічні активи (в тому числі тварин), визначити доходи та витрати сільськогосподарської діяльності, розкрити інформацію про біологічні активи у примітках до фінансової звітності тощо. У додатку до ПБО 30 наведено приклади біологічних активів тваринництва і сільськогосподарської продукції тваринництва
2	Методичні рекомендації № 1315 [5]	Деталізовано норми ПБО 30. Крім того, в додатку 1 до цих Методичних рекомендацій детальніше, ніж в додатку до ПБО 30, наводяться приклади біологічних активів і сільськогосподарської продукції. У додатку 2 до Методичних рекомендацій наведено кореспонденцію рахунків бухгалтерського обліку операцій з біологічними активами та сільськогосподарською продукцією
3	Методичні рекомендації № 132 [6]	Розглянуто питання собівартості продукції (робіт, послуг), у тому числі в тваринництві. У додатку 1 до Методичних рекомендацій наведено об'єкти планування та обліку виробничих витрат, об'єкти калькулювання продукції, одиниці калькулювання. У додатку 2 до Методичних рекомендацій зазначено види побічної продукції (наприклад, гною, вовни, пташиного посліду тощо), одиниці її калькулювання та методику оцінки. Методичні рекомендації слід застосовувати з урахуванням вимог листа № 31-34000-20-5/26023, відповідно до якого окремі норми Методичних рекомендацій не відповідають національним положенням (стандартам) бухгалтерського обліку. У листі також наведено приклади таких невідповідностей
4	Методичні рекомендації № 73 [7]	Наведено форми первинних документів з обліку довгострокових та поточних біологічних активів та рекомендації щодо їх заповнення і застосування

В процесі виробництва продукції тваринництва виникають витрати щодо біологічних

перетворень біологічних активів тваринництва. Так, витрати на виробництво сільськогосподарської продукції, пов'язані з перетвореннями біологічних активів в бухгалтерському обліку визнаються витратами основної діяльності. Нормативне регулювання їх обліку здійснюється відповідно до: НП(С)БО 1, П(С)БО 16, Інструкції про застосування Плану рахунків бухгалтерського обліку активів, зобов'язань і господарських операцій підприємств і організацій, Методичних рекомендацій з планування, обліку і калькулювання собівартості продукції (робіт, послуг) сільськогосподарських підприємств № 132.

НП(С)БО 1 «Загальні вимоги до фінансової звітності» стверджує, що витрати - це зменшення економічних вигод у вигляді вибуття активів або збільшення зобов'язань, які призводять до зменшення власного капіталу (за винятком зменшення капіталу за рахунок його вилучення або розподілу власниками) [8].

Згідно з П(С)БО 16 «Витрати» витратами визнаються або зменшення активів, або збільшення зобов'язань, що приводить до зменшення власного капіталу підприємства (за винятком зменшення капіталу внаслідок його вилучення або розподілу власниками), за умови, що ці витрати будуть достовірно оцінені [2].

Отже в НП(С)БО 1 наводиться визначення поняття «витрати», а в П(С)БО 16 - їх визнання. Проаналізувавши ці визначення, зазначимо, що в НП(С)БО 1 йдеться про «зменшення економічних вигод», тоді як в П(С)БО 16 - про «зменшення активів або збільшення зобов'язань».

Стосовно оцінки біологічних активів тваринництва слід відмітити, що придбаних тварин зараховують на баланс за первісною вартістю, яка визначається стосовно тварин (п. 7 П(С)БО 30 «Біологічні активи»): основного стада відповідно до П(С)БО 7 «Основні засоби»; для вирощування та відгодівлі згідно з П(С)БО 9 «Запаси» [9, 10].

Відповідно до п. 9 П(С)БО 30, додаткові біологічні активи (до яких належить приплід) під час первісного визнання оцінюються за справедливою вартістю, зменшеною на очікувані витрати на місці продажу, або за виробничою собівартістю відповідно до п. 11 П(С)БО 16 «Витрати». Первісне визнання додаткових біологічних активів відображається в тому звітному періоді, у якому вони відокремлені від біологічного активу.

У разі обліку приплоду тварин за собівартістю слід керуватися Методичними рекомендаціями з планування, обліку і калькулювання собівартості продукції (робіт, послуг) сільськогосподарських підприємств № 132 [6].

Для сільськогосподарських підприємств, як і для решти підприємств, діють ті самі правила оформлення первинних документів, що передбачені в Законі України «Про бухгалтерський облік та фінансову звітність в Україні» [1] та Положенні про документальне забезпечення записів у бухгалтерському обліку № 88 [11]. Проте для сільськогосподарської галузі все ж є певні особливості в оформленні первинних документів, які регулюються Методичними рекомендаціями щодо застосування спеціалізованих форм первинних документів з обліку довгострокових та поточних біологічних активів № 73 [7].

Методичні рекомендації № 73 розроблені з метою забезпечення методичних засад формування у бухгалтерському обліку інформації про біологічні активи і про одержані в процесі їх біологічних перетворень додаткові біологічні активи та розкриття інформації про них у фінансовій звітності [7].

Згідно з Планом рахунків та Інструкцією № 291 для обліку витрат та виходу продукції тваринництва передбачено такі рахунки: 16 «Довгострокові біологічні активи (субрахунки 163 «Довгострокові біологічні активи тваринництва, які оцінені за справедливою вартістю» та 164 «Довгострокові біологічні активи тваринництва, які оцінені за первісною вартістю»), рахунок 21 «Поточні біологічні активи» (субрахунки 212 «Поточні біологічні активи тваринництва, які оцінені за справедливою вартістю» та 213 «поточні біологічні активи тваринництва, які оцінені за первісною вартістю») рахунок 23 (аналітичний рахунок «Виробництво продукції тваринництва»), 27 «продукція сільськогосподарського виробництва (за видами продукції тваринництва) [3].

Суттєвою проблемою обліку продукції тваринництва є те, що оцінку біологічних активів слід привести у відповідність з основними положеннями законодавчих актів і нормативних документів, що стосуються бухгалтерського обліку і складання фінансової звітності та усунути розбіжності між ними.

Вимоги П(С)БО 30 «Біологічні активи» щодо оцінювання активів за справедливою вартістю на основі ринкових цін є не зовсім обґрунтованими, тому що певною мірою вони суперечать теоретичним основам бухгалтерського обліку й нормам статті 4 Закону України «Про бухгалтерський облік і фінансову звітність в Україні», згідно з якою для переважної більшості сільськогосподарських підприємств пріоритетним є оцінювання активів, виходячи з витрат на їх виробництво та придбання, тобто принципу історичної (фактичної) собівартості. У той же час, у Концептуальних положеннях Міжнародних стандартів фінансової звітності наголошується на найширшому використанні оцінки за первісною вартістю [12].

При оприбуткуванні на баланс сільськогосподарської продукції за справедливою вартістю та порівнянні її із собівартістю, у підприємства виникає, так би мовити «віртуальний» дохід, який необґрунтований жодними економічними законами та суперечить принципам бухгалтерського обліку і звітності в Україні, а саме: історичної (фактичної) собівартості та обачності.

Більшість сільськогосподарських підприємств сьогодні не дотримуються вимог П(С)БО 30 «Біологічні активи», а саме: не здійснюють оцінку біологічних активів та сільськогосподарської продукції за справедливою вартістю і не визначають доходи (витрати) від первісного визнання біологічних активів та сільськогосподарської продукції. З іншого боку, при дотриманні вимог національного стандарту в результаті визначення фінансового результату сільськогосподарські підприємства включають непідкріплені виручкою доходи у загальну суму чистого прибутку, тобто доходи від «переоцінки» біологічних активів, що призводить до протиріч, які негативно впливають на достовірність відображення інформації у звітності.

Сільськогосподарські підприємства складають Звіт про фінансові результати, виходячи із результатів виробничої діяльності. Згідно П(С)БО 30 «Біологічні активи» на дату балансу такі підприємства повинні оцінювати поточні біологічні активи за справедливою вартістю із списанням різниці між справедливою вартістю і витратами на їх вирощування на витрати або доходи іншої операційної діяльності.

Аналогічно визначають в обліку фінансові результати від первісного визнання сільськогосподарської продукції, що суперечить визначенню основної діяльності, а отже і порядку розрахунку фінансових результатів від основної діяльності. Операції з переоцінки поточних біологічних активів та первісного визнання сільськогосподарської продукції відбуваються за результатами процесу виробництва, а отже повинні формувати фінансовий результат основної діяльності, а не іншої операційної діяльності, як рекомендується відображати згідно П(С)БО 30 «Біологічні активи».

На нашу думку слід відмінити субрахунки 7102 «Дохід від зміни вартості біологічних активів, які обліковуються за справедливою вартістю» та 9402 «Витрати від зміни вартості біологічних активів, які обліковуються за справедливою вартістю», оскільки, як нами було вже зазначено, ніякого доходу чи збитку при застосуванні справедливої вартості до оцінки біологічних активів не виникає. При цьому результати переоцінки пропонуємо відображати на рахунку 42 «Додатковий капітал».

У зв’язку з цим, невідкладного вирішення потребує питання відображення даної інформації у звітності сільськогосподарських підприємств, а саме: у Звіті про фінансові результати, Звіті про власний капітал та Примітках до фінансової звітності.

Нове розкриття інформації про переоцінку біологічних активів пропонуємо формувати у Звіті про фінансові результати, форму якого наведено в таблиці 2.

Таблиця 2 – Запропонований порядок відображення інформації про біологічні активи у Звіті про фінансові результати

Діючий порядок за П(С)БО 30			Запропонований порядок		
Стаття	Код	Інформація, що відображається	Стаття	Код	Інформація, що відображається
1	2	3	4	5	6
Чистий дохід від реалізації продукції (товарів, робіт, послуг)	2000	Виручка від реалізації с/г продукції, поточних та додаткових БА	Чистий дохід від реалізації продукції (товарів, робіт, послуг)	2000	Виручка від реалізації с/г продукції, поточних та додаткових БА
Собівартість реалізованої продукції	2050	Собівартість реалізованої продукції та додаткових біологічних активів	Собівартість реалізованої продукції	2050	Собівартість реалізованої продукції та додаткових біологічних активів
Інші операційні доходи	2120	Дохід від первісного визнання БА і с/г продукції та дохід від зміни вартості БА	Інші операційні доходи	2120	Дохід від первісного визнання БА і с/г продукції
Дохід від первісного визнання БА та с/г продукції	2121	Виділення (із р. 2120) доходу від первісного визнання БА і с/г продукції одержаних внаслідок с/г діяльності	-	-	-
Інші операційні витрати	2180	Витрати від первісного визнання БА і с/г продукції та витрати від зміни вартості БА	Інші операційні витрати	2180	Витрати від первісного визнання БА і с/г продукції
Витрати від первісного визнання БА та с/г продукції	2181	Виділення (із р. 2180) витрат від первісного визнання БА і с/г продукції одержаних внаслідок с/г діяльності	-	-	-
Інші доходи	2240	Доходи від реалізації довгострокових БА, які оцінені за первісною вартістю	Інші доходи	2240	Доходи від реалізації довгострокових БА, які оцінені за первісною вартістю
Інші витрати	2270	Витрати, пов’язані з уцінкою, та собівартість реалізованих довгострокових БА, які оцінені за первісною вартістю, а також витрати, пов’язані з ліквідацією ДБА	Інші витрати	2270	Витрати, пов’язані з уцінкою, та собівартість реалізованих довгострокових БА, які оцінені за первісною вартістю, а також витрати, пов’язані з ліквідацією ДБА

За нової методики переоцінки в статтях 2120 «Інші операційні доходи» та 2180 «Інші операційні витрати» змінюється інформація, яка в них відображається, а статті 2121 «Дохід від первісного визнання біологічних активів та сільськогосподарської продукції» та 2181 «Витрати від первісного визнання біологічних активів та сільськогосподарської продукції»

втрачають свою значимість, тому що інформація, що відображається в них є тотожною інформації, що відображається в статтях 2120 та 2180.

Таким чином сформована доповнена інформація у звіті буде сприяти отриманню достовірної, правдивої інформації щодо біологічних активів на підприємстві, їх вартості та кількості.

Переоцінка біологічних активів може призвести до збільшення чи зменшення додаткового капіталу, що впливає на розмір власного капіталу, тож пропонуємо доповнити структуру Звіту про власний капітал відповідною статтею. Оскільки один з основних принципів звітності є принцип відповідності, то, якщо в балансі буде змінюватись стаття «Додатковий капітал» на відповідну суму, на таку ж суму зміниться власний капітал у Звіті про власний капітал (табл.3).

Таблиця 3 – Запропонований порядок формування інформації про біологічні активи у Звіті про власний капітал

Стаття	Код	Інформація, що відображається
1	2	3
Залишок на початок року	4000	Суми власного капіталу, наведені в балансі підприємства відповідно на початок звітного періоду
Зміна облікової політики	4005	Суми коригувань у зв'язку зі зміною облікової політики
Виправлення суттєвих помилок	4010	Здійснюється коригування сальдо нерозподіленого прибутку (рахунок 44) на початок звітного року
Інші зміни	4090	Мають відображатися всі ті суми коригувань, які мали місце після звітної дати, впливають на розмір власного капіталу та не відображаються у рядках 4005 та 4010
Скоригований залишок	4095	Відображається залишок власного капіталу на початок року після внесення відповідних коригувань
Чистий прибуток (збиток) за звітний період	4100	Сума чистого прибутку (збитку) зі звіту про фінансові результати
Інший сукупний дохід за звітний період	4110	Відображається сума іншого сукупного доходу за звітний період зі Звіту про фінансові результати (рядок 2460 Звіту).
Дооцінка (уцінка) необоротних активів	4111	Додаткова стаття Звіту Сума дооцінки об'єктів основних засобів і нематеріальних активів, зменшена на суму уцінки таких об'єктів протягом звітного періоду в межах сум раніше проведених дооцінок, віднесення сум дооцінки до нерозподіленого прибутку (непокритого збитку)
Дооцінка (уцінка) фінансових інструментів	4112	Додаткова стаття Звіту Сума зміни балансової вартості об'єктів хеджування в порядку, визначеному ПСБО 13
Накопичені курсові різниці	4113	Додаткова стаття Звіту Сума курсових різниць, які відповідно до ПСБО 21 відображаються в складі власного капіталу та визнаються в іншому сукупному доході
Частка іншого сукупного доходу асоційованих і спільних підприємств	4114	Додаткова стаття Звіту Частка іншого сукупного доходу асоційованих, дочірніх або спільних підприємств, облік фінансових інвестицій, який

		ведеться за методом участі в капіталі
Дооцінка (уцінка) біологічних активів	4115	Додаткова стаття Звіту Наводяться дані, які відображають збільшення (зменшення) власного капіталу в результаті переоцінки біологічних активів на певну дату
Інший сукупний дохід	4116	Додаткова стаття Звіту Сума іншого сукупного доходу, для відображення якого за ознаками суттєвості не можна було виділити окрему статтю або який не може бути включений до інших статей

Вважаємо за доцільне у Звіті про власний капітал додати статтю 4115 «Дооцінка (уцінка) біологічних активів», де будуть наводитися дані, які відображають збільшення або зменшення власного капіталу в результаті переоцінки біологічних активів на певну дату.

Разом з тим, пропонуємо залишити оцінку біологічних активів за фактичною собівартістю як можливий альтернативний варіант. Це дозволить бухгалтерам здійснювати оцінку біологічних активів без перекручувань, при виникненні різних ситуацій (наприклад, при відсутності цін на активному ринку або при неможливості їх отримання).

Основна інформація про біологічні активи та сільськогосподарську продукцію слугує для формування Форми 1 «Баланс», Форми 2 «Звіт про фінансові результати» та Форми 4 «Звіт про власний капітал». Досить детальна інформація щодо цих об'єктів обліку відображається і у Примітках до фінансової звітності.

Для відображення інформації про біологічні активи у формі № 5 «Примітки до річної фінансової звітності» призначено два розділи: XIV «Біологічні активи» та XV «Фінансові результати від первісного визнання та реалізації сільськогосподарської продукції та додаткових біологічних активів». Однак вони не надають повної інформації про фінансові результати від сільськогосподарської діяльності відповідно до П(С)БО 30 «Біологічні активи», оскільки не включають показників фінансового результату від зміни справедливої вартості біологічних активів, а також не містять інформації про прибутки (збитки) від вибуття довгострокових біологічних активів, оцінених за первісною вартістю.

Тому доцільно запропоновані зміни у Формі 2 «Звіт про фінансові результати» та Формі 4 «Звіт про власний капітал» обов'язково відображати й у примітках. Це ще раз підтверджує необхідність деталізації обліку за аналітичними рахунками за видами та групами біологічних активів і сільськогосподарського виробництва з орієнтацією на вихід продукції.

Висновки та перспективи подальших досліджень. Узагальнюючи розглянутий матеріал слід відмітити, що специфічні особливості виробництва продукції тваринництва зумовлюють необхідність відповідної організації бухгалтерського обліку. При цьому необхідно мати досконалу законодавчо-нормативну базу, галузеві стандарти і методичні рекомендації з обліку витрат, біологічних активів та сільськогосподарської продукції.

Раціонально організований облік, що враховує вищеназвані чинники, має забезпечити зростання ефективності всієї господарської діяльності шляхом обґрунтованого використання ресурсів, зменшення обсягів непередбачених утрат, збереження та примноження майна власника.

Список літератури

1. Закон України «Про бухгалтерський облік та фінансову звітність в Україні» № 996-XIV від 16 лип. 1999 р. [Електронний ресурс]. - Режим доступу: http://www.rada.gov.ua.
2. 77. Положення (стандарт) бухгалтерського обліку 16 «Витрати», затверджене наказом МФУ від 31.12.99 р. № 318. [Електронний ресурс]. - Режим доступу: http://dtkt.com.ua/show/2bid17066.html

3. Інструкція про застосування Плану рахунків бухгалтерського обліку активів, капіталу, зобов'язань і господарських операцій підприємств і організацій: Наказ Міністерства фінансів України від 30.11.1999 № 291. [Електронний ресурс]. - Режим доступу: http://zakon3.rada.gov.ua..
4. П(С)БО 30 «Біологічні активи» : затверджене наказом Міністерства фінансів України від 18 листопада 2005 р. № 790. [Електронний ресурс]. - Режим доступу: http://www.rada.gov.ua.
5. Методичні рекомендації з бухгалтерського обліку біологічних активів, затверджені наказом МФУ від 29.12.2006 р. № 1315. [Електронний ресурс]. - Режим доступу: http://www.rada.gov.ua.
6. Методичні рекомендації з планування, обліку і калькулювання собівартості продукції (робіт, послуг) сільськогосподарських підприємств, затверджені наказом Мінагрополітики України від 18.05.2001 р. № 132. [Електронний ресурс]. - Режим доступу: http://www.rada.gov.ua.
7. Методичні рекомендації щодо застосування спеціалізованих форм первинних документів з обліку довгострокових та поточних біологічних активів в сільськогосподарських підприємствах, затверджені наказом Мінагрополітики України від 21.02.2008 р. № 73. [Електронний ресурс]. - Режим доступу: http://www.rada.gov.ua.
8. Загальні вимоги до фінансової звітності: НП(С)БО бухгалтерського обліку 1 від 07.02.2013 р. № 73 [Електронний ресурс]. - Режим доступу : http://zakon5.rada.gov.ua/laws/show/z0336-13.
9. Положення (стандарт) бухгалтерського обліку 7 «Основні засоби», затверджене наказом Мінфіну України від 27.04.2000 р. № 92. [Електронний ресурс]. - Режим доступу: http://dtkt.com.ua/show/2bid17066.html
10. Положення (стандарт) бухгалтерського обліку 9 «Запаси»: наказ Міністерства фінансів України від 20. 10. 99 р. № 246. [Електронний ресурс]. - Режим доступу: http://dtkt.com.ua/show/2bid17066.html
11. Положення про документальне забезпечення записів в бухгалтерському обліку, затверджене наказом Мінфіну України від 24.05.95 р. № 88 [Електронний ресурс]. - Режим доступу: - Режим доступу: http://search.ligazakon.ua/l_doc2.nsf/link1/T990996.html
12. Марченко Л.Ю., Придатченко В.В. Оцінювання та облік поточних біологічних активів рослинництва / Марченко Л.Ю., Придатченко В.В. // Економіка і регіон №2 (51), 2015. ПолтНТУ. С. 54-57.

УДК 004

С. Миргородський, магістр гр. КН-18МЗ-1,4
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ ІНФОРМАЦІЙНОГО МОДЕЛЮВАННЯ ЦОД З ВИКОРИСТАННЯМ BIM-ТЕХНОЛОГІ

У статті розроблено програмне забезпечення, яке призначено для системи інформаційного моделювання ЦОД з використанням BIM-технології. Метою розробки є дослідження та програмна реалізація системи інформаційного моделювання ЦОД з використанням BIM-технології. Об’єктом дослідження є процес інформаційного моделювання ЦОД з використанням BIM-технології. Предметом дослідження є методи інформаційного моделювання ЦОД з використанням BIM-технології. Методи дослідження базуються на методах інформаційного моделювання, методах проектування ЦОД, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи інформаційного моделювання ЦОД з використанням BIM-технології. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення. Розроблено зручний інтерфейс користувача. Наведені інструкції по роботі з програмними засобами.
комп’ютерні науки, інформаційне моделювання, ЦОД, BIM-технології

Постановка проблеми. Незважаючи на позитивну динаміку, ринок ЦОД тільки починає відновлюватися. Бум будівництва нових центрів обробки даних залишився в далекому 2008 році. Зараз же обсяг зведення нових об'єктів значно скоротився, через що конкуренція в цьому сегменті ринку різко підсилилася.

Як і колись, одними з основних гравців були й залишаються системні інтегратори. Це обумовлено тим, що ЦОД – унікальний у своєму роді продукт. Його створенням повинна займатися команда фахівців, що володіє всебічними й глибокими знаннями в питаннях

побудови інженерної інфраструктури, а також оснащення об'єктів IT- і телекомунікаційними системами. Зміст подібного кваліфікованого персоналу вимагає серйозних витрат, тому невеликі підприємства найчастіше не здатні вести повноцінну конкурентну боротьбу, а залучити значні інвестиції, необхідні для будівництва центра обробки даних, вдається не всім. Саме тому новачкам досить складно скласти реальну конкуренцію великим компаніям.

Якщо состав ключових гравців не перетерпів серйозних змін, то про запити споживачів цього не скажеш. Незважаючи на тривалий період скороченого фінансування (а в деяких сферах і його повній відсутності), учасники ринку не втрачали часу й продовжували розбиратися в деталях і нюансах будівництва ЦОД. Як наслідок, що течуть запити містять якісно сформовані технічні вимоги до показників об'єктів у цілому, детальний перелік функцій, а також бажану топологію рішення по всіх ключових системах.

Замовники почали пред'являти більше високі вимоги до рівня відказостійкості ЦОД – як правило, не нижче Tier III (по стандартах Uptime Institute). Пильна увага приділяється скороченню капітальних і експлуатаційних витрат. Тепер центр обробки даних споконвічно створюється з розрахунком на певну бізнес-модель, а всі впроваджувані рішення оптимізуються для конкретно поставлених завдань. Щоб адаптуватися до нових вимог, інтеграторам доводиться розширювати спектр пропонованих послуг і підвищувати їхню якість

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи інформаційного моделювання ЦОД з використанням BIM-технологі.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи інформаційного моделювання ЦОД з використанням BIM-технології.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем інформаційного моделювання ЦОД з використанням BIM-технології.

– Дослідження системи інформаційного моделювання ЦОД з використанням BIM-технології.

– Програмна реалізація системи інформаційного моделювання ЦОД з використанням BIM-технології.

Об'єктом дослідження є процес інформаційного моделювання ЦОД з використанням BIM-технології.

Предметом дослідження є методи інформаційного моделювання ЦОД з використанням BIM-технології.

Методи дослідження базуються на методах інформаційного моделювання, методах проектування ЦОД, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. У світі проектування використання комп'ютерної техніки стало звичним. Одержати роздрукований комплект документації часом складніше, ніж створити новий в електронній формі. Завдяки спеціальному програмному забезпеченню – системам автоматизації проектних робіт (САПР), службовцем для перетворення наших ідей у комплект проектної документації, – багато змін у проекті можна реалізувати за лічені годинники. Можна сказати, що основне призначення таких систем – підвищення ефективності дорогої праці експертів і інженерів.

Бонуси, які одержуємо при роботі із САПР:

– створення єдиного інформаційного поля для проектної групи (єдиних шаблонів, стандартів, миттєвий обмін інформацією);

– зменшення числа помилок і доробок при проектуванні і як результат – скорочення строків проектування;

– спрощення планування робіт і контролю результатів, отже, підвищення якості проекту;

– зниження вартості проектування;

– моделювання роботи інженерних систем без створення натурних макетів і моделей;

– скорочення витрат на експлуатацію.

Все це очевидні плюси крокуючої вперед комп'ютеризації в області організації й проведення проектних робіт. У України був прийнятий і діяв ДСТ 23501.101-87 «Системи автоматизованого проектування. Основні положення», що дозволяє впроваджувати САПР у проектних організаціях. Сьогодні в процесі архітектурно-будівельного проектування всі частіше створюється комп'ютерна модель нового будинку, що містить у собі всі відомості про майбутній об'єкт. Система автоматизованого проектування за технологією BIM дозволяє візуалізувати в 3D-форматі будь-які елементи й системи будинку, розраховувати різні варіанти їхнього компонування, а також приводити їх у відповідність із діючими нормами й стандартами, проводити аналіз експлуатаційних характеристик майбутніх будинків, спрощуючи вибір оптимального рішення.

Навіщо потрібна BIM-модель при створенні ЦОДу

Складність і ціна помилок

За рівнем інтеграції інженерної інфраструктури ЦОД як об'єкт будівництва відноситься до групи високотехнологічних і складних. Велика кількість інтегрованих між собою інженерних систем, як правило, погоджується з архітектурним виглядом уже існуючого об'єкта, рідше створюваного знову. У такій ситуації ціна помилок на етапі проектування досить висока: строки збільшуються, вартість росте, нервові клітки руйнуються.

Добре відомий графік залежності витрат на внесення змін у проект від стадії життєвого циклу об'єкта. Чим пізніше виявляємо помилку, тим дорожче вона обходиться. У якийсь момент просто відмовляємося що-небудь міняти, тому що ціна зміни може катастрофічно вплинути на весь проект. Але ж будуємо унікальний об'єкт! Впровадження будь-яких інноваційних ідей може надати нам у майбутньому додаткові переваги на ринку або можливості повернення інвестицій або спростити експлуатацію. Але свідомо відмовляємося від яких-небудь ідей тільки тому, що «час пішов» – аргумент із яким важко сперечатися.

Що ж можна запропонувати для зниження ризиків виникнення такої ситуації або навіть її повного усунення?

Віртуальні моделі об'єктів

Сучасні засоби автоматизації проектування з використанням BIM дозволяють створювати віртуальні моделі об'єкта вже на самих ранніх стадіях проектування. Важливо, що вже на цих етапах маємо можливість побачити, як всі системи погоджуються в єдине ціле. Необхідні дані додаються в модель протягом усього життєвого циклу об'єкта. На кожному етапі їх можна використовувати для бізнес-планування, проектування, організації робіт на різних ділянках проекту, закупівлі матеріалів і організації монтажних робіт, складання, будівництва, передачі в експлуатацію.

При правильному використанні й розвитку BIM-модель об'єкта дозволяє організувати обмін даними між існуючими системами підприємства на кожному етапі життєвого циклу. Наприклад, інформаційна модель може бути постачальником даних для системи закупівель (скажемо, для замовлення встаткування або відновлення комплекту ЗІП), системи календарного планування (для планового обслуговування інженерних систем), системи керування проектами (для візуалізації будівництва ЦОДу), внутрішньої ERP-системи (для планування й розвитку ресурсів).

В BIM-моделі втримуються не просто графічні об'єкти, із цими об'єктами асоційована інформація про їхні властивості, що дозволяє створювати креслення й звіти, аналізувати проект, моделювати графіка виконання робіт, планувати подальшу експлуатацію об'єктів. На кожній стадії проектування інженерній групі надаються можливості для аналізу й вибору найкращого рішення з обліком всіх наявних даних.

Один із ключових моментів – поетапна деталізація BIM-моделі на кожному етапі життєвого циклу об'єкта. Просуваючись від ескізного проекту до робітника в інформаційному полі BIM-моделі, проводимо деталізацію від рівня зв'язаних великих вузлів до рівня замовлених специфікацій конкретного встаткування з відповідною обв'язкою й арматурами.

Аналіз взаємного розташування

Наступний важливий момент – можливість аналізу взаємного розташування всього комплексу інженерного встаткування, у тому числі трубопроводів, кабельних лотків, шинопроводів, розподільних щитів, освітлювальних приладів, стін, сходів, прольотів, стель, фальшполу й т.д. Відомість в обсязі одного приміщення всіх зазначених систем – окреме завдання для проектної команди.

При використанні BIM-моделі відразу одержуємо звіт про можливі перетинання трас або встаткування один з одним. Усунення таких колізій на самих ранніх етапах проектування дозволяє нам одержати комплект дійсно робочої документації, по якій можна будувати об'єкт і монтувати встаткування «точно, як у проекті», а не займатися пошуком обхідного варіанта «по місцю».

Безумовно, такий підхід полегшує й випуск комплекту виконавчої документації. Необхідні зміни в проектній документації можуть бути зроблені практично в режимі реального часу. При використанні мобільного встаткування (наприклад, планшета) можна зрівняти фактично виконаний монтаж на об'єкті із проектним завданням.

Інтеграція із засобами планування

BIM-модель можна інтегрувати із планом будівництва, тобто з календарно-мережним графіком проекту. У такому зв'язуванні BIM-модель дозволяє візуально відобразити ситуацію на об'єкті на будь-який плановий момент часу, що дає можливість аналізувати фактичний хід реалізації проекту в порівнянні із запланованим. Модель також може включати наочну деталізацію вартості проекту або будь-якої іншої обчислювальної характеристики.

Інтеграція 3D BIM-моделі об'єкта із засобами планування (тимчасовими і ресурсними) дає нам четвертий вимір або 4D BIM-модель. Додавши до цього засобу фінансового планування й оцінки вартості на заданий момент часу, одержуємо 5D BIM-модель. Обоє ці розширення надзвичайно корисні при проведенні будівельних і монтажних робіт.

Усіляка користь для експлуатації

Після закінчення будівництва об'єкта ми, як правило, одержуємо «кота в мішку» і стопку виконавчої документації, у якій повинна втримуватися інформація про те, як же в підсумку він побудований. Службі експлуатації, що зароджується на даному етапі має бути створити модель експлуатації, включаючи регламенти, технологічні карти, формуляри, інструкції, списки ЗІП, укласти SLA на обслуговування й ремонт по кожному типу встаткування, створити інформаційну систему керування експлуатацією. Не всі організації готові пройти цей шлях до переможного кінця. У найкращому разі перебуває група універсальних інженерів служби експлуатації, що мають на руках підписані контракти на обслуговування й ремонт найбільш критичних інженерних систем. Є чи альтернатива такої ситуації?

BIM-модель ЦОДу, переданого в експлуатацію, може бути використана для керування об'єктом на всіх подальших етапах його життєвого циклу. Після закінчення будівництва «виконавча документація», оформлена відповідним чином, а саме оновлена BIM-модель, полегшує процес експлуатації, відбиваючи поточний технічний стан систем, даючи чітке подання про відповідальних виробників будь-якого виду робіт і необхідному переліку ЗІП. Інтеграція фінальної BIM-моделі з такими системами, як система керування будинком, система керування ресурсами підприємства, система керування ремонтами й сервісним обслуговуванням, дозволяє нам «в одне торкання» одержати інформаційну систему керування експлуатацією ЦОДу (6D BIM-модель) і тим знизити вартість самої експлуатації.

Безумовно, такий рецепт вимагає впровадження BIM-технології не тільки в організації самого замовника, але у всіх учасників проекту.

Необхідно відзначити, що отримана інформаційна система на базі BIM-моделі буде використовуватися на всіх наступних етапах життєвого циклу ЦОДу: експлуатація й ремонти, модернізація, реконструкція або демонтаж.

Розробка структурної схеми

BIM-технологія (Building Information Modeling, інформаційне моделювання в будівництві) забезпечує ефективне керування даними по будівельному об'єкті, щоб удвічі скоротити проектні строки, детально візуалізувати інтер'єри й екстер'єри у віртуальній реальності, спростити обслуговування готового об'єкта й продовжити строк його служби.

Традиційний підхід до проектування опирається на 2D-моделі – плани, креслення, паперову документацію. BIM-технологія додає нові виміри – плани будівництва, час, вартість – які можуть бути наочно представлені на базі інформаційної моделі об'єкта, будь то житловий або комерційний будинок, дорога, міст або будь-який інший об'єкт.

Застосування BIM для інформаційного моделювання ЦОД

Впровадження BIM для інформаційного моделювання ЦОД спрощує керування будівельним об'єктом протягом усього життєвого циклу – із передпроектної підготовки й аж до заморозки/реконструкції. Познайомтеся з можливостями інформаційного моделювання на кожному етапі існування об'єкта.

Інформаційне моделювання скорочує витрати протягом усього життєвого циклу об'єкта. Сюди входять витрати на керування фінансами, ресурсами, устаткуванням і матеріалами. Накопичені з BIM для інформаційного моделювання ЦОД дані значно спрощують роботу на етапі проектування, будівництва, експлуатації й реконструкцію об'єкта.

Скорочення витрат з BIM для інформаційного моделювання ЦОД

Збереження накопиченої інформації спрощує роботу з об'єктом із самого початку передпроектних робіт. У звичайній ситуації відсутність зв'язку між фахівцями на різних етапах приводить до прискорюваного росту витрат з кожним роком життя об'єкта. BIM для інформаційного моделювання ЦОД забезпечує позитивний ефект за рахунок прискорення комунікації між всіма учасниками робіт, скорочення числа помилок і спрощення їхнього виправлення.

Структура інформаційної моделі

З BIM для інформаційного моделювання ЦОД інформація передається від етапу до етапу протягом усього життєвого циклу об'єкта. Робота в єдиному інформаційному просторі допомагає запобігти більшості колізій, поєднуючи всіх фахівців, що беруть участь, і істотно спрощуючи їхню комунікацію. Інструменти оперативного й стратегічного моніторингу й контролю на кожному етапі допомагають виконати всі роботи в строк.

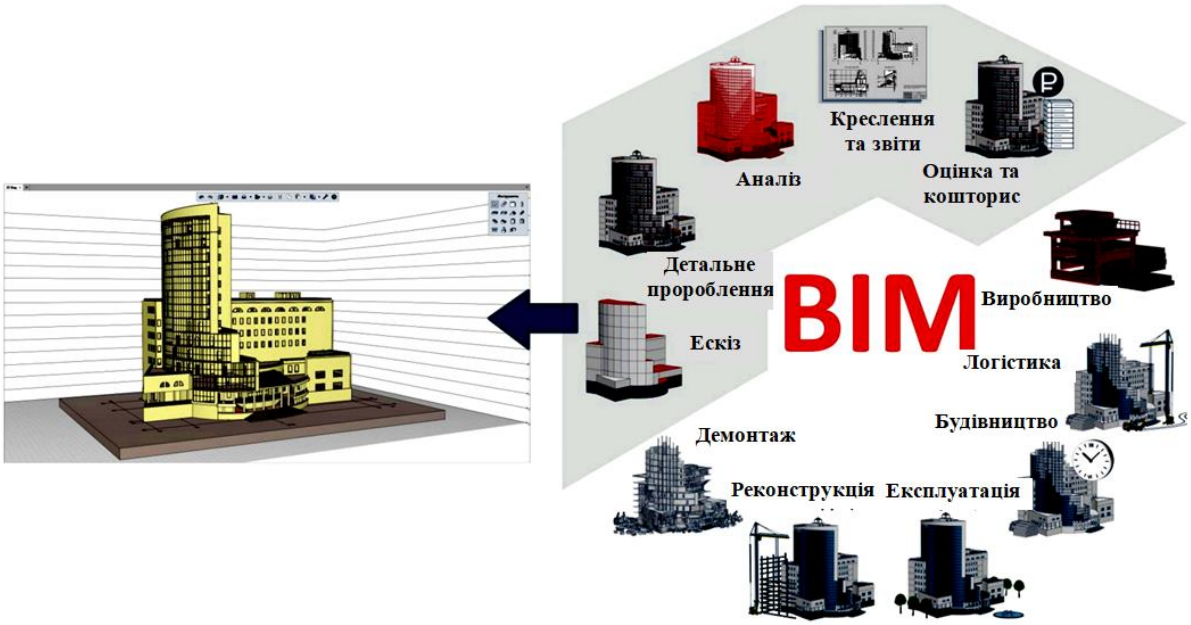


Рисунок 1 – Структурна схема системи

Інтеграція інформації в рамках BIM для інформаційного моделювання ЦОД

Інформаційна модель поєднує дані, з якими щодня працюють учасники проектних команд, будівельники, представники керуючих організацій. Потужний аналітичний інструментарій дозволяє в реальному часі будувати звіти, які налаштовуються, вивантажувати інформацію із запитів регулювальних органів.

Переваги впровадження BIM для інформаційного моделювання ЦОД:

– Керування процесами будівництва в реальному часі, контроль підрядників, відстеження ключових показників і строків у будь-якому потрібному масштабі – від стратегічного до рівня конкретного робітника на тій або іншій ділянці.

– Контроль всіх змін у проекті, оперативне перерахування всіх показників при редагуванні моделі, у тому числі обсяг необхідних матеріалів, працезатрат, строки виконання робіт, бюджет.

– Автоматизоване керування всією будівельною технікою, аж до автоматичного регулювання робочого органа (відвала, ковша й ін.) на основі завантажених у машину проектних даних і практично без участі оператора.

– Інструменти проектування дозволяють на етапі передпроектної підготовки змоделювати різні варіанти створення об'єкта, вибрати оптимальний з них.

– Аналітичний інструментарій дозволяє на всіх етапах одержувати оперативну аналітичну інформацію, забезпечує замовника актуальними даними для стратегічного моніторингу й планування.

– Точний розрахунок витрат на експлуатацію й обслуговування об'єкта на основі зібраної воєдино інформації з різних джерел і даних отриманих з етапу будівництва

– Створення бази всіх підрядників, єдине керування договорами, бухгалтерською документацією програмами розвитку будівництва.

Висновок. У статті розглянуто та проаналізовано програмне забезпечення, яке призначено для системи інформаційного моделювання ЦОД з використанням BIM-технології. В межах України в недостатній мірі представлені вітчизняні розробки в цій області. У роботі наведені теоретичне узагальнення й рішення наукового завдання дослідження методів інформаційного моделювання ЦОД з використанням BIM-технології. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем інформаційного моделювання ЦОД з використанням BIM-технології; Досліджена система інформаційного моделювання ЦОД з використанням BIM-технології; На

основі отриманих результатів досліджень створена програмна реалізація системи інформаційного моделювання ЦОД з використанням BIM-технології. Розроблені під час виконання роботи алгоритми дозволяють успішно вирішувати завдання інформаційного моделювання ЦОД з використанням BIM-технології. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки. Розроблене програмне забезпечення має простий, дружній та зручний інтерфейс користувача, що забезпечує легкість у освоєнні роботи програмного продукту, зручність у використанні, і не потребує особливих спеціальних знань. При створені програмного забезпечення було використано об'єктно-орієнтований підхід, що відповідає сучасним тенденціям у галузі розробки комерційних програмних систем. Програма реалізована на мові високого рівня Builder C++. Дана мова програмування дозволяє найбільш ефективно обробляти дані. Це дозволило мінімізувати строк розробки програмного забезпечення, і, як слід, зменшити витрати на його розробку. Запропоноване програмне забезпечення ділиться на загальне програмне забезпечення, що поставляється із засобами обчислювальної техніки й спеціальне програмне забезпечення, що спеціально розроблене для даної конкретної системи й включає програми, що реалізують її функції. Для підвищення рівня безпеки запропоновано застосовувати алгоритм DSA.

Список літератури

1. Смирнов А.А. Разработка методики оценки среднего времени обслуживания информационных пакетов в телекоммуникационной сети / А.А.Смирнов, В.В.Босько, Е.В.Мелешко // Системи управління, навігації та зв'язку. – Київ: ДП «Центральний науково-дослідний інститут навігації і управління», 2009. – Вип. 2(10). – С.162-165.
2. Смирнов А.А. Анализ и сравнительное исследование перспективных направлений развития цифровых телекоммуникационных систем и сетей / А.А.Смирнов, В.В.Босько, Е.В.Мелешко // Системи обробки інформації. – Х.: ХУ ПС, 2008. – Вип.7(74). – С.120-123.
3. Смирнов А.А. Усовершенствование метода управления очередями в многопротокольных узлах телекоммуникационной сети / А.А.Смирнов, Е.В.Мелешко // Збірник тез та доповідей другої всеукраїнської науково-практичної конференції «Системний аналіз. Інформатика. Управління». Запоріжжя. Тези доповідей. Запоріжжя: КПУ, 2011. – 193-195 с.
4. Современные телекоммуникации. Технологии и экономика / [В.Л. Банкет, О.В. Бондаренко, П.П. Воробьенко и др.]; под ред. С.А. Довгого. – М.: Эко-Трендз, 2003. – 320 с.
5. Столлингс В. Современные компьютерные сети / Вильям Столлингс.– СПб.: Питер, 2003. – 778 с.
6. Сэломон Д. Сжатие данных, изображений и звука / Д. Сэломон. – М.: Техносфера, 2004. – 368 с.
7. Таненбаум Э. Компьютерные сети / Эндрю Таненбаум; пер. с англ. А. Леонтьев. – СПб.: Питер, 2002. – 848 с.
8. Телекоммуникационные системы и сети: учебное пособие. В 3 томах / [В.В. Величко, Е.А. Субботин, В.П. Шувалов, А.Ф. Ярославцев]; под ред. В.П. Шувалова. – М.: Горячая линия-Телеком, 2005, т. 3 – 592 с.
9. Уолрэнд Дж. Телекоммуникационные и компьютерные сети / Дж. Уолрэнд. – М.: Постмаркет, 2001. – 480 с.
10. Хайкин С. Нейронные сети: полный курс / С. Хайкин. – М.:Вильямс, 2006. – 1103 с.
11. Хаусли Т. Системы передачи и телеобработки данных: пер. с англ. / Т. Хаусли; под ред. Ю.М. Мартынова. – М.: Радио и связь, 1994. – 452 с.

УДК 004

Д. Мошуренко, магістр гр. КІ-18М-1,4
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ ОПЕРАЦІЙНОЇ СИСТЕМИ РОБОТИЗОВАНИХ КОМПЛЕКСІВ

У статті розроблено програмне забезпечення, яке призначено для операційної системи роботизованих комплексів. Метою розробки є дослідження та програмна реалізація операційної системи роботизованих комплексів. Об'єктом дослідження є процес створення операційної системи роботизованих комплексів. Предметом дослідження є методи створення операційної системи роботизованих комплексів. Методи дослідження базуються на методах створення операційної системи, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація операційної системи роботизованих комплексів. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.
комп'ютерна інженерія, операційна система, роботизований комплекс

Постановка проблеми. Промислові роботи або ПР все більше застосовуються на виробництві, а саме в галузі машинобудування. Так як в наш час виробництво все більше удосконалюється, використання ПР стає складовою частиною автоматизованого виробництва.

Промисловий робот є частиною роботизированого технологічного комплексу або РТК. Застосування промислових роботів значно спрощує процес виробництва. З часу своєї появи, від перших промислових роботів і до нинішніх розумних машин, ПР одразу ж отримали повагу і затребуваність з боку машинобудівних підприємств, і на сьогодні не можна уявити собі повноцінне автоматизоване виробництво без цієї дуже важливої складової частини.

На сьогодні не існує мови управління механізмами, який не залежав би від специфіки конкретної галузі машинобудування і технічно-апаратних рішень, які були реалізовані для створення конкретного механізму або технологічної лінії. Так, кожне підприємство, яке займається розробкою і впровадженням роботизованих комплексів і технологічних ліній, надає систему управління, алгоритм виконання технологічних тактів в які в загальному випадку можуть задаватися не мовою управління, а іншими засобами, наприклад, мати табличне представлення кроків технологічного такту і параметрів руху.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні операційної системи роботизованих комплексів.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація операційної системи роботизованих комплексів.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем створення операційної системи роботизованих комплексів.
– Дослідження операційної системи роботизованих комплексів.
– Програмна реалізація операційної системи роботизованих комплексів.

Об'єктом дослідження є процес створення операційної системи роботизованих комплексів.

Предметом дослідження є методи створення операційної системи роботизованих комплексів.

Методи дослідження базуються на методах створення операційної системи, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Датчики роботизованих систем

Сенсорні системи

Сенсорні системи призначені для отримання інформації про зовнішнє середовище і положення робота в ній. У окремих системах роботів є також різні чутливі пристрої – датчики, необхідні для функціонування цих систем (наприклад, датчики зворотного зв'язку в приводах, у вторинних джерелах живлення і тому подібне). Ці пристрої, орієнтовані на внутрішні параметри робота, не специфічні для нього в цілому і не відносяться до сенсорних систем робота. Але властивостям, що виявляються, і параметрам сенсорні системи можна розділити на наступні 3 групи:

– системи, що дають загальну картину довкілля з подальшим виділенням окремих об'єктів, значимих для виконання роботом його функцій;

– системи, що визначають різні фізико-хімічні властивості зовнішнього середовища і її об'єктів;

– системи, що визначають координати місця розташування робота і параметри його руху, включаючи його координати відносно об'єктів зовнішнього середовища і зусилля взаємодії з ними.

До сенсорних систем першої групи відносяться системи технічного зору і різного типу локатори. Друга група сенсорних систем найбільш різноманітна. Це вимірники геометричних параметрів, щільності, температури, оптичних властивостей, хімічного складу і так далі. Третя група сенсорних систем визначає параметри, що відносяться до самого робота. Це вимірники його географічних координат в просторі від супутникових систем до тих, що використовують магнітне поле Землі, вимірників кутових координат (гіроскопи), вимірників переміщення і швидкості, у тому числі і відносно окремих об'єктів зовнішнього середовища аж до фіксації зіткнення з ними. У складі робота усі ці сенсорні системи орієнтовані на обслуговування двох систем – пересування і маніпуляції. Це визначає і основні вимоги до сенсорних систем – дальність дії, точність, швидкодія і так далі. Сенсорні системи, використовувані в системах пересування робота, підрозділяються на системи, що забезпечують навігацію в просторі і системи, що забезпечують безпеку руху (відвертання зіткнень з перешкодами і перекидань на ухилах, попадання в неприпустимі для робота зовнішні умови і тому подібне).

Сенсорні системи, обслуговуючі маніпулятори, теж утворюють дві підгрупи: системи, що входять в контур управління рухом маніпулятора, і системи, яка контролюэ дії його робочого органу. До числа останніх систем часто входять розміщені у робочого органу маніпулятора системи технічного зору і вимірники зусиль. Важливим параметром сенсорних систем є дальність дії. За цим показником сенсорні системи роботів можна розділити на контактні, ближньої, далекої і наддалекої дії. Контактні сенсорні системи застосовуються для контролю дій робочих органів маніпуляторів і корпусу (бампера) мобільних роботів. Вони дозволяють фіксувати контакт з об'єктами зовнішнього середовища (тактильні сенсори), вимірювати зусилля, що виникають в місці взаємодії (силомоментні сенсори), визначати прослизання об'єктів при їх утриманні захватним пристроєм. Контактним сенсорним системам властива простота, але вони накладають істотні обмеження на динаміку і передусім на швидкодію управління роботом. Тактильні сенсори окрім отримання інформації про контакт застосовуються і для визначення розмірів об'єктів (шляхом їх обмацування).

Вони реалізуються за допомогою кінцевих вимикачів, герметизованих магнітоуправляємих контактів, на основі струмопровідної гуми ("штучна шкіра") і так далі. Важливою вимогою, що пред'являється до цих пристроїв, є висока чутливість (спрацьовування при зусиллі в одиниці і десятки грам), малі габарити, висока механічна міцність і надійність.

Сенсорні системи ближньої дії забезпечують отримання інформації про об'єкти, розташовані у безпосередній близькості від робочого органу маніпулятора або корпусу

робота, тобто на відстанях, сумірних з їх розмірами. До таких систем відносяться оптичні локатори, далекоміри, дистанційні вимірники щільності грунту і тому подібне. Такі безконтактні пристрої технічно складніше за контактних, але дозволяють роботові виконувати завдання з більшою швидкістю і заздалегідь видавати інформацію про різні об'єкти до зіткнення з ними.

Сенсорні системи далекої дії служать для отримання інформації про зовнішнє середовище в об'ємі усієї робочої зони маніпуляторів роботів і довкілля мобільного робота. Сенсорні системи наддалекої дії застосовуються головним чином в мобільних роботах. До них відносяться різні навігаційні системи, локатори і інші сенсорні системи відповідної дальності дії. Ці пристрої знаходять застосування і в стаціонарних роботах при роботі з рухливими об'єктами, щоб заздалегідь передбачати їх появу в робочій зоні. У безконтактних сенсорних системах для отримання необхідної інформації використовуються випромінювані ними спеціальні сигнали (оптичні, радіотехнічні, ультразвукові і так далі) і природні випромінювання середовища і її об'єктів. Залежно від цього розрізняють активні і пасивні сенсорні системи.

Активні сенсорні системи мають передавач, випромінюючий первинний сигнал, і приймач, що реєструє минулий через середовище прямий сигнал або вторинний сигнал, відбитий від об'єктів середовища. Пасивні системи мають, природньо, тільки приймальний пристрій, а роль випромінювача грають самі об'єкти зовнішнього середовища. Тому пасивні сенсорні системи зазвичай технічно простіше і дешевше за активних, але менш універсальні. Для деяких застосувань важлива також скритність дії пасивних систем. Помітимо, що усі органи чуття людини є пасивними. Проте у деяких тварин (кажани, дельфіни), оскільки подібні системи і, передусім, зір не забезпечують їх необхідною інформацією, існують і активні сенсорні системи. Нарешті, сенсорні системи роботів можна розділити на системи з фіксованим напрямом сприйняття і зі змінним (скануючі). Нині для очувствленния роботів найбільш широке застосування отримали системи технічного зору, локаційні, силомоментні і тактильні.

Датчики роботів і їх інтерфейси

Датчики зіткнень і нахилу

Як правило, датчик зіткнень є вимикачем, що подає інформацію логічного типу. Вимикач може знаходитися в одному з двох положень – розімкненому або замкнутому. Може здатися, що цю інформацію легко перетворити для використання в програмі. У фізичному сенсі датчики зіткнень є вимикачами кінцевого типу, або кнопками. Вони використовуються як бампери мобільних роботів на колесах, а також для зупинки обертання осі, що прийшла в положення зіткнення з обмежувальним упором. На рисунку 3.1 представлені схеми інтерфейсу для датчиків такого типу.

Як правило, в стані спокою вимикач знаходиться в розімкненому положенні, але це необов'язково. Важливим є те, що, коли датчик знаходиться в стані спокою, в центр управління подається верхній рівень напруги, визначуваний резистором навантаження. Це необхідно з двох причин. Перша полягає в споживаному струмі, оскільки передбачається використання датчика тільки в певні моменти, а друга – в тому, що резистор частенько встановлюється на платі управління, поблизу фізичних входів процесора.

У цих датчиків є серйозний недолік: контакт не замикається відразу. З'являється ефект брязкоту контакту, який може бути неправильно інтерпретований центром управління. Вирішення цієї проблеми полягає у введенні в програму досить тривалої затримки, що перекриває інтервал часу брязкоту контакту, між двома інтервалами часу читання цих входів. Таке рішення використовується в програмах, що мають вузол реального часу. Датчики нахилу призначені для використання на пересіченій місцевості, але не просто знайти модель, що вказує нахил з великою точністю до двох градусів нахилу і більше.

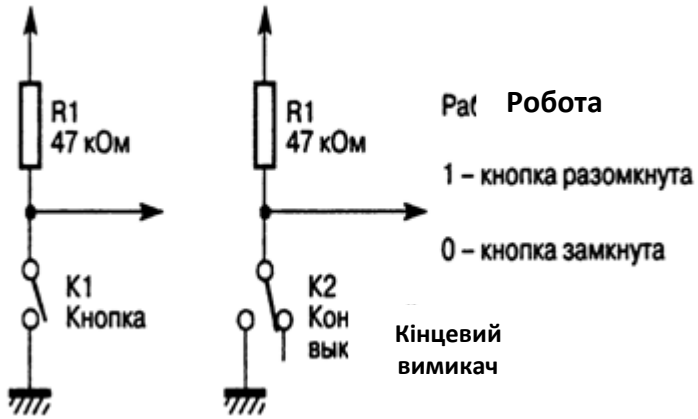


Рисунок 1 – Інтерфейс для датчика зіткнень

Положення датчика дуже важливе щоб уникнути отримання неправдивої інформації. Щонайменше прискорення робота викликає спрацьовування датчиків. Необхідно встановити декілька датчиків для перевірки істинності отриманої інформації і дочекатися зупинки робота для прочитання їх значення. Інтерфейси датчиків нахилу ідентичні інтерфейсам, призначеним для датчиків зіткнень.

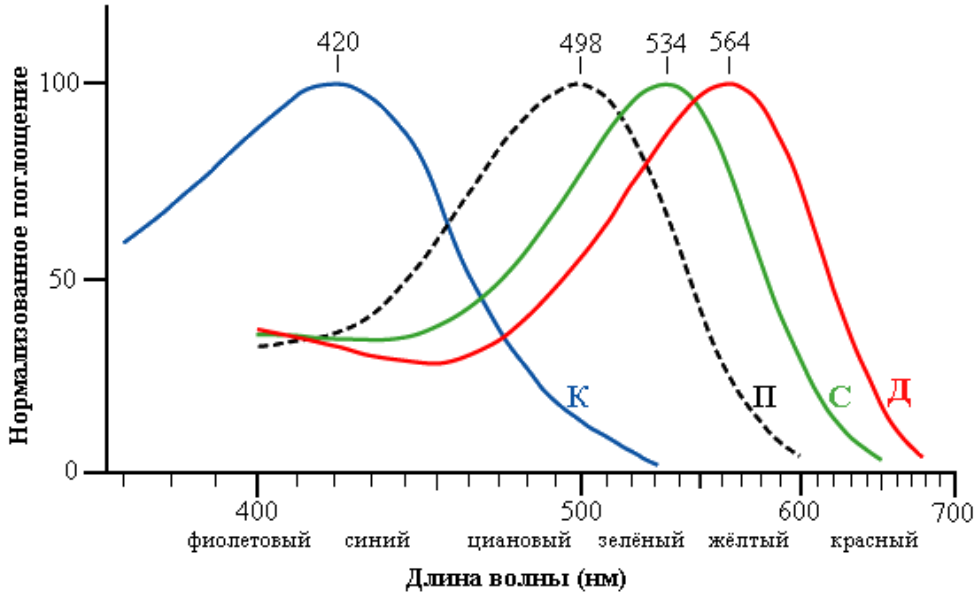


Рисунок 2 – Довжина хвиль оптичного спектру випромінювання

Оптичні датчики

Оптичні датчики включають фоторезистори, фототранзистори, фотодіоди, піроелектричні датчики і відеокамери. Вибір того або іншого типу залежить від таких параметрів, як довжина хвилі оптичного спектру випромінювання або швидкість прочитування свідчень датчика. Завдовжки хвилі визначається колір джерела світла, яке може мінятися від ультрафіолетового до інфрачервоного, проходячи через видиму область спектру. На рисунку 2 показані області відомих джерел світла.

Час спрацьовування є важливим чинником часу розрахунку для підтвердження інформації. Фотодіоди і фототранзистори є найшвидшими, а фоторезистори і відеокамери – повільнішими. Ці датчики можуть оснащуватися як простими електронними інтерфейсами подібно до датчиків зіткнень, так і складними інтерфейсами, необхідними, наприклад, для відеокамери. Дані, що отримуються від датчика, можуть бути аналоговими або цифровими залежно від вибраного інтерфейсу. Для поліпшення чутливості при конкретному застосуванні може знадобитися додаткове джерело світла. Наприклад, кодована ІЧ-звістка

інформує робот-пилосос про місцезнаходження роз'єму для зарядки батареї. Фоторезистор є напівпровідниковим резистором, опір якого залежить від освітленості, при зменшенні якої його опір збільшується. Дуже просто виготовити інтерфейс для цього компонента з аналоговим входом для підключення плати управління. Досить всього одного резистора у парі з фоторезистором. За допомогою резистора ми створюємо дільник напруги, вихідне значення якогозалежить від освітлення(рис.3).

Цей датчик дуже чутливий до видимого світла, відповідно, ця інформація може бути дуже корисна для управління роботом. Подібно до людини датчик має бути здатний розрізняти градації світла: темряву, затемнені зони і зміни яскравості світла. ІЧ-датчиками є фототранзистори або фотодіоди.

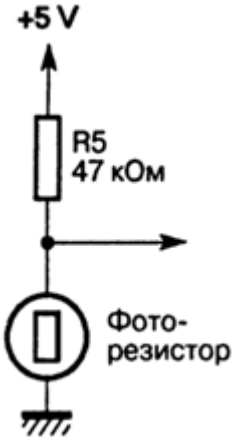


Рисунок 3 – Інтерфейс для фоторезистора

Фототранзистор і фотодіод мають максимальне покриття ІЧ-області спектру, але їх також можна застосовувати і в червоній області спектру. Фотодіод має швидший час спрацьовування, ніж фототранзистор. Фотодіоду віддають перевагу, коли потрібне виявлення кодованого повідомлення, наприклад, при прийомі сигналів пультом дистанційного керування телевізора. Але для посилення прийнятого сигналу потрібний інтерфейс, і, відповідно, фотодіод не може підключатися безпосередньо до плати управління. Фототранзистор використовується як заміна фоторезистора для виявлення швидких перепадів освітленості навколишнього простору. Як і фоторезистор, фототранзистор підключається безпосередньо до плати управління за допомогою простого інтерфейсу (рис. 4).

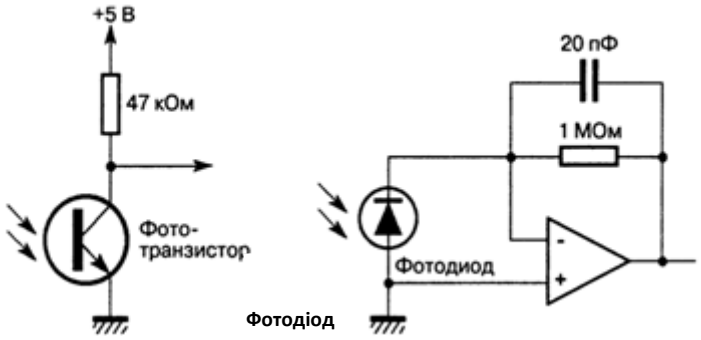


Рисунок 4 – Інтерфейс для фототранзисторів та фотодіодів

Фототранзистори часто використовуються спільно з випромінювачем фотонів – джерелом світла, наприклад світлодіодом (французьке позначення – Del, англійське позначення – Led). Ці спільно працюючі компоненти називаються оптопарою і залежно від орієнтації можуть утворювати датчик відображення або оптокомутатор. Схема включення незмінна для обох типів датчиків (рис. 5).

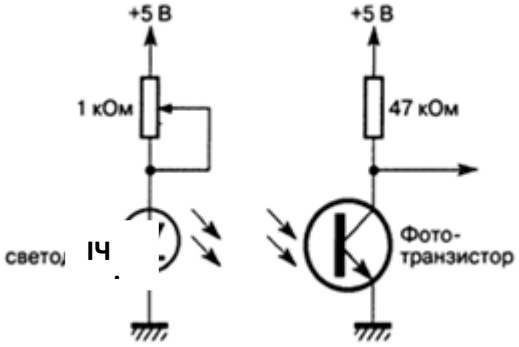


Рисунок 5 – Інтерфейс для датчика відображення та оптокомутатора

Для зведення до мінімуму впливу навколишнього світла на датчик використовується ІЧ-модель світлодіода. Світлодіод налаштовується на оптимальне значення світлового випромінювання за допомогою змінного резистора, яким регулюється кількість випромінюваних фотонів. Це дозволяє уникнути насичення приймача, в результаті якого приймач стає непридатним для використання. Опір навантаження фототранзистора залежить від моделі. Оптимальне значення опору підбирається дослідним шляхом. Датчик відображення використовується для виявлення градацій монохромного (чорно-білого) кольору на плоскій поверхні. Темна поверхня поглинає фотони, що випромінюють, і транзистор залишається в закритому стані. Світла поверхня відбиває світло у напрямі фототранзистора, внаслідок чого відбувається його насичення – транзистор переходить в інший, відкритий, стан. Так само можливе виявлення і інших кольорів, наприклад зеленого. Оптимальна відстань виявлення складає близько 5 мм При зміні цієї відстані характеристики датчику значно погіршуються.

Детектори наближення Дуже корисно уміти ухилятися від зіткнення з нерухомим або мобільним перешкодами. Зіткнення може привести до несподіваних наслідків. Це уміння – дуже цінна перевага робота. Для виявлення перешкод, розташованих на невеликій відстані, можна використати випромінюючий ІЧ-світлодіод з невеликим фотоприймачем. В сукупності компоненти називають оптопарою. Використовуваний принцип виявлення перешкоди близький до принципу роботи датчика відображення, але з одним удосконаленням. ІЧ-випромінювання має бути не безперервним, а імпульсним, що дозволить виключити паразитні ІЧ-випромінювання (сонячне світло, джерело тепла). За наявності перешкоди перед роботом випромінювання відбивається і приймається приймачем. Але ефективність цієї системи залежить від потужності випромінювання, кута відображення, походження і кольору перешкоди. Імпульсне випромінювання модулює хвилю, яка іде, на частоті 40 кГц. Ця частота є стандартною частотою усіх комунікаційних систем, які використовують ІЧ-випромінювання (пульти дистанційного управління телевізорами та інші прилади0. Сигнал, який випромінюється, приймається спеціальним приймальним модулем, який включає фотодіод, підсилювач і демодулятор, працюючий на частоті 40 кГц.

Модуль після демодуляції перетворить її в цифрову форму і в рівнях, безпосередньо сумісних з рівнями сигналів на входах плати управління. Для забезпечення достовірності інформації необхідно, щоб тривалість випромінювання складала приблизно 1 мс, а між випромінюваннями витримувалася пауза тривалістю 1 мс. Під час випромінювання виконується читання приймача, наявність перешкоди підтверджується відсутністю сигналу приймача за відсутності випромінювання. Вказані проміжки можуть бути скорочені при випробуваннях в конкретній ситуації. Схема датчика представлена на рисунку 6.

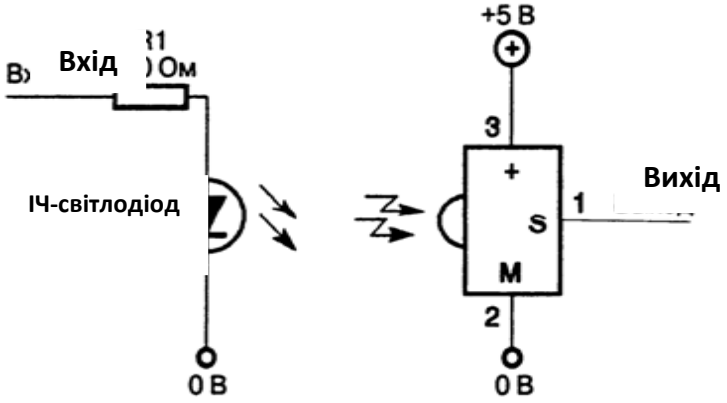


Рисунок 6 – Схема детектора зближення

Для збільшення або зменшення відстані виявлення можна змінити номінал резистора. Функція виміру відстані забезпечує перевірку положення робота, розрахованого іншими способами. Довгий час вимір відстані був прерогативою ультразвукових систем із-за відносно невеликої вартості в порівнянні з лазерними телеметричними датчиками. Ситуація змінилася після розробки технологічних телеметричних ІЧ-датчиків. Вони забезпечують досить точно вимір відстаней в межах від 10 до 80 см за допомогою інфрачервоного випромінювання. Для розрахунку відстані або наявності об'єкту в полі зору ці датчики використовують тріангуляцію спільно з мережею фотодіодів. Ідея полягає у випромінюванні коротких і потужних ІЧ-імпульсів, які відбиваються об'єктом або втрачаються, якщо не потрапили в поле його зору. У разі відображення на детектор поступає промінь в точці, що утворює трикутник з точкою випромінювання і виявленим об'єктом (рис. 7).

Кут відображення в трикутнику міняється залежно від відстані до виявленого об'єкту. Точність датчика підвищується лінзою детектора. Фазочутливий детектор положення визначає кут відображення і розраховує відстань до об'єкту. Цей засіб дозволяє виключити вплив навколишнього освітлення, а також кольори виявленого об'єкту. Відповідно, можливо виявити чорну стіну при повному освітленні приміщення.

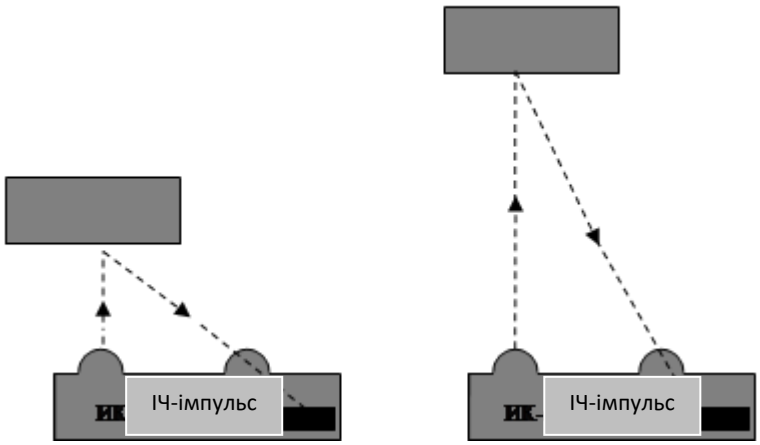


Рисунок 7 – Принцип роботи телеметричних ІЧ-датчиків

Піроелектричні датчики

Піроелектричні датчики здатні виявляти тепло, витікаюче від людського тіла або від вогню. Насправді, живі істоти – люди або теплокровні тварини – випромінюють інфрачервоне випромінювання (у діапазоні від 8 до 10 мкм), яке може бути виявлене піроелектричними датчиками. Ця особливість використовується для виявлення несанкціонованого руху людини в системах тривожної сигналізації. Піроелектричні датчики іншого типу використовуються для виявлення займання і подання сигналу спрацьовування

на систему пожежної сигналізації. Датчики останнього типу є УФ-датчики, чутливі до випромінювань, витікаючих від вогню (від 185 до 260 нм).

Звукові датчики

Предмети, що оточують нас, можуть передавати корисні звуки, якими навіть лікують хворих або проводять релаксацію працівників, схильних до стресу. Але вони можуть видавати і шкідливі звуки, які називають джерелами звукових "забруднень". Чим вище частота звуку, тим з більшою точністю можна визначити напрям на нього. Звуки поширюються із швидкістю 320 м/с, якщо їх вимірювати на рівні моря при температурі 25 °С. За інших умов швидкість може відрізнятися від приведеної. Звуки використовуються різними способами. З їх допомогою можна спілкуватися з роботом або виявляти перешкоди, на яких звуки утворюють луну. Датчик детектування звуків є класичним мікрофоном, сигнал якого посилюється до певного рівня. Декодування звукової команди для виконання роботом може зажадати значних ресурсів, якщо йдеться про розпізнавання звуків людського голосу. Але якщо для спілкування з роботом задовольнятися вибором однієї певної частоти, положення справ значно спрощується.

У цьому полягає причина успіху невеликих роботів, які реагують на такі прості однотонні звуки, як ляскання в долоні або свист. В даному випадку, як правило, використовується два електронні пристрої: частотний детектор, якийвибирає з множини одну певну частоту, і перетворювач "частота-напруга", що генерує напругу, пропорційну частоті, що поступає на його вхід.

Схема, показана на рисунку 8, є однією з можливих реалізацій перетворювача частоти в напругу. Пристрій працює за наступним принципом: сигнал, що виробляється мікрофоном, посилюється інтегральною схемою LM386. Вона є підсилювачем звукових частот визначуваних джерелом живлення +5 В, працюючий в діапазоні низької напруги. Інтегральна схема LM2917 -- це перетворювач частота-напруга.

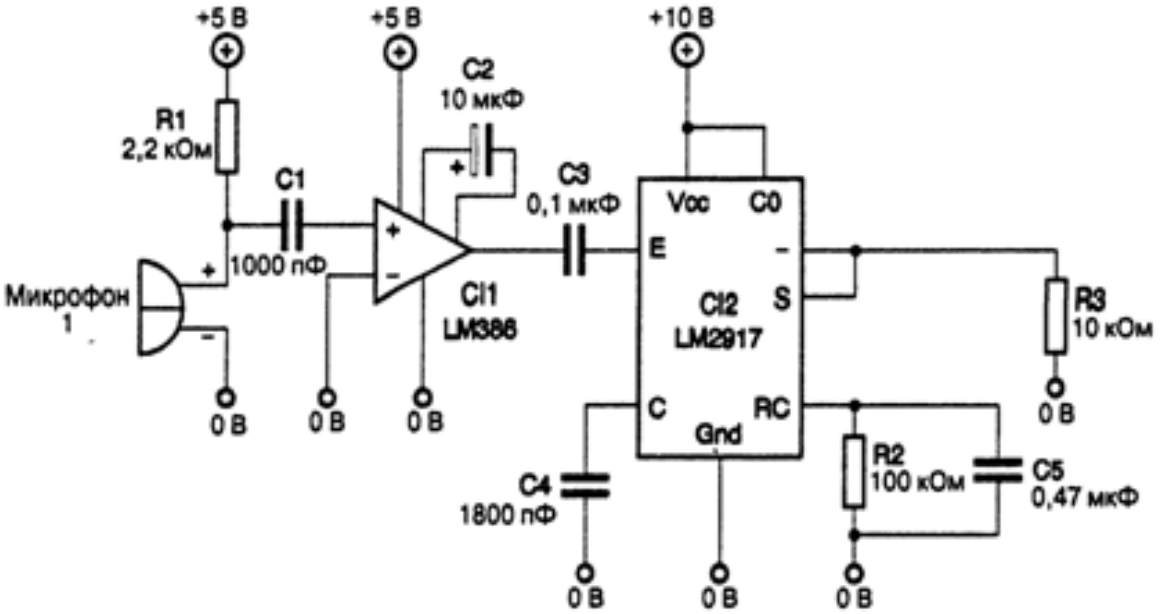


Рисунок 8 – Схема перетворення частоти у напругу

Ультразвукові частоти лежать вище за діапазон звукових частот і мають вузьку спрямованість. Ця властивість ультразвукових сигналів дозволила використати їх для виміру відстаней від декількох сантиметрів до 11 м. Ультразвукова система виміру відстані випромінює спектр частот в смузі частот 40 кГц, а потім вимірює час повернення (відгуку) відбитого сигналу. Оскільки сигнал, що випромінює, пройшов відстань від джерела до перешкоди двічі, виміряний час має бути розділений на два. Для отримання відстані залишається помножити отриманий результат на швидкість звуку. Теоретично виміряти

відстань за допомогою ультразвуку може здатися простим завданням, але на практиці виникають проблеми з правильним прийомом відбитого сигналу.

Перша проблема – паразитна взаємодія передавача і приймача, коли частина сигналу передавача "просочується" на вхід свого ж приймача, внаслідок чого через декілька секунд після випромінювання імпульсу генерується неправдива луна. По-друге, амплітуда відбитого сигналу зменшується пропорційно пройденій відстані. Першою рішення цих проблем запропонувала компанія Polaroid, яка вже 20 років тому винайшла миттєвий фотоапарат зі вбудованою системою роздруку знімків. Polaroid розв'язала проблему, змінюючи коефіцієнт посилення залежно від часу (мінімальний коефіцієнт посилення на початку збільшується із закінченням часу), і блокуючи впродовж декількох мілісекунд будь-який прийнятий відбитий сигнал.

Датчики положення

Знання положення для вибору напряму руху – це одна з проблем для орієнтації робота. Точне знання свого положення і орієнтація відносно відправної точки є непростим завданням, яке вимагає залучення значних математичних ресурсів. Але не завжди вимагається знати точне положення. Для деяких роботів досить простої вказівки для орієнтації напряму їх руху. Для визначення свого місця розташування робот може скористатися декількома засобами. Використовувана інформація буває абсолютною або відносною. Система глобального позиціонування (GPS – Global Position System) дозволяє визначити місце розташування будь-якого мобільного (сухопутного або водного) транспортного засобу на земній кулі з точністю, достатньою для нього, але недостатньою для робота, встановленого на підприємстві. Рішення полягає в установці нерухомих маяків на маршруті руху робота для передачі йому необхідній інформації.

Для підвищення точності визначення місця розташування в якості можливого додаткового навігаційного маяка можна використати електроний компас, але магнітні поля двигунів часто знижують достовірність його роботи. В деяких випадках досить знати кут обертання відносно осі. Робот-пилосос, спрямовуючись до роз'єму зарядного пристрою, задовольняється зміною кута обертання відносно джерела світла, встановленого в пристрої. Орієнтири виконують для роботів ту ж роль, що і маяки для морських суден. Вони можуть вказувати на перешкоди, від яких слід відхилитися, або передавати іншу потрібну роботові інформацію. У випадку з роботами маяк може бути пасивним або активним. Прості пасивні маяки є відбиваючою стрічкою, а найскладніші – штрих-коди. Вони можуть передавати просту або складнішу інформацію. Таким чином, декілька маяків, встановлених на маршруті руху робота, передають йому інформаційні повідомлення про відносне або абсолютне положення.

Активні маяки дають можливість проводити виміру на базі сигналів різних діапазонів частот. Для спілкування з роботом використовуються інфрачервоні, ультразвукові або звукові сигнали. Ультразвукові сигнали забезпечують можливість виміру відстаней або курсових кутів між маяками і роботом. Завдання робота полягає в ідентифікації цих маяків. ІЧ-сигнали дозволяють кодувати випромінювання для розрізнення маяків. Звукові сигнали здатні при необхідності замінити ультразвукові сигнали. Перший варіант взаємодії сигналів різних частот – маяки передають кодовані ІЧ-сигнали, які робот отримує, спрямовуючись до них. Другий варіант взаємодії – робот випромінює ІЧ-промінь, що активує маяки. У свою чергу, маяки випромінюють спектр ультразвукових сигналів, вимірюваний роботом.

Ще один вид датчиків положення – гіроскопи є датчиками, що дозволяють вимірювати кут обертання робота відносно вибраної осі. Гіроскоп призначений для двох наступних вимірів: кута повороту робота або його кутової швидкості. Він є датчиком кутової швидкості, грунтованим на явищі кориолісових сил. Це явище виникає в результаті передачі на гіроскоп певної кутової швидкості обертання.

На рис. 9 представлений принцип роботи датчика.

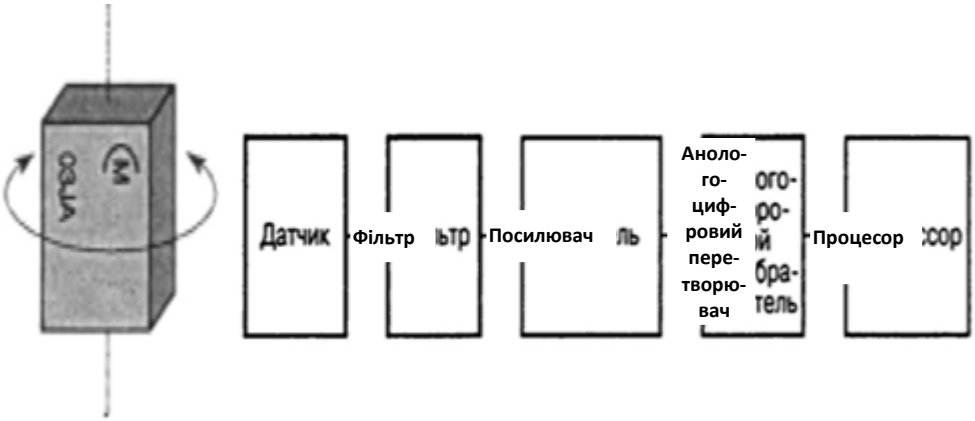


Рисунок 9 – Принцип роботи п’єзоелектричного гіроскопу

Датчики внутрішнього стану робота

Датчики цього типу повідомляють інформацію про внутрішній стан робота. Плата управління робота обробляє інформацію з датчиків – передусім, струм споживання двигунів і напругу живлення батареї. Але внутрішні датчики можуть також повідомляти інформацію про температуру або виконувати тестування зовнішніх датчиків. Для виміру напруги батареї використовується дільник напруги з активним опором, який забезпечує напругу 5 В при повній зарядці батареї. Значення напруги, що набувають при вимірах, міняються залежно від того, чи працює робот, або він вимкнений. У стані спокою напруга завжди вище значення для батареї, що подає струм. Про реальний стан батарей слід судити по їх напрузі при роботі робота.

Вимір струму споживання двигунів також є дуже важливою інформацією. Вона може або підтвердити нормальну роботу робота, або вказати блокування одного з двигунів. У разі блокування робот повинен обертатися навколо своєї реї замість руху по прямій. Якщо ця несправність не буде вчасно усунена, двигун може вийти з ладу при підвищенні струму більше за максимально допустимий. Як правило, для визначення струму, споживаного двигунами, використовуються резистори невеликого номінала, що підключаються послідовно з кожним з двигунів. Надмірне збільшення температури електронних компонентів або двигунів є вірною ознакою несправності в їх роботі. В цьому випадку досить використати терморезистор з негативним або позитивним температурним коефіцієнтом опору спільно з яким-небудь резистором для створення дільника напруги, напругу з якого можливо прочитати через аналоговий вхід плати управління. Існують також датчики температури, які виробляють аналогову напругу, пропорційну температурі.

Розробка структурної схеми

Виходячи з короткого технічного завдання, та структури ОС Linux, в якій система драйверів зовнішніх пристроїв добре підтримується внутрішньою файловою системою (базовий католог /dev), а також приймаючи до уваги, що жорсткий диск з точки зору ядра є блочним пристроєм, який підтримується базовими функціями вбудованими в ядро. Розглянемо наступну структурну схему системи (рисунок 10).

Система програмного забезпечення складається з двох рівнів – апаратного-програмного і програмного. На програмно-апаратному рівні потрібно забезпечити взаємодію між жорстким диском та ос на рівні системних викликів та API ядра ОС. Взаємодія між ядром та жорстким пристроєм забезпечується базовою програмою поблочного зчитування даних та перевірки на помилку. В свою чергу програмне забезпечення за принципами системного та об'єктно орієнтованого підходів поділяється на два рівні:

– системний, який забезпечує математику перевірки ушкодженних блоків та їх маркування на нижньому(апаратному) рівні;

– інтерфейсний, який забезпечує інтерфейс між пересічним користувачем та тестуючим модулем.

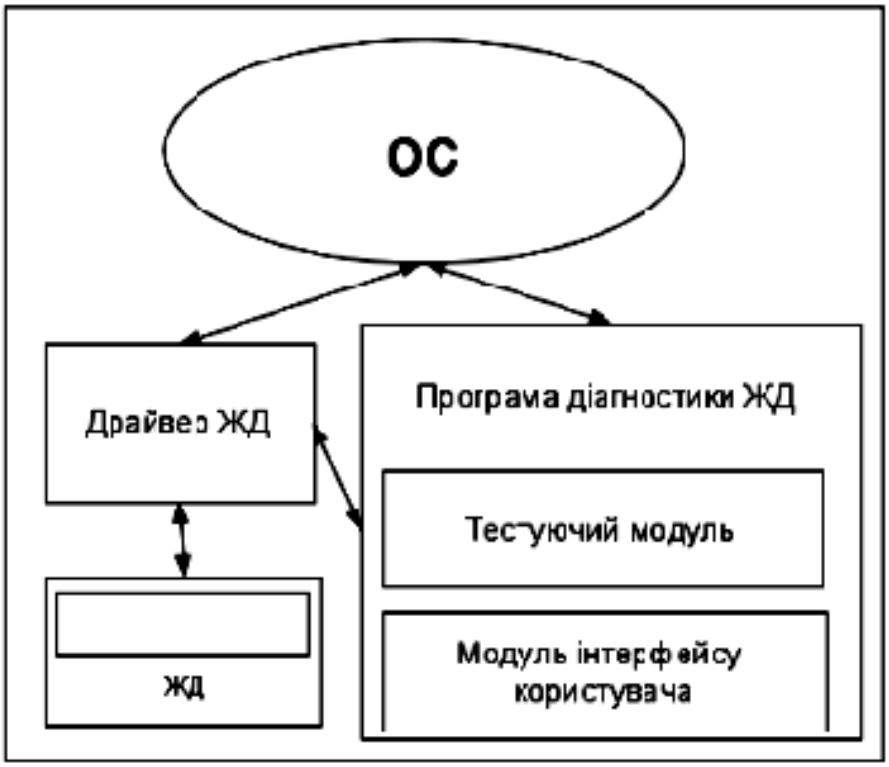


Рисунок 10 – Структурна схема системи

Висновок. У статті розглянуто та проаналізовано програмне забезпечення, яке призначено для операційної системи роботизованих комплексів. В межах України в недостатній мірі представлені вітчизняні розробки в цій області. У роботі наведені теоретичне узагальнення й рішення наукового завдання дослідження методів створення операційної системи роботизованих комплексів. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем створення операційної системи роботизованих комплексів; Досліджена система створення операційної системи роботизованих комплексів; На основі отриманих результатів досліджень створена програмна реалізація операційної системи роботизованих комплексів. Розроблені під час виконання роботи алгоритми дозволяють успішно вирішувати завдання створення операційної системи роботизованих комплексів. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки. Розроблене програмне забезпечення має простий, дружній та зручний інтерфейс користувача, що забезпечує легкість у освоєнні роботи програмного продукту, зручність у використанні, і не потребує особливих спеціальних знань. При створені програмного забезпечення було використано об’єктно-орієнтований підхід, що відповідає сучасним тенденціям у галузі розробки комерційних програмних систем. Програма реалізована на мові високого рівня IDE Qt Creator та Borland Delphi. Дана мова програмування дозволяє найбільш ефективно обробляти дані. Це дозволило мінімізувати строк розробки програмного забезпечення, і, як слід, зменшити витрати на його розробку. Запропоноване програмне забезпечення ділиться на загальне програмне забезпечення, що поставляється із засобами обчислювальної техніки й спеціальне програмне забезпечення, що спеціально розроблене для даної конкретної системи й включає програми, що реалізують її функції. Програма призначена для виконання під управлінням багатозадачної операційної системи Linux. Даються необхідні рекомендації з установки розробленого програмного забезпечення. Для підвищення рівня безпеки запропоновано застосовувати алгоритм AES.

Список літератури

1. Коваленко А.С. Обґрунтування необхідності створення систем технічної діагностики інтегрованих інформаційних систем / А.С. Коваленко, О.А. Смірнов, О.В. Коваленко // Інформатика та системні науки: V Всеукр. наук.-практ. конф., 13–15 бер. 2014 р., м. Полтава: зб. тез. – Полтава: ПУЕТ, 2014. – С. 292-294.
2. Коваленко А.С. Задачи распознавания ситуаций в системах организационной стратегии интеграции производства и операций / А.С. Коваленко, А.В. Коваленко // Комбінаторні конфігурації та їх застосування: XVI міжнар. наук.-практ. сем., 11-12 квіт. 2014 р., м. Кіровоград: зб. тез. – Кіровоград: КНТУ, 2014. – С. 53-55.
3. Коваленко А.С. Створення систем технічної діагностики для автоматизації процесів керування в інтегрованих інформаційних системах / А.С. Коваленко, О.А. Смірнов, О.В. Коваленко // Проблеми і перспективи розвитку ІТ-індустрії: VI між нар. наук.-практ. конф., 17-18 квіт. 2014 р., м. Харків: зб. тез. – Харків: ХНЕУ, 2014. – С. 241.
4. Коваленко А.С. Визначення понятійного апарату та напрямів досліджень для синтезу систем технічної діагностики інтегрованих інформаційних систем / А.С. Коваленко, О.А. Смірнов, О.В. Коваленко // Комп'ютерне моделювання у наукоємних технологіях (КМНТ-2014): наук.-техн. конф. з міжнар. участю, 28-31 трав. 2014 р., м. Харків: зб. наук. праць. – Харків: ХНУ, 2014. – С. 190-193.
5. Коваленко А.С. Основні складові та функції системи технічної діагностики інтегрованих інформаційних систем / Коваленко А.С. // Інформаційні технології та комп'ютерна інженерія: наук.-практ. конф., 4 груд. 2014 р., м. Кіровоград: зб. тез доп. – Кіровоград: КНТУ, 2014. – С. 236.
6. Коваленко А.С. Розробка структури бази даних інтегрованої інформаційної системи / А.С. Коваленко, О.А. Смірнов, О.В. Коваленко // Проблеми і перспективи розвитку ІТ-індустрії: VII міжнар. наук.-практ. конф., 17-18 квіт. 2015 р., м. Харків: зб. тез. – Харків: ХНЕУ, 2015. – С. 15.
7. Коваленко А.С. Дослідження елементів інтегрованої інформаційної системи / А.С. Коваленко, О.А. Смірнов, О.В. Коваленко // Комбінаторні конфігурації та їх застосування: XVII між нар. наук.-практ. сем., 17-18 квіт. 2015 р., м. Кіровоград: зб. тез – Кіровоград: КНТУ, 2015. – С. 5.
8. Коваленко А.С. Метод автоматизованої перевірки результатів вимірювання параметрів об'єкті в інтегрованої інформаційної системи / А.С. Коваленко, О.А. Смірнов, О.В. Коваленко // Стратегія якості у промисловості і освіті: XI міжнар. конф., 1 – 5 черв. 2015 р., м. Варна, Болгарія.: зб. матер. – Варна: ТУВ, 2015. – С. 423-426.
9. Коваленко А.С. Обґрунтування необхідності створення розподіленої бази даних для забезпечення захисту рухомих повітряних об`єктів / А.С. Коваленко, О.А. Смірнов, О.В. Коваленко // Перспективні напрями захисту інформації: I всеукр. наук.-практ. конф., 07 вер. 2015 р., м. Одеса: зб. тез доп. – Одеса: ОНАЗ, 2015. – С. 35-39.
10. Коваленко А.С. Розробка інформаційної моделі автоматизованої оцінки технічного стану інтегральної інформаційної системи / А.С. Коваленко, О.А. Смірнов, О.В. Коваленко // Інформаційні технології та взаємодії (IT & I): II між нар. наук.-практ. конф., 3-5 лист. 2015 р., м. Київ: тези доп. – Київ: КНУ ім. Т. Шевченка, 2015. – С. 41-42.

УДК 004

І. Недоступ, магістр гр. КІ-18М-1,4
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ ОЦІНКИ ПРОДУКТИВНОСТІ СИСТЕМ ЗБЕРІГАННЯ ДАНИХ

У статті розроблено програмне забезпечення, яке призначено для системи оцінки продуктивності систем зберігання даних. Метою розробки є дослідження та програмна реалізація системи оцінки продуктивності систем зберігання даних. Об'єктом дослідження є процес оцінки продуктивності систем зберігання даних. Предметом дослідження є методи оцінки продуктивності систем зберігання даних. Методи дослідження базуються на методах Big Data, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи оцінки продуктивності систем зберігання даних. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

комп'ютерна інженерія, оцінка продуктивності, системи зберігання даних

Постановка проблеми. Щоб правильно вибрати нову систем зберігання даних СЗД або спланувати модернізацію існуючої, необхідно з'ясувати вимоги, пропоновані IT-системою до зберігання даних. Основні з них – ємність і продуктивність. І якщо питання «Скільки терабайтів корисної ємності вам потрібно?», як правило, не викликає проблем, то прохання вказати необхідну продуктивність можуть багатьох загнати в глухий кут.

Як довідатися продуктивність систем зберігання даних (СЗД)? Існують два підходи для її оцінки – технічний і користувальницький. У першому випадку продуктивність описується рядом технічних параметрів, пов'язаних з роботою СЗД. Такий підхід використовується в основному IT-фахівцями. У другому випадку продуктивність оцінюється на підставі суб'єктивних думок користувачів щодо того, наскільки швидко працює IT-система. Очевидно, що для реальної оцінки продуктивності СЗД цей підхід не годиться, але про нього не треба забувати, оскільки користувачі інформаційних систем бачать продуктивність будь-якого компонента IT-системи крізь призму своїх моніторів.

Отже, з погляду IT-фахівця, продуктивність СЗД – це в першу чергу кількість операцій введення-виводу в секунду (IOPS) і обсяг переданих мегабайтів у секунду (Мбайт/с), які система зберігання здатна забезпечити при читанні й записі даних. Продуктивність СЗД в IOPS використовується для оцінки навантаження транзакційних застосунків: баз даних Online Transaction Processing (OLTP), файлових сховищ, поштових систем і іншого. Інший технічний параметр, тісно пов'язаний із транзакційним навантаженням, – час відгуку при операціях введення-виводу (response time). Іншими словами, цей час, витрачений СЗД на обробку однієї операції введення-виводу й передачу її результатів хосту.

Час відгуку й раніше використовувалося поряд з кількістю IOPS для детального планування конфігурації СЗД. Але широку популярність цей параметр придбав після появи СЗД, цілком побудованих на базі флеш-накопичувачів. Основна особливість цих систем – здатність обробляти введення-вивід застосунків згодом відгуку менше однієї мілісекунди. Для ряду застосунків, зокрема баз даних OLTP, мінімально можливий час відгуку так само важливо, як і IOPS.

Для оцінки продуктивності застосунків, у яких профіль навантаження на СЗД являє собою послідовний доступ до даних, прийнято використовувати обсяг переданих даних, виражений у мегабайтах у секунду (Мбайт/с). Приклад таких застосунків – бази даних у конфігурації «сховище даних» (Data Warehouse, DWH), застосунки для обробки відеоконтента й резервного копіювання

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи оцінки продуктивності систем зберігання даних.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи оцінки продуктивності систем зберігання даних.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

- Огляд існуючих систем оцінки продуктивності систем зберігання даних.
- Дослідження системи оцінки продуктивності систем зберігання даних.
- Програмна реалізація системи оцінки продуктивності систем зберігання даних.

Об'єктом дослідження є процес оцінки продуктивності систем зберігання даних.

Предметом дослідження є методи оцінки продуктивності систем зберігання даних.

Методи дослідження базуються на методах Big Data, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Підготовку нового сервера до роботи варто починати з налаштування резервного копіювання. Всі, здавалося б, про це знають – але часом навіть досвідчені системні адміністратори допускають непрощенні помилки. І справа тут не тільки

в тому, що завдання налаштування нового сервера потрібно вирішувати дуже швидко, але ще й у тому, що далеко не завжди буває ясно, який спосіб резервного копіювання потрібно використовувати.

Звичайно, ідеальний спосіб, який би всіх улаштовував, створити неможливо: скрізь є свої плюси й мінуси. Але в той же час цілком реальним представляється підібрати спосіб, що максимально підходить під специфіку конкретно проекту.

При виборі способу резервного копіювання потрібно насамперед звернути увагу на наступні критерії:

– Швидкість (час) резервного копіювання в сховище;
– Швидкість (час) відновлення з резервної копії;
– Скільки копій можна буде тримати при обмеженому розмірі сховища (сервері зберігання бекапів);
– Обсяг ризиків через неконсистентності резервні копії, неналагодженості методу виконання бекапів, повної або часткової втрати бекапів;
– Накладні витрати: рівень навантаження, створюваної на сервер при виконанні копіювання, зменшення швидкості відгуку сервісу й т.п.
– Вартість оренди всіх сервісів, що використовуються.

У цьому розділі розповімо про основні способи резервного копіювання серверів під керуванням Linux-систем і про найбільш типові проблеми, з якими можуть зштовхнутися новачки в цій дуже важливій області системного адміністрування.

Схема організації зберігання й відновлення з резервних копій

При виборі схеми організації методу резервування варто звернути увагу на наступні базові моменти:

– Резервні копії не можна зберігати в одному місці з резервуємими даними. Якщо ви зберігаєте резервну копію на одному дисковому масиві з вашими даними, то ви втратите її у випадку ушкодження основного дискового масиву.
– Дзеркальовані (RAID1) не можна порівнювати з резервним копіюванням. Рейд захищає вас тільки від апаратної проблеми з одним з дисків (а рано або пізно така проблема буде, тому що дискова підсистема майже завжди є вузьким місцем на сервері). До того ж при використанні апаратних рейдів є ризик поломки контролера, тобто необхідно зберігати його запасну модель.
– Якщо ви зберігаєте резервні копії в рамках однієї стійки в дата-центрі (ДЦ) або просто в рамках одного ДЦ, то в такій ситуації теж є певні ризики.
– Якщо ви зберігаєте резервні копії в різних ДЦ, то різко зростають витрати на мережу й швидкість відновлення з віддаленої копії.

Часто причиною відновлення даних служить ушкодження файлової системи або дисків. Тобто бекапи потрібно зберігати десь на окремому сервері-сховищі. У цьому випадку проблемою може стати «ширина» каналу передачі даних. Якщо у вас виділений сервер, то резервне копіювання дуже бажано виконувати по окремому мережному інтерфейсі, а не на тім же, що виконує обмін даних із клієнтами. Інакше запити вашого клієнта можуть не «поміститися» в обмежений канал зв'язку. Або через трафіку клієнтів бекапи не будуть зроблені в строк.

Далі потрібно подумати про схему й час відновлення даних з погляду зберігання бекапів. Може бути вас цілком улаштовує, що бекап виконується за 6 годин уночі на сховище з обмеженою швидкістю доступу, однак відновлення довжиною в 6 годин вас навряд чи влаштує. Значить доступ до резервних копій повинен бути зручним і дані повинні копіюватися досить швидко. Так, наприклад, відновлення 1Тб даних зі смугою в 1Гб/с займе майже 3 години, і це якщо ви не «упретеся» у продуктивність дискової підсистеми в сховищі й сервері. І не забудьте додати до цього час виявлення проблеми, час на рішення про відкіт, час перевірки цілісності відновлених даних і обсяг наступного невдоволення клієнтів/колег.

Інкрементальне резервне копіювання

При **інкрементальному** резервному копіюванні копіюються тільки файли, які були змінені із часу попереднього бекапа. Наступне інкрементальне резервне копіювання додає тільки файли, які були змінені з моменту попереднього. У середньому інкрементальне резервне копіювання займає менше часу, тому що копіюється менша кількість файлів. Однак процес відновлення даних займає більше часу, тому що повинні бути відновлені дані останнього повного резервного копіювання, плюс дані всіх наступних інкрементальних резервних копіювань. При цьому на відміну від диференціального копіювання, що змінилися або нові файли не заміщають старі, а додаються на носій незалежно.

Інкрементальне копіювання найчастіше виробляється за допомогою утиліти rsync. З його допомогою можна заощадити місце в сховище, якщо кількість змін за день не дуже велико. Якщо змінені файли мають великий розмір, то вони будуть скопійовані повністю без заміни попередніх версій.

Процес резервного копіювання за допомогою rsync можна розділити на наступні кроки:

– Складається список файлів на резервуємому сервері й у сховище, по кожному файлі зчитуються метадані (права, час зміни й т.д.) або контрольна сума (при використанні ключа -checksum).

– Якщо метадані файлів відрізняються, то файл б'ється на блоки й по кожному блоці вважається контрольна сума. блоки, Що Відрізняються, накачуються в сховище.

– Якщо під час підрахунку контрольних сум або передачі файлу в нього була внесена зміна, його резервування повторюється з початку.

– За замовчуванням rsync передає дані через SSH, а значить кожний блок даних додатково шифрується. Rsync можна також запустити як демон і передавати дані без шифрування по його протоколі.

З більше докладною інформацією про роботу rsync можна ознайомитися на офіційному сайті.

Для кожного файлу rsync виконує дуже велика кількість операцій. Якщо файлів на сервері багато або якщо процесор сильно завантажений, то швидкість резервного копіювання буде істотно знижена.

З досвіду можемо сказати, що проблеми на SATA-дисках (RAID1) починаються приблизно після 200G даних на сервері. Насправді всі, кінцеве ж, залежить від кількості inode. І в кожному випадку ця величина може зміщатися як в одну так і в іншу сторону.

Після певної риси час виконання резервного копіювання буде дуже довгим або попросту не буде відпрацьовувати за добу.

Для того, щоб не порівнювати всі файли, є lsyncd. Цей демон збирає інформацію про файли, що змінилися, тобто ми вже заздалегідь будемо мати готовий їхній список для rsync. Треба, однак, урахувати, що він дає додаткове навантаження на дискову підсистему.

Диференціальне резервне копіювання

При **диференціальному** резервному копіюванні кожний файл, що був змінений з моменту останнього повного резервного копіювання, копіюється щораз заново. Диференціальне копіювання прискорює процес відновлення. Усе, що вам необхідно – це остання повна й остання диференціальна резервна копія. Популярність диференціального резервного копіювання росте, тому що всі копії файлів робляться в певні моменти часу, що, наприклад, дуже важливо при зараженні вірусами.

Диференціальне резервне копіювання здійснюється, наприклад, за допомогою такої утиліти, як rdiff-backup. При роботі із цією утилітою виникають ті ж проблеми, що й при інкрементальному резервному копіюванні.

У цілому, якщо при пошуку різниці в даних здійснюється повний перебір файлів, проблеми такого роду резервування аналогічні проблемам з rsync.

Хочемо окремо відзначити, що якщо у вашій схемі резервного копіювання кожний файл копіюється окремо, те варто видаляти/виключати непотрібні вам файли. Наприклад, це

можуть бути кеши CMS. У таких кешах звичайно дуже багато маленьких файлів, втрата яких не позначиться на коректній роботі сервера.

Повне резервне копіювання

Повне копіювання звичайно торкає всієї вашої системи й всіх файлів. Щотижневе, щомісячне й щоквартальне резервне копіювання має на увазі створення повної копії всіх даних. Звичайно воно виконується по п'ятницях або протягом вихідних, коли копіювання великого обсягу даних не впливає на роботу організації. Наступні резервні копіювання, виконувані з понеділка по четвер до наступного повного копіювання, можуть бути диференціальними або інкрементальними, головним чином для того, щоб зберегти час і місце на носії. Повне резервне копіювання варто проводити принаймні щотижня.

У більшості публікацій по відповідній тематиці рекомендується повне резервне копіювання виконувати один або два рази в тиждень, а в інший час час – використовувати інкрементальне й диференціальне. У таких радах є свій резон. У більшості випадків повного резервного копіювання раз у тиждень цілком достатньо. Виконувати його повторно має сенс у тому випадку, якщо у вас немає можливості на стороні сховища актуалізувати повний бекап і для забезпечення гарантії коректності резервної копії (це може знадобитися, наприклад, у випадках, якщо ви по тим або інших причинах не довіряєте наявним у вас скриптам або софту для резервного копіювання.

Насправді повне резервне копіювання можна поділити на 2 частині:

– Повне резервне копіювання на рівні файлової системи;
– Повне резервне копіювання на рівні пристроїв.

Розглянемо їхні характерні риси на прикладі:

```
root@komarov:~# df -h
Filesystem                Size  Used Avail Use% Mounted on
/dev/mapper/komarov_ system-root  3.4G  808M  2.4G  25% /
/dev/mapper/komarov_ system-home  931G  439G  493G  48% /home
udev                      383M  4.0K  383M   1% /dev
tmpfs                     107M  104K  107M   1% /run
tmpfs                     531M     0  531M   0% /tmp
none                      5.0M     0  5.0M   0% /run/lock
none                      531M     0  531M   0% /run/shm
/dev/xvda1                138M   22M  109M  17% /boot
```

Резервувати ми будемо тільки /home. Все інше можна швидко відновити вручну. Можна також розгорнути сервер системою керування конфігураціями й підключити до нього наш /home.

Повне резервне копіювання на рівні файлової системи

Типовий представник: dump.

Утиліта створює «дамп» файлової системи. Можна створювати не тільки повну, але й інкрементальну резервну копію. dump працює з таблицею inode і «розуміє» структуру файлів (так, розріджені файли стискуються).

Створювати дамп працюючої файлової системи «нерозумно й небезпечно», тому що файлова система (ФС) може змінюватися під час створення дампа. Його треба створювати зі снапшоту (трохи пізніше ми обговоримо особливості роботи зі снапшотами більш докладно), відмонтованої або замороженої ФС.

Така схема так само залежить від кількості файлів, і час її виконання буде рости з ростом кількості даних на диску. У той же час в dump швидкість роботи вище, ніж в rsync.

У випадку, якщо потрібно відновити не резервну копію цілком, а, наприклад, тільки пари випадково зіпсованих файлів), добування таких файлів утилітою restore може зайняти занадто багато часу.

Повне резервне копіювання на рівні пристроїв

mdraid і DRBD

Фактично настроюється RAID1 з диском/рейдом на сервері й мережному диску, і час від часу (по частоті виконання бекапів) додатковий диск синхронізується з основним диском/рейдом на сервері.

Найбільший плюс – швидкість. Тривалість виконання синхронізації залежить тільки від кількості внесених за останній день змін.

Така система резервного копіювання використовується досить часто, але мало хто усвідомлює тім, що отримані з її допомогою резервні копії можуть бути недієздатними, і от чому. Коли синхронізація дисків завершена, диск із резервною копією відключається. Якщо в нас, наприклад, запущена СУБД, що пише дані на локальний диск порціями, зберігаючи проміжні дані в кеші, немає ніякої гарантії того, що вони взагалі потраплять на бекапний диск. У найкращому разі ми втратимо частину змінюваних даних. Тому такі бекапи навряд чи варто вважати надійними.

LVM + dd

Снапшоти – чудовий инстумент для створення консистентних бекапів. Перед створенням снапшота необхідно скинути кеш ФС і вашого ПЗ на дискову підсистему.

Наприклад, з одним MySQL це буде виглядати так:

```
$ sudo mysql -e 'FLUSH TABLES WITH READ LOCK;'
$ sudo mysql -e 'FLUSH LOGS;'
$ sudo sync
$ sudo lvcreate -s -p r -l100%free -n %s_backup /dev/vg/%s
$ sudo mysql -e 'UNLOCK TABLES;'
```

Далі можна копіювати снапшот у сховище. Головне – стежити за тим, щоб під час копіювання снапшот не самознищився й не забувати, що при створенні снапшота швидкість запису впаде в рази.

Бекапи СУБД можна створити окремо (наприклад, використовуючи бінарні логи), усунувши тим найпростіший на час скидання кеша. А можна створювати дампи в сховище, запустивши там инстанс СУБД. Резервне копіювання різних СУБД – це тема для окремих публікацій.

Копіювати снапшот можна з використанням докачки (наприклад, rsync з патчем для копіювання блокових пристроїв:

bugzilla.redhat.com/show_bug.cgi?id=494313),

можна по блоках і без шифрування (netcat, ftp). Можна передавати блоки в стислому виді й монтувати їх у сховище за допомогою AVFS, і примонтувати на сервері розділ з бекапами по SMB.

Стиск усуває проблеми швидкості передачі, завантаження каналу й місця в сховище. Але, однак якщо ви не використовуєте AVFS у сховище, то на відновлення тільки частини даних у вас піде багато часу. Якщо будете використовувати AVFS, то зштовхнетеся з її «вогкістю».

Альтернатива стиску блоками – squashfs: можна підмонтувати, приміром, по Samba розділ до сервера й виконати mksquashfs, але ця утиліта так само працює з файлами, тобто залежить від їхньої кількості.

До того ж при створенні squashfs витрачається досить багато ОЗП, що може легко привести до виклику oom-killer.

Безпека

Необхідно убезпечити себе від ситуації коли сховище або ваш сервер будуть зламані. Якщо зламано сервер, то краще щоб не було прав на видалення/зміна файлів у сховище в користувача, що записує туди дані.

Якщо зламано сховище, то права бекапного користувача на сервері так само бажано обмежити по максимуму.

Якщо канал резервного копіювання може бути прослуханий, то потрібні засоби шифрування.

У підсумку, при виборі системи резервного копіювання під ваш проект, потрібно провести тести обраного типу резервного копіювання й звернути увагу на:

– час резервного копіювання в поточній стадії проекту;
– час резервного копіювання у випадку, якщо даних буде в рази більше;
– навантаження на канал;
– навантаження на дискову підсистему на сервері й у сховище;
– час відновлення всіх даних;
– час відновлення пари файлів;
– необхідність у консистентності даних, особливо БД;
– витрата пам'яті й наявність викликів oom-killer;

Розробка структурної схеми

Продуктивність IT-системи в цілому визначається продуктивністю її окремих компонентів:

– за стосунків;
– операційної системи;
– фізичного або віртуального сервера;
– мережі передачі даних між сервером і СЗД;
– самої СЗД.

Кожний із цих компонентів, як правило, складається з безлічі окремих підсистем, кожна з яких здатна впливати на загальну продуктивність IT-системи. Так, недолік оперативної пам'яті в сервері навіть при наявності 100 високопродуктивних процесорних ядер може привести до помітного зниження загальної продуктивності IT-системи. Або, приміром, невірно обрана конфігурація дискової підсистеми СЗД старшого класу буде «гальмувати» всю IT-систему, незважаючи на те що така СЗД здатно витримати дуже більше навантаження.

Очевидно, що продуктивність IT-системи – це не сума показників всіх її компонентів. Найчастіше вона залежить від характеристик найбільше «слабкої ланки». Тому якщо ставиться завдання підвищити продуктивність IT-системи, те не завжди необхідно купувати нову СЗД, установлювати нові сервери із процесорами останнього покоління й т.п. Набагато важливіше виявити вузьке місце в поточній конфігурації IT-системи й зрозуміти, чи можна виправити ситуацію, використовуючи наявні ресурси. Наприклад, заміна СЗД на флеш-масив (All-Flash Array, AFA) може дати приріст продуктивності IT-системи на кілька десятків відсотків, тоді як проста оптимізація SQL-Запиту до СУБД дозволить збільшити цю продуктивність багаторазово.

Якщо ж покупка нової СЗД неминуча, потрібно ретельно продумати всі деталі. Щоб правильно вибрати нову СЗД або спланувати модернізацію існуючої, необхідно зібрати всі вимоги, пропоновані IT-системою до зберігання даних, основні з яких – ємність і продуктивність. І якщо питання «Скільки терабайтів корисної ємності вам потрібно?», як правило, не викликає проблем, то прохання вказати величину необхідної продуктивності можуть багатьох загнати в глухий кут.

Здавалося б, простіше нікуди: щоб забезпечити високу продуктивність ИТ для всіх підрозділів бізнесу, потрібно купити саму дорогу й швидку СЗД – тільки й усього. Але так може здатися тільки на перший погляд. Таким придбанням будуть задоволені далеко не всі відділи підприємства, і насамперед, звичайно, фінансовий департамент, адже між продуктивністю СЗД і її вартістю існує чітка кореляція, а витрати на впровадження повинні якнайменше позначатися на бюджеті. Разом з тим чим менше засобів буде витрачено на нову СЗД, тим нижче буде її продуктивність – і тоді в збитку виявляться рядові користувачі IT-системи. Відповідно, IT-фахівець, що відповідає за впровадження нового сховища даних, повинен знайти золоту середину, коли й фінансові обмеження будуть враховані, і продуктивність виявиться достатньою.

Для вже існуючих IT-систем, яким потрібно лише відновлення (приміром, у зв'язку з ростом або розширенням бізнесу), це досить просте завдання: необхідно виміряти поточні

показники продуктивності і ємності СЗД, після чого спланувати їхнє збільшення на найближчі рік-три й закупити відповідні компоненти СЗД.

Впровадження нового рішення теж, як правило, не викликає особливих труднощів: постачальники програмного забезпечення звичайно вже мають готові рекомендації з розгортання своїх систем. Приміром, у компанії VMware існує поняття «шаблонового користувача» стосовно до рішень по віртуалізації робітників місць (VDI). У прийнятій класифікації всі користувачі діляться на три категорії: light-користувачі несильно навантажують систему, тоді як medium- і heavy-користувачі більше вимогливі до ресурсів. По кожній категорії підготовлені кількісні характеристики: рекомендується емкость, що, пам'яті, число процесорних ядер, IOPS, обсяг переданих мегабайтів у секунду й так далі. Таким чином, знаючи, що необхідно розгорнути VDI-систему на 1000 користувачів, фахівці заздалегідь можуть оцінити, які IT-ресурси для цього будуть потрібні.

Однак бувають ситуації, коли інформація про вимоги до продуктивності дискової підсистеми відсутній або є обґрунтовані сумніви в застосовності шаблонових даних. У цьому випадку можна протестувати IT-систему на планованому до придбання встаткуванні. Багато виробників устаткування й програмних продуктів надають послугу, що дозволяє оцінити поводження конкретної IT-системи, що здійснює обробку певних даних, при різних програмно-апаратних конфігураціях і зрозуміти, що необхідно для її успішного впровадження.

Як показує досвід впровадження й експлуатації IT-систем, перед відновленням програмної або апаратної складової існуючої IT-системи необхідно зібрати статистику про продуктивність роботи всіх її компонентів – застосунків, серверів, СЗД – і повторити ту ж процедуру після впровадження. Це, по-перше, допоможе оцінити, наскільки виросла продуктивність кожного компонента IT-системи, а по-друге, дасть можливість продемонструвати бізнес-користувачам ефективність відновлення. Найчастіше оцінка досягнутих результатів залежить від суб'єктивної думки: в одного фахівця за консоллю встаткування працює повільніше, в іншого – швидше. Таким чином, маючи чіткі кількісні характеристики, зафіксовані до й після відновлення, можна встановити, які зміни відбулися із системою насправді.

Самий оптимальний варіант використання дисків різних типів у СЗД – багаторівневе зберігання даних. По суті, цей не засіб збільшення продуктивності дискової підсистеми системи зберігання, а спосіб економії фінансів за рахунок установки в одному дисковому пулі декількох типів дисків, різних за рівнем продуктивності й вартості.

Яким образом досягається економія? В основу багаторівневого зберігання покладений наступний факт: дані, що зберігаються на СЗД, у більшості випадків затребувані нерівномірно. Так, у застосунку, що збирає й накопичує, скажемо, дані про погоду, активно використовуваних – або, у термінології багаторівневого зберігання, «гарячих» – не більше 5–15% від загального обсягу. Це пов'язане з тим, що свіжі дані запитуються набагато частіше, ніж, наприклад, дані п'ятирічної давнини.

Для зберігання «гарячих» даних завжди рекомендується використовувати високопродуктивні диски. Звертання до оставшихся «холодного» даним відбувається набагато рідше, і тому для їхнього зберігання краще задіяти більше дешеві і ємні, але менш продуктивні диски SAS або NL-SAS. При цьому система зберігання автоматично перерозподіляє активні й неактивні дані між відповідними швидкими й повільними рівнями зберігання.

Таким чином, ми одержуємо дисковий пул, продуктивність якого ледве менше продуктивності найшвидшого рівня зберігання в ньому, але загальна вартість дисків (з урахуванням ліцензії на багаторівневе зберігання для СЗД) виявляється істотно нижче, ніж якби в дисковому пулі використовувалися тільки високопродуктивні диски.

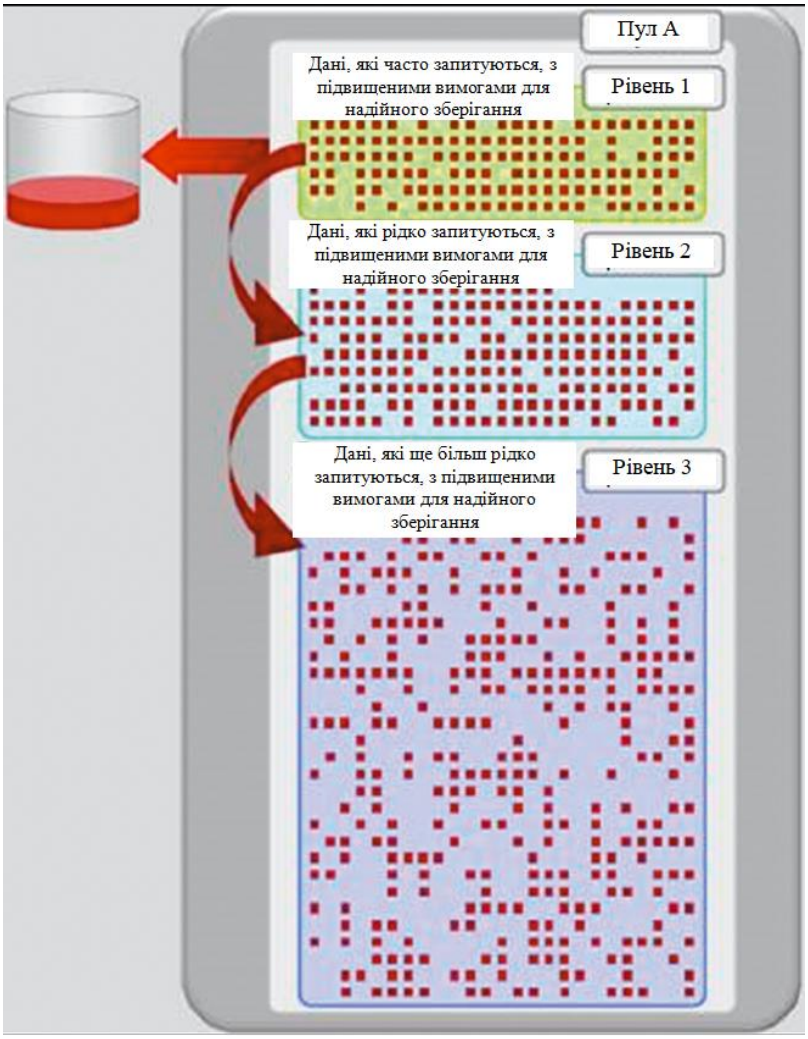


Рисунок 1 – Структурна схема системи

Основний критерій вибору багаторівневого зберігання, як уже було сказано, – нерівномірність використання даних. Найбільше часто багаторівневе зберігання використовується з базами даних OLTP і віртуальними середовищами, побудованими на основі VMware і Microsoft Hyper-V. Однак необхідно відзначити, що універсальних рецептів, що гарантують, що цей підхід буде ефективним абсолютно для всіх рішень, не існує. Якщо в компанії є сумніву в правильності застосування багаторівневого зберігання, вона завжди може протестувати свою IT-систему на конкретній системі зберігання даних і оцінити її ефективність.

Висновок. У статті розглянуто та проаналізовано програмне забезпечення, яке призначено для операційної системи оцінки продуктивності систем зберігання даних. В межах України в недостатній мірі представлені вітчизняні розробки в цій області. У роботі наведені теоретичне узагальнення й рішення наукового завдання дослідження методів оцінки продуктивності систем зберігання даних. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем оцінки продуктивності систем зберігання даних; Досліджена система оцінки продуктивності систем зберігання даних; На основі отриманих результатів досліджень створена програмна реалізація системи оцінки продуктивності систем зберігання даних. Розроблені під час виконання роботи алгоритми дозволяють успішно вирішувати завдання оцінки продуктивності систем зберігання даних. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки. Розроблене програмне забезпечення має простий, дружній та зручний інтерфейс користувача, що

забезпечує легкість у освоєнні роботи програмного продукту, зручність у використанні, і не потребує особливих спеціальних знань. При створені програмного забезпечення було використано об'єктно-орієнтований підхід, що відповідає сучасним тенденціям у галузі розробки комерційних програмних систем. Програма реалізована на мові високого рівня Visual C#. Дана мова програмування дозволяє найбільш ефективно обробляти дані. Це дозволило мінімізувати строк розробки програмного забезпечення, і, як слід, зменшити витрати на його розробку. Запропоноване програмне забезпечення ділиться на загальне програмне забезпечення, що поставляється із засобами обчислювальної техніки й спеціальне програмне забезпечення, що спеціально розроблене для даної конкретної системи й включає програми, що реалізують її функції. Даються необхідні рекомендації з установки розробленого програмного забезпечення. Для підвищення рівня безпеки запропоновано застосовувати алгоритм NTRUEncrypt.

Список літератури

1. Коваленко А.С. Разработка структуры базы данных интегрированной информационной системы / А.С. Коваленко, А.В. Коваленко // Информационные технологии и защита информации в информационно-коммуникационных системах: монографія / Под редакцией профессора В.С. Пономаренко. – Х.: Вид-во ТОВ «Щедра садиба плюс», 2015. – С. 54-64.
2. Кожанова А.С. Обґрунтування необхідності створення систем технічної діагностики інтегрованих інформаційних систем / О.А. Смірнов, А.С. Кожанова, О.В. Коваленко // Системи обробки інформації. – Х.: ХУПС, 2013. – Вип. 6(113). – С. 255-257.
3. Коваленко А.С. Задачи распознавания ситуаций в ERP системах / А.В. Коваленко ., А.А. Смірнов, А.С. Коваленко // Системи обробки інформації. – Х.: ХУПС, 2014. – Вип. 4(120). – С. 161-164.
4. Коваленко А.С. Підсистема технічної діагностики для автоматизації процесів керування в інтегрованих інформаційних системах / А.С. Коваленко , О.А.Смірнов, О.В. Коваленко // Системи озброєння і військова техніка.– Х.: ХУПС, 2014. – № 1(37). – С. 126-129.
5. Коваленко А.С. Анализ эффективности использования экспертной системы технической диагностики с традиционной структурой / А.С. Коваленко, А.А. Смирнов, А.В. Коваленко // Системи озброєння і військова техніка. – Х.: ХУПС, 2014. – № 2(38). – С. 106-108.
6. Коваленко А.С. Разработка структуры экспертной системы технической диагностики интегрированной информационной системы / А.С. Коваленко, А.А. Смирнов, А.В. Коваленко // Наука і техніка Повітряних Сил Збройних Сил України. – Харків: ХУПС, 2014. – № 2(15). – С.154-157.
7. Коваленко А.С. Разработка структуры экспертной системы технической диагностики интегрированной информационной системы / А.С. Коваленко, А.А. Смирнов, А.В. Коваленко // Наука і техніка Повітряних Сил Збройних Сил України. – Харків: ХУПС, 2014. – № 2(15). – С.154-157.
8. Коваленко А.С. Структура системи технічної діагностики інтегрованих інформаційних систем / А.С. Коваленко, О.А. Смірнов, О.В. Коваленко // Збірник наукових праць Кіровоградського національного технічного університету / техніка в сільськогосподарському виробництві, галузеве машинобудування, автоматизація. – Кіровоград: Вид-во КНТУ, 2014. – Вип. 27. – С. 245-251.
9. Коваленко А.С. Дослідження будови інтегрованої інформаційної системи та її елементів / А.С. Коваленко, О.А. Смірнов, О.В. Коваленко // Системи озброєння і військова техніка. – Х.: ХУПС, 2014. – № 4(40). – С. 85-88.
10. Коваленко А.С. Розробка структури бази даних для обліку технічного стану елементів інтегрованої інформаційної системи з урахуванням вимог споживачів інформації / А.С. Коваленко, О.А. Смірнов, О.В. Коваленко // Системи обробки інформації. – Х.: ХУПС, 2015. – Вип. 1(126). – С. 75-79.

УДК 004

С. Немикін, магістр гр. КІ-18М-1,9
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ ПРОАКТИВНОГО СИСТЕМНОГО МОНІТОРИНГУ СЕД

У статті розглянуто програмне забезпечення, яке призначено для проактивного системного моніторингу СЕД. Метою розробки є дослідження та програмна реалізація проактивного системного моніторингу СЕД. Об'єктом дослідження є процес проактивного системного моніторингу СЕД. Предметом дослідження є методи проактивного системного моніторингу СЕД. Методи дослідження базуються на методах теорії побудови систем електронного документообігу, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація проактивного системного моніторингу СЕД. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення. Розроблено зручний інтерфейс користувача. Наведені інструкції по роботі з програмними засобами.
комп'ютерна інженерія, система електронного документообігу

Постановка проблеми. Одним з першочергових завдань, на яке варто виділити ресурси й час при супроводі системи електронного документообігу, є організація процесу моніторингу. Інструменти моніторингу полегшують рішення й попередження проблем. При цьому в довгостроковій перспективі проактивний підхід більше ефективний, ніж реактивний, і може бути реалізований за допомогою доступних засобів.

Після впровадження системи електронного документообігу (СЕД) процеси в компанії необхідно розвивати й адаптувати з урахуванням мінливого оточення.

Щоб уникнути дисбалансу між ростом запитів з боку співробітників бізнес-підрозділів і можливістю розвитку системи електронного документообігу, важливо на самому початку визначити вимоги, причому не тільки функціональні (які дії повинна виконувати система), але й нефункціональні (доступність, швидкодія, цілісність, можливості доробки/налаштування й ін.). Зокрема, для великих компаній можуть бути актуальними підтримка цілодобової роботи, одночасне підключення тисяч користувачів, масштабованість системи, схоронність і безпека даних.

Ще на старті проекту варто позначити цільові показники для цих параметрів з урахуванням потенційного росту масштабу розв'язуваних завдань. Крім системного ПЗ й устаткування, необхідно подбати про формування команди супроводу й підтримки.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини проактивного системного моніторингу СЕД.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація проактивного системного моніторингу СЕД.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем проактивного системного моніторингу СЕД.
– Дослідження проактивного системного моніторингу СЕД.
– Програмна реалізація проактивного системного моніторингу СЕД.

Об'єктом дослідження є процес проактивного системного моніторингу СЕД.

Предметом дослідження є методи проактивного системного моніторингу СЕД.

Методи дослідження базуються на методах теорії побудови систем електронного документообігу, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу.

Опис функціонування системи

Впровадження електронного документообігу на підприємстві – завдання дуже відповідальна й найчастіше пов'язана з корінною зміною діючих у Вас бізнес-процесів. За великим рахунком, з установкою електронного документообігу Ви міняєте стиль керування бізнесом. Переходити або не переходити на електронний документообіг? Якщо так – то яку систему електронного документообігу (СЕД) вибрати? Як швидко окупиться система? Яких зусиль і засобів зажадає технічна підтримка системи під час її штатної експлуатації? На всі ці й інші питання так чи інакше прийде відповісти, перш ніж буде схвалено рішення про придбання й установку СЕД на підприємстві.

У даному розділі коротко розглянуто:

– Коли потрібний електронний документообіг.
– Функції сучасних СЕД українських постачальників.
– Критерії вибору СЕД.

Коли необхідний електронний документообіг?

Власне кажучи, електронний документообіг ні в якому разі не повинен впроваджуватися як данина моді на "прогресивні технології". Якщо Ваш бізнес успішно працює й без електронного або навіть взагалі без паперового документообігу, дуже малоймовірно, що установка СЕД зробить його більше ефективним. Мова в цьому випадку, швидше за все, може йти лише про зручність роботи з документами. Так, наприклад, ми всі давно вже звикли до електронної пошти й до "загальноприйнятого" користувальницькому інтерфейсу поштового клієнта, у якому Ваші листи розкладені по папках. Аналогічним образом СЕД помістить Ваші документи в деякі папки й прийме на себе всі проблеми, пов'язані з пошуком, доступом і зберіганням документів. Оптимальним рішенням тут може бути такий інтерфейс робочого місця користувача системи, у який інтегровані функції звичного поштового клієнта, наприклад, такого як Microsoft Outlook. Т.е. Ви одержите можливість єдиним образом працювати як з електронними листами, так і іншими електронними документами.

Однак якщо на підприємстві існують нижчеперелічені проблеми, простим сховищем документів не обійтися, і Вам варто всерйоз задуматися над автоматизацією робіт з документами й бізнес-процесами:

– Існує великий документопотік вхідних, вихідних і внутрішніх (службових) документів, розгляд яких серйозно збільшує строки виконання робіт.
– Нарад у керівників різного рівня стає більше і їхня тривалість затягається.
– Оперативність прийняття й виконання рішень низька й постійно знижується.
– Знаходження винних у порушенні виконавської дисципліни стає проблематичним.
– Кількість форм для звітності росте.
– Існує проблема витоку інформації й порушення комерційної таємниці.

Ігнорування вищезгаданих ситуацій або спроби вирішити ці завдання без допомоги автоматизованих програмних систем приведе до ще більшого збільшення проблем.

Функції сучасних СЕД

Системи автоматизації документообігу, пропоновані в цей час на ринках Україні й України, в основному, вітчизняних виробників або інтеграторів закордонного програмного забезпечення, зокрема, на платформі Lotus Notes/Domino від компанії IBM. Серед відомих СЕД українських постачальників можна назвати: Справа, Бос-референт, CompanyMedia, DIRECTUM, DOCUMENTUM, DocsVision, Євфрат-документообіг, Optima-Workflow, LanDocs, МОТИВ, Lotsia PDM Plus. З українських розроблювачів можна відзначити Атлас ДОК, Megapolis.Документообіг, ДОКА ПРОФ, АСКОД і FossDoc.

Функції, пропоновані СЕД своїм користувачам, досить різноманітні. У першому наближенні їх можна розділити на такі категорії:

– зберігання й пошук документів;
– підтримка канцелярії;
– маршрутизація й контроль виконання документів;
– аналітичні звіти;
– інформаційна безпека;
– додаткові (специфічні) функції.

Розглянемо коротко найбільш затребувані функції з перерахованих категорій:

Зберігання й пошук документів

Централізоване зберігання документів – чи не єдина мета переходу на електронний документообіг для маленьких компаній. У зв'язку із цим варто звернути увагу на постачальника сховища даних, використовуваного в тої або інший СЕД. Можуть використовуватися:

– сховища Lotus Notes/Domino (наприклад, Бос-референт, CompanyMedia);
– власні формати зберігання даних (Євфрат-документообіг);
– Microsoft SQL Server у різних редакціях (Справа, DIRECTUM, DocsVision, LanDocs і ін.);
– Oracle (Атлас ДОК, ДОКА ПРОФ і ін.);
– одночасна підтримка MS SQL і Oracle (Справу, Євфрат-документообіг, FossDoc і ін.);
– інші СУБД.

Серед функцій для пошуку документів розрізняють:

– пошук по атрибутах (полям) документів;
– пошук по вкладеним у документи файлам (повнотекстовий пошук);
– складний пошук (з використанням логічних операцій).

Підтримка канцелярії й діловодства

Підтримка роботи канцелярії – важливий компонент СЕД, орієнтованих на роботу, як у державних органах, так і в комерційних організаціях. До основного "канцелярським" функціям можна віднести наступне:

– подання документа у вигляді електронної картки – аналога реєстраційної картки документа;
– підтримка уведення документів у систему зі сканера;
– ведення номенклатури справ;
– реєстрація документів, у тому числі які надійшли по електронній пошті;
– повний цикл роботи із вхідними/вихідними документами;
– підтримка службових записок;
– робота зі зверненнями громадян;
– робота із заявками;
– ведення журналів реєстрації й обліку паперових оригіналів документів;
– підтримка ієрархічних довідників.

Маршрутизація й контроль виконання документів

Функції даної категорії затребувані як у великих, так і дрібних організаціях і дозволяють управляти документопотоками на підприємстві й контролювати виконання робіт з документів. До основних функцій даної категорії відносяться:

– проектування маршрутів документів з можливістю послідовно-паралельного їхнього виконання;
– підтримка різних дій над документами під час маршруту: візування, узгодження, накладення резолюції, підпис і т.п.;
– відправлення документів як по типовим, раніше спроектованим, так і по вільним, обумовленим користувачем у процесі виконання завдання, маршрутам;

– повідомлення співробітників про надходження до них на виконання нових документів;
– повідомлення про завершення етапів маршрутів;
– підтримка версійності документів (проектів документів);
– автоматичний контроль строків виконання документів.

Аналітичні звіти

Як правило, звіти в СЕД створюються під конкретного замовника. Однак існують і загальноприйняті звіти, такі як:
– звіт про поточну занятість співробітників;
– звіт про виконання робіт з документів (ретроспективний);
– звіт про прострочені доручення.

Інформаційна безпека

Функції даної категорії забезпечать інформаційну безпеку підприємства наступними засобами:
– автентифікація користувачів системи;
– розподіл прав доступу для співробітників-користувачів СЕД;
– підтримка електронного цифрового підпису документів;
– шифрування листів і документів;
– ведення історії й статистики роботи з документами;
– аудит роботи користувачів у системі.

Додаткові (специфічні) функції

Деякі розроблювачі СЕД пропонують ряд специфічних функцій, властивій тільки даній конкретній системі. Наприклад, Lotsia PDM Plus інтегрована із САПР-системами й підтримує роботу з конструкторською документацією. Система FossDoc може бути інтегрована з корпоративною поштовою системою FossMail того ж розроблювача. Цікаві також рішення, що пропонують інтеграцію з популярної ERP-системою 1С:Підприємство. Багато які СЕД надають власні API-інтерфейси для розробки нової функціональності "під замовника".

Критерії вибору системи документообігу

На нашу думку при виборі СЕД споживачам доводиться шукати компромісне рішення, по максимуму задовольняючим наступним критеріям:
– забезпечення необхідної функціональності з можливістю подальшої розширюваності системи;
– мінімальна сукупна вартість володіння й швидка окупність системи;
– достатній рівень технічної підтримки;
– виробник з реальними впровадженнями;
– облік вітчизняної законодавчої бази;
– суб'єктивні переваги замовника.

Розглянемо докладніше деякі з перерахованих вище критеріїв.

Забезпечення функціональності

В інтернеті можна знайти досить багато оглядів, присвячених порівнянню різних СЕД. Тому що більшість із цих оглядів складено за замовленням тих або інших розроблювачів, не варто занадто серйозно ставитися до виводів про те, що та або інша система по своєму функціоналі перевершує всі інші. У цей час усе ще формується загальноприйнята термінологія для позначення функціональності СЕД. Крім того, реалізація тих самих функцій, заявлених різними виробниками, може сильно відрізнятися.

Повна функціональність сучасних СЕД може зацікавити тільки великих корпоративних клієнтів або державних органів і навряд чи буде затребувана, наприклад, клієнтами від малого й середнього бізнесу. Тому перевага повинне бути зроблене постачальникам, що пропонують модульний принцип ліцензування системи. Ви вибираєте модулі, які призначені для рішення тільки Ваших завдань. Наприклад, системи на базі Lotus Notes/Domino у силу особливостей архітектури платформи Lotus забезпечують модульність

"за замовчуванням". Але й серед вітчизняних розробок є СЕД, що реалізують свої функції й ліцензуємі за модульним принципом. Так, наприклад, система FossDoc представлена лінійкою продуктів, що є набором модулів для рішення певних завдань документообігу й керування бізнес-процесами. Аналогічним образом ліцензуються системи DIRECTUM, LanDocs і ін.

Варто також звернути увагу на можливість додаткового нарощування функцій системи при подальшій експлуатації.

Сукупна вартість володіння

Як правило, у повну сукупну вартість володіння системою входять:

– вартість серверної частини, що реалізує бізнес-логікові системи;
– вартість клієнтських робочих місць;
– вартість сховища даних;
– вартість впровадження й технічної підтримки під час експлуатації;
– вартість продуктів сторонніх розроблювачів, інтегрованих з даною системою документообігу.
– вартість реалізації додаткових функцій ("під замовника").

Вартість сховища даних є вагомим чинником загального подорожчання системи. Так із цієї причини рішення на платформі Lotus відрізняються порівняно високою вартістю. Досить дорого будуть коштувати СЕД, що зберігають дані на Oracle, системі, використовуваної, як правило, у великих організаціях з високими вимогами до надійності й безпеки. Якщо Ви представник малого або середнього бізнесу, оптимальним рішенням для Вас можуть бути СЕД з підтримкою Microsoft SQL Server. Серед лінійки MS SQL Server є умовно безкоштовні сервіси, підтримувані деякими СЕД (Справа, FossDoc і ін.).

Техпідтримка

Якісна технічна підтримка припускає, що постачальник СЕД надає всі можливі засоби для всебічного вивчення роботи системи й надання послуг з консультування користувачів і оперативному усуненню замічених помилок. Компонентами ефективної техпідтримки є:

– безкоштовна (або умовно безкоштовна) демо-версія системи;
– демонстраційні й/або навчальні ролики по роботі користувачів із системою;
– докладна документація на продукт із локалізацією на рідну мову користувачів;
– форум технічної підтримки.
– Інші он-лайн сервіси й традиційна телефонна підтримка користувачів

Облік вітчизняного законодавства

При виборі СЕД для державних структур актуальною проблемою є відповідність системи законодавчій і нормативній базі. Наприклад, провайдери електронного цифрового підпису, використовувані в СЕД, повинні бути сертифіковані відповідними держорганами.

Для українських держструктур важливим моментом є повна українськомовна локалізація, як користувальницьких інтерфейсів, так і документації, включаючи можливість технічної підтримки державною мовою.

Суб'єктивні переваги замовника

Часто на практиці вирішальними факторами на користь вибору тої або іншої системи документообігу виявляються тяжкоформалізуємі, суб'єктивні переваги клієнта. Проте, можна вказати наступні розповсюджені переваги замовників при виборі СЕД:

– використання в бізнес-логіці СЕД термінології співпадаючої з термінологією існуючі на підприємстві паперового діловодства й документообігу;
– подібність користувальницького інтерфейсу СЕД на звичним, використовуваним замовником програмне забезпечення (наприклад, на поштовий клієнт);
– можливість інтеграції СЕД із програмним забезпеченням сторонніх виробників, що забезпечує критично важливі функції роботи підприємства.

У цей час на ринку програмного забезпечення України широко представлені системи для автоматизації діловодства, документообігу й інших бізнес-процесів підприємств і

установ. Для вибору СЕД для впровадження на підприємстві, рекомендуємо почати ряд наступних кроків:

– Зробіть порівняльний аналіз функціональності СЕД, що найбільше повно відповідають Вашим вимогам.

– Оцініте сукупну вартість володіння обраних Вами систем, зверніть увагу на вартість ПЗ сторонніх розроблювачів, необхідного для роботи СЕД.

– Вивчите схеми ліцензування, пропоновані постачальниками СЕД, і виберіть найбільш оптимальні для себе варіанти.

– Ознайомтеся з комплексом послуг з надання технічної підтримки, оцініте самого постачальника СЕД по заявленим їм впровадженням.

– Якщо є можливість – установите демо-версію системи, вивчите демонстраційні матеріали (відеоролики), пропоновані постачальниками СЕД.

– Виділите функціональні можливості аналізованих Вами систем, які є критично важливими з погляду законодавства, сумісності із установленим ПЗ, зручності роботи співробітників і т.п.

Остаточне рішення на користь вибору тієї або іншої системи документообігу може бути отримано, наприклад, шляхом середньозваженого аналізу оцінок, які Ви виставили вибраним СЕД за відповідність перерахованим критеріям.

Розробка структурної схеми

Організація моніторингу

У числі інших першочергових мір необхідно виділити ресурси й час на організацію процесу моніторингу. Системний моніторинг складається з декількох рівнів. У цій розділі розглядаються основні інструменти, використовувані в рамках цього процесу.

На верхньому рівні моніторингу здійснюється контроль впровадження в СЕД нових процесів. Допустимо, на старті проекту визначені ключові показники: які завдання має бути вирішувати, скільки користувачів буде працювати й скільки документів створюватися за рік. Виходячи із цього, вибирається певне встаткування, у якому, з урахуванням можливого розширення системи, передбачається певний «запас» продуктивності на випадок непередбаченого завантаження.

Подальший розвиток СЕД зажадає моніторингу навантаження на встаткування. Контроль за продуктивністю дозволить визначити, чи здатне наявне «залізо» підтримувати нові процеси. Якщо показники завантаження наближаються до 60-80%, то без відновлення встаткування автоматизувати нові завдання буде вкрай складно, тому що виникає ризик непрацездатності вже впроваджених процесів і зупинки системи.

В ідеалі такий сценарій розвитку подій варто взяти до уваги ще на нульовому етапі впровадження й реалізації системи. Навантаження на встаткування рекомендується вказувати в плані впровадження нових процесів на 1-3-5 років (або аналогічному документі).

На наступному рівні системного моніторингу необхідно відслідковувати поточні процеси:

– завантаження встаткування;

– тривалість виконання операцій користувачами, оскільки цей показник не завжди корелює із завантаженням устаткування (наприклад, навантаження на SQL-сервер можуть бути низкою, але робота користувачів утруднена внаслідок тривалих затримок через проблеми з каналами або конкретною робочою станцією);

– динаміку інцидентів.

Розглянемо кожний з них більш докладно й визначимо оптимальну періодичність і необхідні інструменти моніторингу.

Контроль завантаження встаткування

Якщо СЕД має клієнт-серверну архітектуру, як, наприклад, система DIRECTUM, то мова йде про відстеження тільки рівня завантаження серверної частини системи. Контроль завантаження встаткування на клієнтських місцях адміністратори здійснюють локально.

Ключове значення для досягнення необхідної продуктивності має SQL-сервер. Основними контрольованими показниками при моніторингу є наступні:

– Навантаження на ЦПУ. Відповідно до рекомендацій Microsoft, значення цього показника не повинне перевищувати 80%. Якщо ж постійне навантаження становить 60-80%, необхідно або оптимізувати процеси, або міняти встаткування.

– Навантаження на диски (IOPS). Microsoft рекомендує як ідеальні показники відсутність черги на дисках і відпрацьовування запиту до диска не більш ніж за 25 мс. В остаточному підсумку від часу виконання запиту залежить тривалість здійснення операції з погляду користувача.

– Блокування запитів. Вони теж впливають на тривалість виконання операцій у користувачів.

– Кеш планів запитів.

– Час знаходження сторінки в оперативній пам'яті.

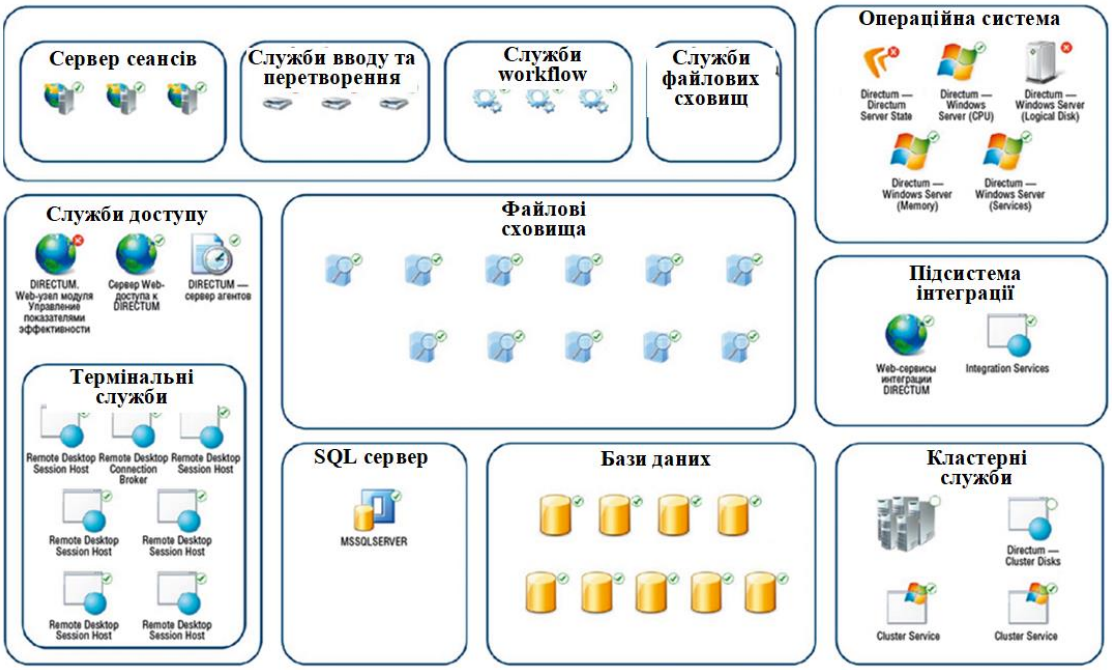


Рисунок 1 – Структурна схема системи

Інші показники вже не так явно позначаються на тривалості виконання операцій і не так швидко змінюються, тому їх можна аналізувати рідше.

При організації моніторингу серверної частини не можна забувати про «слона» – про працездатність сервісних служб. Якщо звернутися до приклада DIRECTUM, то в цій системі використовується безліч подібних служб: сервіс інтеграції (DISI), сервіс захвату й перетворення (DCTS), workflow, сервер сеансів. SQL-сервер у даному контексті теж є службою. Рекомендується відслідковувати роботу всіх наявних служб.

Які інструменти використовуються:

– SCOM, Zabbix або аналоги;

– лічильники Windows Server для контролю показників сервера за тривалий період і відстеження їхньої динаміки;

– інструменти SQL-сервера;

– інструменти центру адміністрування DIRECTUM для моніторингу служб.

Періодичність контролю:

– Навантаження на диски й процесор бажано відслідковувати постійно. За допомогою SCOM можна настроїти граничні значення, при досягненні яких адміністратор одержить оповіщення.

– Загальний контроль працездатності служб на рівні системи теж здійснюється постійно – за допомогою оповіщень SCOM. У ході моніторингу на основі емпіричних даних для кожного сервера встановлюється максимально припустиме навантаження за одиницю часу. Виходячи із цього, обчислюється границя, при досягненні якої буде потрібно приймати які-небудь міри. Якщо навантаження довго тримається на граничному рівні, команда супроводу повинна розглянути можливість заміни встаткування.

– Динаміку зміни навантаження на серверну частину необхідно фіксувати один раз на місяць і один раз у квартал. Для виявлення причин відхилення варто встановити, що змінилося усередині системи: кількість підтримуваних користувачів, інтенсивність їхньої роботи, впровадження нових рішень. Накопичуючи й аналізуючи таку інформацію, можна заздалегідь прогнозувати, які наслідки будуть мати ті або інші зміни.

Контроль тривалості операцій

У системі виконується безліч операцій: збереження карток документів, відправлення завдань, формування звітів, відкриття записів довідників і т.д. На етапі формування вимог визначається типова тривалість виконання кожної операції, що потім контролюються. Цей показник важливий для команди супроводу, тому що від нього залежить загальне враження користувача про систему нарівні зі зручністю інтерфейсу.

Інструменти моніторингу. Моніторинг здійснюється за допомогою засобів користувальницького профілювання (профайлингу), а також (частково) журнальних файлів системи, де фіксується час виконання конкретних операцій. Потім інформація із всіх користувачів агрегується й аналізується.

Класифікація інформації й аналіз. У великих компаніях накопичується великий обсяг даних, що дозволяє робити репрезентативні прогнози на основі середніх значень. Тому в першу чергу варто виділити однотипні операції й обчислити середнє значення. Це дозволяє зробити вивід про те, наскільки задовільно працює система при виконанні тих або інших операцій, і зрозуміти, як вплинули зміни конкретного процесу на його середню тривалість.

Потім складається список самих тривалих операцій – перших кандидатів на оптимізацію. Далі виявляються користувачі, у яких система працює більш повільно, ніж в інших. Роботу конкретного користувача можуть утрудняти зовнішні перешкоди, слабкий ПК, віруси, погано настроєна мережа. У кожному разі профайлинг допоможе вирішувати такі проблеми проактивно й усувати їх ще до надходження скарг у службу підтримки.

Крім класифікації по видах операцій, необхідна класифікація груп користувачів по бізнес-ролям. Приміром, діловоди переважно працюють із довідниками й документами, а керівники – із завданнями. Від особливостей роботи користувача залежить, які операції будуть найбільш критичними для виконання його ролі в системі – їх варто контролювати в першу чергу.

Крім того, можна виділити групи користувачів, які часто виконують ту саму операцію. Це дозволяє визначити пріоритети для оптимізації. Крім цього, відстеження тривалості операцій по бізнес-ролям допомагає виявити ситуацію, коли кінцевий користувач працює із системою не так, як рекомендовано. Це може стати приводом для навчання його оптимальному способу виконання тої або іншої операції.

У профайлингу, крім іншого, утримується інформація про роботу служб DIRECTUM. Фіксація відхилень від рекомендується тривалості виконання операцій допоможе виявити помилки в прикладній розробці й поліпшити функціонування служби.

Періодичність контролю. У випадку профайлингу мова йде про обробку дуже великого обсягу інформації, тому постійний моніторинг неможливий. У зв'язку із цим рекомендується один раз у тиждень аналізувати список тривалих операцій, щомісяця здійснювати повний профайлинг по всіх перерахованих зрізах і щокварталу відслідковувати динаміку.

Контроль динаміки інцидентів

У випадку виникнення інцидентів моніторинг здійснюється по декількох напрямках. У першу чергу варто проаналізувати журнальні файли системи. Збирати їх треба централізовано й потім обробляти за допомогою автоматичних інструментів.

Деякі помилки фіксуються в журналах у фоновому режимі й не вимагають якихось дій з боку користувача, але впливають на тривалість виконання операцій. Завдання полягає в тім, щоб відслідковувати ті помилки, які виникають досить часто й можуть критичним образом вплинути на роботу системи. У випадку разових помилок, що відбуваються приблизно в те саме час у великої кількості користувачів, необхідне втручання команди супроводу. Це ж стосується великої кількості однотипних помилок, що з'являються протягом короткого проміжку часу. Крім того, варто контролювати обсяг файлів з журналами – як правило, його помітне збільшення вказує на наявність якоїсь проблеми.

На етапі супроводу системи в службу Service Desk надходять обігу користувачів. Їх можна класифікувати в такий спосіб:

– Обігу, пов'язані із тривалістю операцій. Ця інформація аналізується разом з результатами профайлингу.

– Безпосередньо інциденти. У цьому випадку обчислюються середні значення їхньої частоти (кількість за день), які рівняються із цільовим показником. Якщо в ході розвитку СЕД відзначається ріст числа інцидентів по одному компоненті або бізнес-процесу, виходить, останні доробки могли вплинути й потрібно оптимізувати роботу системи.

Проаналізувавши характер звернень, можна виділити проблемні компоненти й «проблемних» користувачів, а також об'єднати інциденти по місцю виникнення (відділ, філія, будинок). Маючи таку інформацію, простіше з'ясувати першоджерело проблем, що не завжди очевидний при реактивній роботі з зверненнями. Користувачі можуть зштовхнутися з однієї й тією же помилкою при виконанні різних операцій і по-різному їх описати. Класифікація дасть можливість дозволити тисячу інцидентів у тисячі користувачів шляхом усунення загальної для них проблеми.

Отже, існують два підходи до підтримки й супроводу системи. Виниклі проблеми можна вирішувати в міру надходження (реактивно) або пророкувати й попереджати їх за допомогою описаних інструментів (проактивно). Другий підхід дозволить зменшити кількість позаштатних ситуацій, нагромадити історичні дані й спрогнозувати, як буде поводитися система при тих або інших змінах. Проактивний підхід більше ефективний у довгостроковій перспективі й може бути реалізований за допомогою доступних засобів.

Висновок. У статті розглянуто та проаналізовано програмне забезпечення, створене в результаті виконання роботи, призначено для проактивного системного моніторингу СЕД. В межах України в недостатній мірі представлені вітчизняні розробки в цій області. У роботі наведені теоретичне узагальнення й рішення наукового завдання дослідження методів проактивного системного моніторингу СЕД. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем проактивного системного моніторингу СЕД; Досліджена система проактивного системного моніторингу СЕД; На основі отриманих результатів досліджень створена програмна реалізація проактивного системного моніторингу СЕД. Розроблені під час виконання роботи алгоритми дозволяють успішно вирішувати завдання проактивного системного моніторингу СЕД. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки. Розроблене програмне забезпечення має простий, дружній та зручний інтерфейс користувача, що забезпечує легкість у освоєнні роботи програмного продукту, зручність у використанні, і не потребує особливих спеціальних знань. При створені програмного забезпечення було використано об’єктно-орієнтований підхід, що відповідає сучасним тенденціям у галузі розробки комерційних програмних систем. Програма реалізована на мові високого рівня Visual C++. Дана мова програмування дозволяє найбільш ефективно обробляти дані. Це дозволило мінімізувати строк розробки програмного забезпечення, і, як слід, зменшити витрати на його розробку.

Запропоноване програмне забезпечення ділиться на загальне програмне забезпечення, що поставляється із засобами обчислювальної техніки й спеціальне програмне забезпечення, що спеціально розроблене для даної конкретної системи й включає програми, що реалізують її функції. Програма призначена для виконання під управлінням багатозадачної операційної системи Windows XP/Vista/7/8/10. Даються необхідні рекомендації з установки розробленого програмного забезпечення. Для підвищення рівня безпеки запропоновано застосовувати алгоритм RSA.

Список літератури

1. Коваленко А.С. Разработка структуры базы данных интегрированной информационной системы / А.С. Коваленко, А.В. Коваленко // Информационные технологии и защита информации в информационно-коммуникационных системах: монографія / Под редакцией профессора В.С. Пономаренко. – Х.: Вид-во ТОВ «Щедра садиба плюс», 2015. – С. 54-64.
2. Кожанова А.С. Обґрунтування необхідності створення систем технічної діагностики інтегрованих інформаційних систем / О.А. Смірнов, А.С. Кожанова, О.В. Коваленко // Системи обробки інформації. – Х.: ХУПС, 2013. – Вип. 6(113). – С. 255-257.
3. Коваленко А.С. Задачи распознавания ситуаций в ERP системах / А.В. Коваленко ., А.А. Смірнов, А.С. Коваленко // Системи обробки інформації. – Х.: ХУПС, 2014. – Вип. 4(120). – С. 161-164.
4. Коваленко А.С. Підсистема технічної діагностики для автоматизації процесів керування в інтегрованих інформаційних системах / А.С. Коваленко , О.А.Смірнов, О.В. Коваленко // Системи озброєння і військова техніка.– Х.: ХУПС, 2014. – № 1(37). – С. 126-129.
5. Коваленко А.С. Анализ эффективности использования экспертной системы технической диагностики с традиционной структурой / А.С. Коваленко, А.А. Смирнов, А.В. Коваленко // Системи озброєння і військова техніка. – Х.: ХУПС, 2014. – № 2(38). – С. 106-108.
6. Коваленко А.С. Разработка структуры экспертной системы технической диагностики интегрированной информационной системы / А.С. Коваленко, А.А. Смирнов, А.В. Коваленко // Наука і техніка Повітряних Сил Збройних Сил України. – Харків: ХУПС, 2014. – № 2(15). – С.154-157.
7. Коваленко А.С. Разработка структуры экспертной системы технической диагностики интегрированной информационной системы / А.С. Коваленко, А.А. Смирнов, А.В. Коваленко // Наука і техніка Повітряних Сил Збройних Сил України. – Харків: ХУПС, 2014. – № 2(15). – С.154-157.
8. Коваленко А.С. Структура системи технічної діагностики інтегрованих інформаційних систем / А.С. Коваленко, О.А. Смірнов, О.В. Коваленко // Збірник наукових праць Кіровоградського національного технічного університету / техніка в сільськогосподарському виробництві, галузеве машинобудування, автоматизація. – Кіровоград: Вид-во КНТУ, 2014. – Вип. 27. – С. 245-251.
9. Коваленко А.С. Дослідження будови інтегрованої інформаційної системи та її елементів / А.С. Коваленко, О.А. Смірнов, О.В. Коваленко // Системи озброєння і військова техніка. – Х.: ХУПС, 2014. – № 4(40). – С. 85-88.
10. Коваленко А.С. Розробка структури бази даних для обліку технічного стану елементів інтегрованої інформаційної системи з урахуванням вимог споживачів інформації / А.С. Коваленко, О.А. Смірнов, О.В. Коваленко // Системи обробки інформації. – Х.: ХУПС, 2015. – Вип. 1(126). – С. 75-79.

УДК 657

Л. Непорожнева, магістр гр. ООУ-18МЗ-1,9
І. Смірнова, канд. екон. наук, доцент
Центральноукраїнський національний технічний університет

ВПЛИВ ЕЛЕМЕНТІВ ОБЛІКОВОЇ ПОЛІТИКИ НА ФОРМУВАННЯ ФІНАНСОВОЇ ЗВІТНОСТІ БЮДЖЕТНИХ УСТАНОВ

Стаття присвячена дослідженню впливу елементів облікової політики на показники фінансової звітності бюджетних установ. У статті зясовано склад елементів облікової політики бюджетних установ, що чинять вплив на показники фінансової звітності. Запропоновано їх групування за трьома ознаками залежно від ступеня впливу. Проаналізовано вплив складових, що найбільше впливають на показники фінансової звітності бюджетних установ
бухгалтерський облік, облікова політика, фінансова звітність, податкова звітність, бюджетна установа, активи, зобов'язання, капітал

Статья посвящена исследованию влияния элементов учетной политики на показатели финансовой отчетности бюджетных учреждений. В статье выяснено состав элементов учетной политики бюджетных учреждений, оказывающих влияние на показатели финансовой отчетности. Предложено их группировки по трем признакам в зависимости от степени воздействия. Проанализировано влияние составляющих, больше всего влияют на показатели финансовой отчетности бюджетных учреждений
бухгалтерский учет, учетная политика, финансовая отчетность, налоговая отчетность, бюджетное учреждение, активы, обязательства, капитал

Постановка проблеми. Облікова політика підприємства, установи чи організації є важливим засобом формування основних показників діяльності, оскільки вона має істотний вплив на показники прибутку, податків, показники фінансового стану. Облікова політика може виступати інструментом управління витратами, фінансовими результатами, що впливає на значення показників звітності та фінансові коефіцієнти; інструментом управління нарахованими податками; дієвим інструментом практичного вирішення протиріч нормативних актів з бухгалтерського обліку та оподаткування; інструментом уніфікації облікових процедур і зниження їх трудомісткості; інструментом реалізації базових принципів МСФЗ – безперервності діяльності та методу нарахування.

Інтеграція України до Європейського економічного простору вимагає адаптації нормативної бази України, у тому числі з питань бухгалтерського обліку, до європейських та міжнародних норм. У бюджетній сфері адаптація бухгалтерського обліку до міжнародних норм відбувається на підставі Стратегії модернізації системи бухгалтерського обліку в державному секторі, на виконання якої затверджено відповідні Національні положення (стандарти) бухгалтерського обліку в державному секторі (НП(С)БОДС), які узгоджені з відповідними Міжнародними стандартами в державному секторі (МСБОДС), що сприяє розумінню національної фінансової звітності установ державного сектору не лише резидентами, а й нерезидентами.

Перехід на ведення бухгалтерського обліку суб'єктами бухгалтерського обліку в державному секторі за НП(С)БОДС вимагає нових підходів як до його організації, так і до формування облікової та інших політик, а також складання звітності.

Аналіз останніх досліджень і публікацій. Загальні проблеми формування облікової політики господарюючих суб'єктів розглядались у працях Ф.Ф. Бутинця, Б.І. Валуєва, А.М. Герасимовича, С.Ф. Голова, Н.М. Малюги, М.С. Пушкаря, Я.В. Соколова, В.В. Сопко, Н.М. Ткаченко, В.Г. Швеця та інших.

Дослідження з удосконалення бухгалтерського обліку в бюджетній сфері проводили такі вітчизняні науковці: О.О. Дорошенко, Т.В. Канєва, Н.А. Лиско, С.В. Свірко, Н.І. Сушко, Н.М. Хорунжак, О.О. Чечуліна.

Проблеми методики складання звітності бюджетних установ висвітлено в працях багатьох вітчизняних науковців облікової сфери діяльності бюджетних установ та державного сектору економіки. Зокрема, можна виділити провідних науковців таких, як: Лень В.С., Свірко С.В., Хорунжак Н.М., Лучко М.Р., Штимер Л.Т., Сушко Н.І. Попри різносторонній розгляд звітності та взяття за основу авторських позицій різних її характеристик науковці й практики єдині в думці про те, що це надзвичайно важлива складова загальної інформаційної бази прийняття управлінських рішень, формування якої в сучасних умовах супроводжується низкою проблем.

Проте питання впливу облікової політики на показники фінансової та податкової звітності бюджетних установ досліджені ними недостатньо і потребують подальших напрацювань.

Постановка завдання. Мета написання статті полягає в дослідженні питань впливу облікової політики на показники фінансової та податкової звітності бюджетних установ.

Виклад основного матеріалу. Вибір елементів облікової політики обумовлює вплив на показники усіх форм фінансової звітності. Це обумовлено тим, що кожен із обраних підприємством, установою чи організацією способів обліку чи оцінки прямо або опосередковано впливає на вартість активів, зобов'язань, власного капіталу та/або розмір доходів, витрат і фінансових результатів, які відображаються у різних формах фінансової звітності підприємства, установи чи організації.

Умови ринкових відносин передбачають наявність альтернатив щодо вибору напрямів розвитку, обсягів діяльності, ресурсів, джерел фінансування, форм і способів інвестицій тощо. Всі ці управлінські рішення пов'язані з поняттям «політика». У господарській практиці широко розповсюдженими є такі поняття, як економічна, технічна, соціальна, фінансова, податкова політика тощо.

Облікова політика – одне з найважливіших питань організації бухгалтерського обліку, правильне формування якого і повне розкриття забезпечує реалізацію мети бухгалтерського обліку і фінансової звітності: надання користувачам для прийняття рішень повної, правдивої та неупередженої інформації про фінансовий стан, результати діяльності та рух грошових коштів підприємства.

Користувачі фінансової звітності мають право і повинні бути поінформованими щодо застосованих методів і процедур, оскільки альтернативні їх варіанти суттєво змінюють показники фінансової звітності підприємства, установи чи організації. З огляду на це, Міжнародним стандартом бухгалтерського обліку 1 (п.7) [5], а також стандартами GAAP вимагається подання облікової політики, як окремого компонента повного комплекту фінансових звітів.

Нажаль, зазначені вимоги не реалізуються на практиці. У кращому випадку, на підприємствах, установах чи організаціях складається Наказ про облікову політику, інформація якого ніяким чином не представлена у фінансовій звітності. Причиною тому є недостатня увага до цього питання з боку регламентуючих органів, а також неузгодженість нормативних документів, що стосуються облікової політики.

Вимога щодо подання інформації про облікову політику у фінансовій звітності національних підприємств, установ та організацій є декларативною, оскільки склад та форми фінансової звітності в Україні суворо регламентовані і в них не відведено місця для облікової політики.

Слід зауважити, що створення облікової політики в бюджетній установі – дуже трудомісткий і відповідальний процес. Адже установі доведеться не один рік працювати і обліковувати свої активи, зобов’язання, доходи і видатки згідно з розробленою обліковою політикою. Це вимагає більш зваженого підходу до розробки облікової політики, яка відповідає специфіці діяльності.

Тож, деякі науковці, як-то Павло Житний [2], вважають, що при розробці облікової політики необхідно керуватися не тільки специфічними, властивими бухгалтерському обліку принципами, а й загальними організаційно-управлінськими, які впливають на вибір істотних чинників і характеризують зв'язки внутрішніх господарських процесів із зовнішнім середовищем. Таким чином, уміння фахівців пристосовуватися до змін зовнішніх і внутрішніх (організаційно-технологічних) чинників є гарантією формування облікової політики, здатної забезпечити не тільки виживання, а й послідовний розвиток підприємства, установи чи організації.

На жаль, як справедливо наголошується в економічних дослідженнях, керівництво підприємств, установ та організацій не приділяє належної уваги процесу формування облікової політики. Основною причиною такої ситуації є те, що в Україні ще не сформувалися стійкі фінансові та товарні ринки, а також їх інфраструктура, основними елементами якої є біржі, аукціони, кредитна та емісійна системи, інформаційні технології й засоби ділової комунікації, система страхування комерційного ризику, спеціальні зони вільного підприємництва тощо. Поступово долається спад промислового виробництва, налагоджуються виробничі та комерційні зв'язки, накреслюються шляхи стратегічного розвитку. Це відбувається в умовах гострого дефіциту фінансових і матеріальних ресурсів, що особливо відчутно у бюджетній сфері.

Поряд з цим відбуваються процеси становлення нового економічного мислення, нової етики управління, адаптації бухгалтерського обліку до реалій господарювання, наближення його до світової облікової практики та умов ринкової економіки. Відсутність достатнього досвіду роботи у новому економічному середовищі негативно позначається на процесах формування та представлення облікової політики. Ця проблема в сучасних умовах господарювання підприємств є досить гострою.

Підприємства, установи та організації мають висвітлювати свою облікову політику шляхом опису принципів оцінки та методів обліку щодо окремих статей звітності.

Наказ про облікову політику – внутрішній нормативний документ з організації та порядку ведення обліку, який містить сукупність способів та процедур організації і ведення обліку, що використовуються з метою підготовки, складання та подання фінансової звітності.

На відміну від форм організації бухгалтерського обліку, які можуть змінюватися щороку, облікова політика розробляється та затверджується на тривалу перспективу.

Розпорядчим документом, яким встановлюється або уточнюється облікова політика, є Наказ про облікову політику. Саме цей документ містить опис методів оцінок, які будуть використані підприємством, установою чи організацією при складанні фінансових звітів, а також викладення конкретних аспектів облікової політики щодо окремих об'єктів і статей обліку.

Загалом, вплив елементів облікової політики на показники фінансової звітності підприємства проявляється по-різному:

- через вартість активів і зобов'язань обрані підприємством елементи облікової політики впливають на показники Балансу та Приміток до річної фінансової звітності;

- через розмір доходів, витрат, і як наслідок фінансових результатів (чистий прибуток та нерозподілений прибуток) обрані підприємством елементи облікової політики впливають на показники Балансу, Звіту про фінансові результати, Звіту про власний капітал та Приміток до річної фінансової звітності.

Враховуючи напрацювання авторів наукових публікацій з проблем формування ефективної облікової політики організації [1, 3, 4], всі елементи облікової політики рекомендуємо класифікувати за трьома групами з урахуванням суттєвості впливу на фінансові результати і аналітичні показники фінансової звітності:

1) елементи, що не здійснюють впливу на фінансові результати і аналітичні показники звітності;

2) елементи, за якими неможливо дати однозначну оцінку впливу;

3) елементи з ймовірним впливом на аналітичні показники звітності і фінансові результати, які, в свою чергу, поділяємо на: елементи облікової політики з довгостроковим періодом впливу (більше 12 міс.) та елементи облікової політики з короткостроковим періодом впливу (менше 12 міс.).

Класифікацію елементів облікової політики з урахуванням суттєвості впливу на фінансові результати і аналітичні показники фінансової звітності представлено на рис. 1.

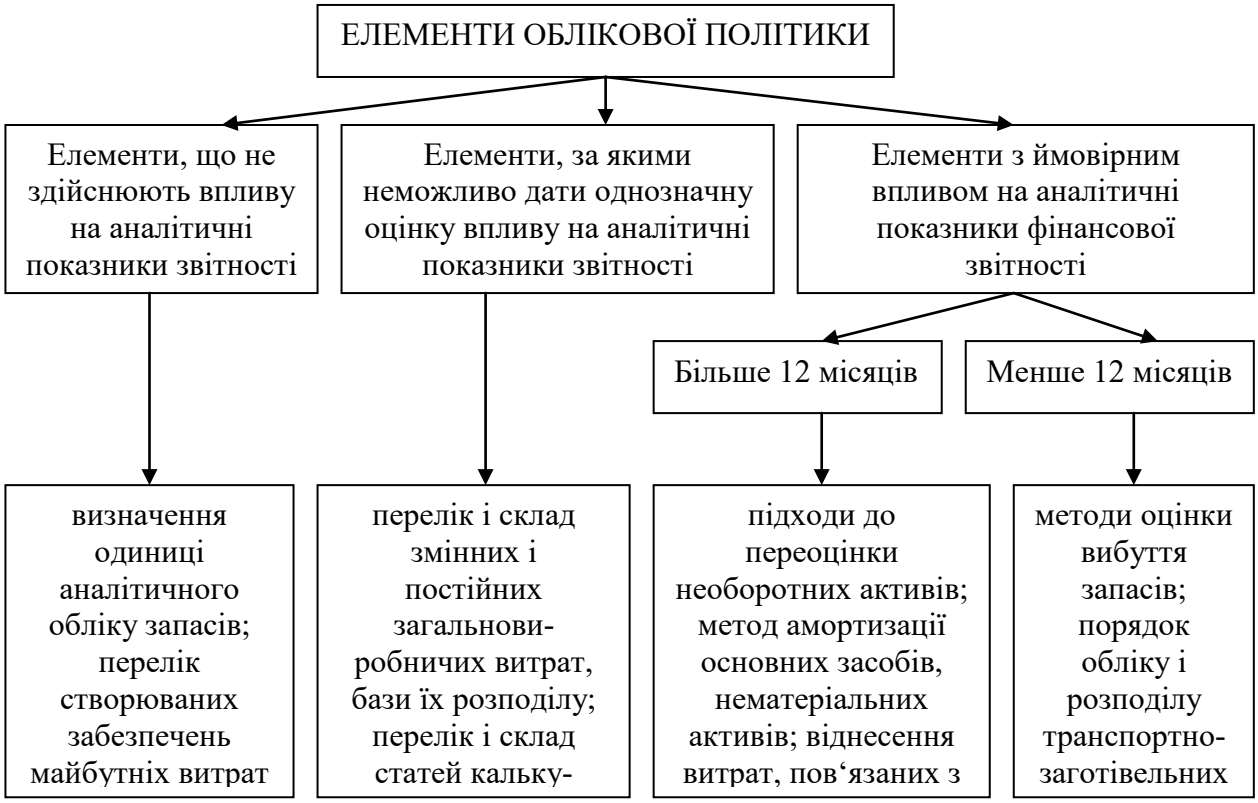


Рисунок 1 - Класифікація елементів облікової політики за ступенем впливу на показники фінансової звітності

До елементів облікової політики, що найбільше впливають на показники фінансової звітності, слід віднести: модель оцінки основних засобів (за первісною вартістю або за переоціненою вартістю), визначення методу оцінки вибуття запасів; визначення методу нарахування амортизації (прямолінійний, виробничий або прискорене списання).

Про суб‘єктивність облікової політики та її здатність впливати на прибуток підприємства відзначалося у працях прихильників соціологічного підходу до обліку, які вважали, що відносність звітних даних є наслідком ліберальності менеджменту суб‘єкта господарювання та відносності оцінок вартості вибуття активів.

В результаті проведеної переоцінки основних засобів до справедливої вартості змінюється, і значно, фінансовий результат до оподаткування. Дооцінка об'єктів основних засобів призводить до збільшення їх залишкової вартості і, відповідно, до збільшення амортизації. Уцінка веде до зниження амортизації, зменшення витрат і збільшення прибутку.

Відтак, фінансовий результат до оподаткування збільшується на суму уцінки основних засобів, включеної до витрат звітного періоду, та зменшується на суму дооцінки основних засобів. Об'єктами впливу даного елемента облікової політики є собівартість, інші витрати операційної діяльності, капітал у дооцінках, а отже, валюта балансу і вартість активів. В разі переоцінки змінюється величина першого розділу активу балансу, відтак ця зміна вплине на такий показник ділової активності підприємства як фондовіддача. Дооцінка призведе до збільшення величини чистих активів, коефіцієнта фінансової стійкості, коефіцієнта автономії і зменшення таких показників, як рентабельність продажів, рентабельність власного капіталу, рентабельність активів, фондовіддача, капіталовіддача.

Значний вплив на аналітичні показники фінансової звітності має вибір методів оцінки вибуття запасів. Так, метод ФІФО завищує фінансові результати, адже при його застосуванні занижується собівартість внаслідок списання запасів за нижчими «першими» цінами. З точки зору розрахунку показників платоспроможності, метод ФІФО – це найкращий варіант оцінки вибуття запасів, проте він, зазвичай, веде до збільшення податку на прибуток. При виборі способу нарахування амортизації необоротних активів бухгалтеру важливо врахувати, що застосування прискорених методів амортизації збільшить коефіцієнт поточної ліквідності, коефіцієнт забезпеченості власними оборотним капіталом і фондовіддачу, і зменшення, в свою чергу, таких показників як рентабельність продажів, рентабельність активів.

Висновки та перспективи подальших досліджень. Для того, щоб облікова політика стала не формальним атрибутом облікового механізму, а інформативною базою для прийняття управлінських рішень, необхідно провести аналіз умов господарювання підприємства, установи чи організації, їх організаційної структури; проаналізувати фактичний стан бухгалтерського обліку та системи внутрішнього контролю; та визначити мету формування ефективної облікової політики. Виходячи із суттєвого впливу облікової політики на фінансову звітність підприємства, установи чи організації, в основу вибору елементів облікової політики має бути покладена обрана ними стратегія.

Перспективи подальших досліджень полягають у розробці методичних рекомендацій з формування облікової політики бюджетних установ в розрізі облікових обєктів залежно від їх впливу на показники фінансової звітності.

Список літератури

1. Верига, Ю. А. Облікова політика підприємства: навч. посіб. / Верига Ю. А., Кулик В. А., Ночовна Ю. О., Іванюк С. Ю. — Полтава: ПУЕТ «ЦУЛ», 2015. — 310 с.
2. Житний П.Є. Облікова політика в умовах розвитку фінансово-промислових систем: методологія та організація: монографія / П.Є. Житний. - К.:Луганськ: Вид-во СНУ ім. В. Даля, 2007. - 352 с.
3. Кругляк, З. И. Влияние отдельных элементов учетной политики на статьи отчетности и показатели финансового состояния / З. И. Кругляк // Научный журнал КубГАУ. – 2014. –№101(07).
4. Макарова, Н. Н. Анализ подходов к формированию учетной политики / Н. Н. Макарова // Аудит и финансовый анализ. – 2009. – № 3.
5. Міжнародний стандарт бухгалтерського обліку в державному секторі 1 “Подання фінансових звітів” [Електронний ресурс]. – Режим доступу: www.minfin.gov.ua/document/81047/1a.pdf.

УДК 004

С. Нестеренко, магістр гр. КІ-18М-1,4
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ ХМАРНОГО КЕРУВАННЯ ПРИСТРОЯМИ КОМПЛЕКСУ «РОЗУМНИЙ ДІМ»

У статті розроблено програмне забезпечення, яке призначено для хмарного керування розумним будинком. Метою розробки є дослідження та програмна реалізація системи хмарного керування розумним будинком. Об’єктом дослідження є процес забезпечення хмарного керування «розумним будинком». Предметом дослідження є методи забезпечення хмарного керування системами розумного будинку. Методи дослідження базуються на методах теорії кодування, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи хмарного керування розумним будинком. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних

засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення. Розроблено зручний інтерфейс користувача. Наведені інструкції по роботі з програмними засобами.
комп'ютерна інженерія, IoT, MQTT, smart house

Постановка проблеми. Протягом останнього десятиліття ми всі стали звикати керувати аспектами нашого життя за допомогою технологій, від інтернет-банкінгу до онлайн-магазинів, інтернет зробив життя набагато зручнішим. Зараз подібна інтелектуальна революція відбувається в домашніх умовах. Розумний дім - це той, де практично будь-який аспект можна контролювати цифровим способом. Ваш дверний дзвінок, ваше освітлення, Ваша домашня безпека, опалення та вода, все, навіть керування шторами, можна контролювати дистанційно завдяки технологіям.

Розумні технології роблять роботу у будинку набагато простішою та зручною, і можуть дати Вам душевний спокій, що все працює так, як потрібно, навіть якщо ви перебуваєте далеко протягом тривалого часу. Розумні технології спрощують роботу у домі, зменшуючи необхідність дротів та пультів для керування телевізорами та музикою. Деякі технології розумного будинку зосереджені більше на безпеці - інтегрована система розумного спостереження для дому може дозволити Вам стежити за тим, що відбувається, де б ви не були. Ви також можете придбати системи, які зберігають ваш будинок в безпеці від пожежі та ризиків затоплення. Розумний будинок дає вам змогу краще контролювати і знати більше про те, що відбувається з вашим будинком.

Технологія розумного дому може бути представлена у вашому будинку по частинах, відповідно до ваших приорітетів. Якщо відкриття штор силою вашого голосу є вашим приорітетом, то ви можете почати тільки з цього! Однак цей крок все більше спрямований на інтегровану технологію, яка з'єднує різні елементи вашого будинку в одному центрі.

Концепція smart home поступово формувалася в США починаючи з 50-х років 20 сторіччя. Основою метою тоді було створення системи, принцип дії якої був присутній лише в фантастичних книжках – вона повинна була самостійно керувати життєвими процесами в будинку. Це була, в першу чергу, «система комфорту» для заможних американців. У 70-х роках Вашингтонський інститут інтелектуального будинку сформував остаточне тлумачення терміну smart home. Вчені вкладали у нього наступне: можливість класифікації різноманітних ситуацій в помешканні та адаптація й самостійне прийняття рішень щодо адекватного реагування на кожну з них. Плюс тотальний контроль над не тільки усією екосистемою будинку, а ще й над іншими самостійними системами. Інше кажучи, «система комфорту» повинна була бути головною та єдиною. Концепція отримала дуже велику підтримку – як соціальну, так і фінансову. Численні компанії з великою наснагою взялися експериментувати з кабелями та електрикою, щоб створити пристрій здатний, скажімо, самостійно вмикати чи вимикати світло, в залежності від присутності людини в кімнаті. З хаосу ідей та експериментів, у 1975 році виринув перший універсальний стандарт для створення елементарної автоматизованої домашньої системи, під назвою X10. Авторами інноваційної технології були спеціалісти шотландської компанії Pico Electronics. Забігаючи вперед, підкреслимо, що X10 виявився дуже вдалим – він продовжує використовуватися і в наш час. Не втрачаючи місяці марно, талановиті шотландські інженери заснували компанію X10 USA, з якою вийшли на американський ринок. Вже у 1978 році, в тандемі з фірмою Leviton, ними був створений повністю робочий механізм автоматизованого керування домашньою побутовою технікою за допомогою звичайної електромережі. Це був прорив. Саме тому, 1978 рік прийнято вважати знаковим у історії розвитку «розумного будинку». З нього починається етап бурхливого розквіту smart-технологій. З'являються прототипи альтернативних технологій EIB (пізніше KNX), протоколи IEC61158, LonTalk та інше. За майже сорок років, технології «розумного будинку» зробили феноменальний ривок у розвитку та стали доступні кожному талановитому інженеру. Створено безліч автоматичних систем контролю за кліматом, електрикою, опаленням, безпекою у помешканні тощо. І це

вже не кажучи про різноманітні індивідуальні smart-ґаджети, які також є частиною інноваційної екосистеми.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи хмарного керування пристроями комплексу «розумний дім».

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи хмарного керування пристроями комплексу рішень «розумний дім».

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем хмарного керування комплексами «розумний дім»
– Дослідження системи систем хмарного керування розумним будинком.
– Програмна реалізація системи хмарного керування розумним будинком.

Об'єктом дослідження є процес хмарного керування розумним будинком.

Предметом дослідження є методи реалізації систем хмарного керування розумним будинком.

Методи дослідження базуються на методах теорії кодування,методах захисту інформації, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Виходячи з теми магістерської роботи потрібно розробити програмне забезпечення системи хмарного керування «Розумний дім» та розробити саму автоматизовану систему управління з встановленням необхідних датчиків та систем.

Устаткування для розумного будинку

Спершу поговоримо про те, як зі звичайної квартири, дачі або котеджу зробити розумний будинок. Для цього, як правило, потрібно розмістити в житло наступне обладнання:

- датчики, які вимірюють різні параметри зовнішнього середовища;
- виконавчі пристрої, які впливають на зовнішні об'єкти;
- контролер, що виробляє обчислення відповідно до вимірами датчиків і закладеної логікою, і видає команди для виконавчих пристроїв.

На наступному малюнку показана схема розумного будинку, на якій розташовані датчики протікання води (1) у ванній, температури (2) і освітлення (3) в спальні, розумна розетка (4) на кухні і камера відеоспостереження (5) в передпокої.

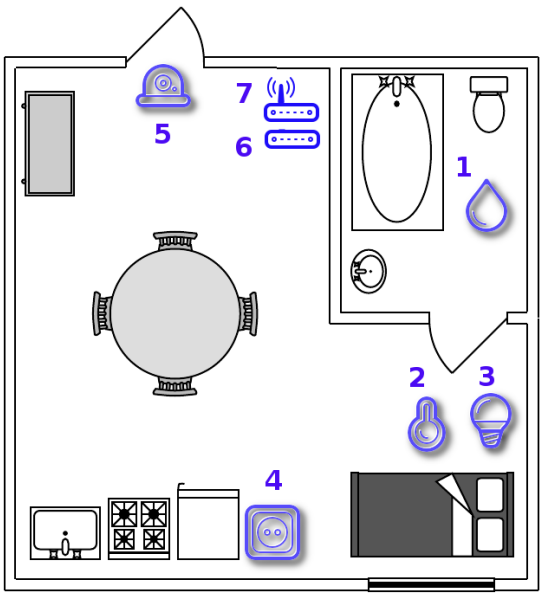


Рисунок 1 - Обладнання «розумного будинку»

Датчики

В даний час широкого поширення набули бездротові датчики, що працюють по протоколах RF433, Z-Wave, ZigBee, Bluetooth і WiFi. Їх головні переваги - зручність монтажу і використання, а також дешевизна і надійність, тому що виробники прагнуть вивести свої пристрої на масовий ринок і зробити їх доступними пересічному користувачеві.

Датчики та виконавчі пристрої, як правило, підключаються по бездротовому інтерфейсу до контролера розумного будинку (6) - спеціалізованому мікрокомп'ютеру, об'єднуючого всі ці пристрої в єдину мережу і керуючому ними. Втім, деякі рішення можуть поєднувати в собі датчик, виконавчий пристрій і контролер одночасно. Наприклад, розумна розетка може бути запрограмована на включення або вимикання за розкладом, а камера хмарного відеоспостереження вміє записувати відео за сигналом детектора руху. У найпростіших випадках можна обійтися без окремого контролера, але для створення гнучкої системи з безліччю сценаріїв він необхідний.

Для підключення контроллера розумного будинку до глобальної мережі може бути використаний звичайний Інтернет-роутер (7), який вже давно став звичним побутовим приладом в будь-якому будинку. Тут є ще один аргумент на користь контролера розумного будинку - якщо пропаде зв'язок з Інтернет, то розумний будинок продовжить роботу в штатному режимі завдяки блоку логіки, що зберігається всередині контролера, а не в хмарному сервісі.

Контролер розумного будинку

Збірка контролера дуже проста - мікрокомп'ютер (1) встановлюється в пластиковий корпус (2), далі в нього у відповідні слоти встановлюється 8 ГБ карта пам'яті в форматі microSD з програмним забезпеченням (3) і USB-контролер мережі Z-Wave (4). Контролер розумного будинку підключається до електромережі через адаптер живлення 5В, 2.1А (5) і кабель USB - micro-USB (6). Кожен контролер має унікальний ідентифікаційний номер, який записується в файлі конфігурації при першому запуску і необхідний для взаємодії з сервісами хмарного розумного будинку.

Програмне забезпечення контролера

Програмне забезпечення контролера розумного будинку розроблено автором даної статті на основі операційної системи Linux. Воно складається з наступних основних підсистем:

- серверного процесу для взаємодії з обладнанням розумного будинку і хмарою;
- графічного інтерфейсу користувача для налаштування конфігурації і робочих параметрів контролера;
- бази даних для зберігання конфігурації контролера.

База даних контролера розумного будинку

База даних контролера розумного будинку реалізована на основі вбудованої СУБД Postgry і являє собою файл на SD-карті з системним ПО. Вона служить сховищем конфігурації контролера - інформації про підключене обладнанні і його поточний стан, блоку логічних продукційних правил, а також інформації, що вимагає індексації (наприклад, імен файлів локального відеоархіву). При перезавантаженні контролера ця інформація зберігається, що робить можливим відновлення працездатності контролера в разі збоїв електроживлення.

Графічний інтерфейс контролера

Графічний інтерфейс контролера розумного будинку розроблений на мові PHP 7 з використанням мікрофреймворка Slim. За роботу додатка відповідає веб-сервер lighttpd, часто застосовується у вбудованих пристроях завдяки своїй гарній продуктивності і низьким вимогам до ресурсів.

Хмарний сервіс розумного будинку

Хмарний сервіс розумного будинку пропонує простий, гнучкий і недорогий спосіб зберігання і доступу до даних, отриманих від пристроїв розумного будинку. Користувачеві хмарного сервісу не потрібно турбуватися про збереження своїх даних. Можливості

многопроцессорного медіасерверів, оснащеного дискової кошиком з RAID-масивом з декількох 10 - 12 ТБ дисків, набагато перевершують по ємності SD- або Flash-карту всередині контролера розумного будинку. Крім того, карти пам'яті ненадійні, так як мають обмежене число циклів перезапису і часто виходять з ладу. Глибина зберігання даних в хмарі визначається тарифом користувача і легко налаштовується в його особистому кабінеті. Крім цього, для доступу до даних немає необхідності в «кидок портів» на маршрутизаторі користувача, коли пристрої розумного будинку приховані від зовнішніх мереж протоколом NAT. В особистому кабінеті користувача, доступному з мобільних пристроїв, можна легко налаштувати конфігурацію і логіку роботи розумного будинку. Дані в хмарі зручно не тільки зберігати, але й обробляти, надаючи користувачу статистику за різні періоди часу. Нижче буде розглянуто приклад обчислення середньої температури в приміщенні за тиждень на основі вимірів мультісенсора.

Розробка структурної схеми

Структурна схема системи – це сукупність об’єктів та частин та взаємозв’язки між ними. Призначенням структурної схеми є наглядне відображення складових частин розробляємої системи, її основних блоків, вузлів та взаємозв’язок між ними.

Структурна схема розробленої системи зображена на рисунку 2 . На ній показано структуру.

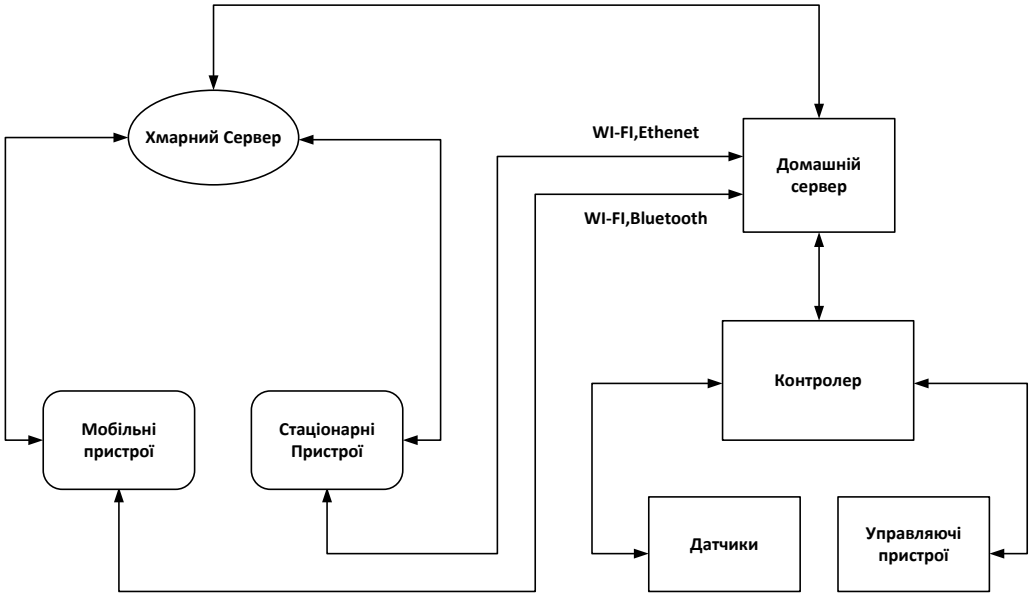


Рисунок 2 – Структурна схема системи «Розумний дім»

Пристрій, побудований за наведеною структурною схемою, як вже було згадано раніше, живиться від електромережі (220В, 50Гц). Змінна напруга на вході пристрою за допомогою бустерного конвертера перетворюється у стабілізовану постійну напругу 3.5В, що живить мікроконтролер, крім цього мікроконтролер формує сигнали для виконавчого елементу що виконує комутацію електроприладу. У електричному приладі встановлені датчики напруги та струму, що у вигляді аналогового сигналу (0-3.5В) подаються на входи АЦП мікроконтролера.

Висновок. У статті розглянуто та проаналізовано програмне забезпечення, яке призначено для системих марного керування пристроями комплексу рішень «розумний дім». В межах України в недостатній мірі представлені вітчизняні розробки в ційобласті. У роботі наведені теоретичне узагальнення й рішення наукового завдання дослідження методів управління розумним будинком з підсистемою безпеки передачі даних. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем хмарного керування управління розумним будинком; Досліджена система хмарного керування розумним будинком; На снові отриманих результатів досліджень створена

програмна реалізація системи хмарного керування розумним будинком. Розроблені під час виконання роботи алгоритми дозволяють успішно вирішувати завдання хмарного керування системою «Розумний дім». Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудовано алгоритм і обрано середовище розробки. Розроблене програмне забезпечення має простий, дружній та зручний інтерфейс користувача, що забезпечує легкість у освоєнні роботи програмного продукту, зручність у використанні, і непотребуєособливихспеціальних знань. Пристворені програмного забезпечення було використано об'єктно-орієнтований підхід, що відповідає сучасним тенденціям у галузі розробки комерційних програмних систем. Програма реалізована на мові високого рівня C++ та PHP. Дана мова програмування дозволяє найбільш ефективно обробляти дані. Це дозволило мінімізувати строк розробки програмного забезпечення, і, як слід, зменшити витрати на його розробку. Запропоноване програмне забезпечення ділиться на загальне програмне забезпечення, що поставляється із засобами обчислювальної техніки й спеціальне програмне забезпечення, що спеціально розроблене для даної конкретної системи й включає програми, щореалізують її функції. Даються необхідні рекомендації з установки розробленого програмного забезпечення. Для підвищення рівня безпеки запропоновано застосовувати змішану систему шифрування що використовує Base64, AES, RSA. В цілому створене програмне забезпечення підтверджує правильність використаних проектних рішень та повністю відповідає вимогам технічного завдання. Створене програмне забезпечення має потенційну можливість для подальшого вдосконалення і застосування у різних галузях.

Список літератури

1. Смірнов О.А. Програмування комп'ютерних мереж. Основи HTML, CSS, JAVA-SCRIPT. Методичні вказівки. Кіровоград 2007–107 с.
2. Основы информационных и телекоммуникационных технологий: Книга 3: Сетевые информационные технологии. Автор: Попов В.Б.
3. Основы сетей передачи данных. Автор: Олифер В., Олифер Н.
4. Основы построения систем и сетей передачи информации. Учебноепособие для вузов. Автор: Щекотихин В.М., Шестак К.В., Михайлов А.И., Ломовицкий В.В.
5. Компьютерные сети и сетевыетехнологии. Автор: СпортакМарк.
6. Введение в сетевыетехнологии. Автор: Иртегов Д. В.
7. Сетевыетехнологии. Учебник-практикум. Автор: Л. Ф. Соловьева.
8. Информационные технологии. Автор: Б.Я. Советов, В.В. Цехановский.
9. Храмцов П.Б., Брик С.А., Русак А.М., Сурин А.И. Основы web-технологий БИНОМ. Лаборатория знаний, Интернет-университетинформационныхтехнологий - ИНТУИТ.ру, 2007.
10. Храмцов П.Б. Видеокурс: Введение в HTML и CSS (2 DVD)Интернет-университетинформационныхтехнологий - ИНТУИТ.ру, 2008
11. Капустин М.А., Капустин П.А., Копылова А.Г. Flash MX для профессиональных программистов Интернет-университет информационных технологий - ИНТУИТ.ру, 2006

УДК 004

А. Нечаєва, магістр гр. КІ-18М
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ УПРАВЛІННЯ РОЗУМНИМ БУДИНКОМ З ПІДСИСТЕМОЮ БЕЗПЕКИ ПЕРЕДАЧІ ДАНИХ

У статті розроблено програмне забезпечення, яке призначено системи управління розумним будинком з підсистемою безпеки передачі даних. Метою розробки є дослідження та програмна реалізація системи управління розумним будинком з підсистемою безпеки передачі даних. Об'єктом дослідження є процес забезпечення управлінням «розумним будинком». Предметом дослідження є методи забезпечення управління системами розумного будинку. Методи дослідження базуються на методах теорії кодування, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи управлінням розумним будинком з підсистемою безпеки передачі управляючих команд. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення. Розроблено зручний інтерфейс користувача. Наведені інструкції по роботі з програмними засобами.
комп'ютерна інженерія, відеонагляд, smart house

Постановка проблеми. З початку нового тисячоліття людство крокує в епоху нових технологічних відкриттів, одним з яких є побутова автоматизація. Час сучасної людини має величезну цінність і такі системи автоматизації як "розумний будинок" істотно економлять цей життєво-важливий ресурс. Включити кондиціонер, вимкнути світло в вітальні, активувати нічну сигналізацію - це лише маленький перелік дій, які можна покласти на систему "розумного будинку". Але такі пристрої мають один мінус - велику ринкову вартість. Тому розробка відносно дешевої системи, з аналогічними можливостями отримує все більше актуальності.

З 2010 року такі системи як "розумний дім" отримали великого розголосу в сучасному суспільстві, бо вони допомагають заощадити пару важливих ресурсів людського життя - час і гроші. Інноваційні розробки подібного роду спрямовані не тільки на підвищення зручності життя, але і на поліпшення енергозбереження приміщень. Простим прикладом такої автоматизації служить освітлення вашого холодильника. Коли дверцята відкриті - освітлення активно, дверцята зачинені - освітлення вимикається. Таким чином можна виключити неефективне використання електроприладів і опалювальних систем, а якщо врахувати, що ціна на енергоресурси постійно зростає - це дозволить отримати істотну економію як енергії, так і грошових коштів.

Більш сучасні проекти будинку майбутнього передбачають наявність цілої системи модулів, розташованих по всьому будинку. Кожен пристрій є повноцінним комп'ютером, об'єднаним в загальну мережу. Практично кожен крок власника контролюється цією системою. Завдяки пристрою можна налаштувати навколишнє оточення на свій смак і практично миттєво змінити інтер'єр. Ще один варіант передбачає практично повне виключення людини від управління харчовими запасами. Все здійснюється автоматично.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи управління розумним будинком з підсистемою безпеки передачі даних.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи управління розумним будинком з підсистемою безпеки передачі даних.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем управління розумним будинком з підсистемою безпеки передачі даних

– Дослідження системи систем управління розумним будинком .

– Програмна реалізація системи управління розумним будинком з підсистемою безпеки передачі даних.

Об'єктом дослідження є процес управління розумним будинком.

Предметом дослідження є методи реалізації систем управління розумним будинком.

Методи дослідження базуються на методах теорії кодування,методах захисту інформації, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Виходячи з теми роботи потрібно розробити програмне забезпечення системи управління для проекту «Розумний дім» та розробити саму автоматизовану систему управління з встановленням необхідних датчиків та ситем.

Розумний будинок - це система інтелектуальної автоматики для управління інженерними системами сучасної будівлі.

Будь-якій людині в будинку, в квартирі або в офісі важливо відчувати себе комфортно і в безпеці. Саме ці два завдання плюс естетика зовнішнього вигляду пристроїв - і є основні цільові установки, на які орієнтовані системи «Розумний Дім». Інтелектуальна автоматика управляє всіма інженерними системами в будинку, дозволяє людині централізовано встановлювати комфортні для себе - температуру, вологість, освітленість в кімнатах, зонах, і забезпечує безпеку.

Система Розумний будинокповинна забезпечувати механізм централізованого контролю та інтелектуального управління в житлових, офісних або громадських приміщеннях. З інсталяцією подібної системи вдома чи на роботі кожен користувач отримує можливість:

- Здійснювати управління необхідною системою (освітлення, клімат, відеоспостереження тощо)

- Отримувати доступ до інформації про стан всіх систем життєзабезпечення будинку (перебуваючи всередині нього або віддалено)

Загальна схема системи управління виглядає наступним чином:

- Центральний процесор управління / головний блок управління

- Датчики (температури, освітленості, задимленості, руху та ін.)

- Керуючі пристрої (диммери, реле, ІЧ-емітери та ін.)

- Інтерфейси управління (кнопкові вимикачі, пульти ІК і радіопульт, сенсорні панелі, web / wap інтерфейс)

- Власна мережа управління, що об'єднує вищевказані елементи

- Керовані пристрої (світильники, кондиціонери, компоненти домашнього кінотеатру та ін.)

- Допоміжні мережі (Ethernet, телефонна мережа, дистрибуція аудіо і відеосигналу)

- Програмне забезпечення проекту.

Основна функція центрального процесора - управління підпорядкованими йому пристроями з використанням наступних інтерфейсів: Ethernet, RS-232, RS-485, IR, аналогових і цифрових входів / виходів та ін. Також центральний процесор управління містить багатозадачну операційну систему, інструментальні засоби програмування і в деяких випадках Web сервер. Датчики розташовуються в певних місцях квартири, які безпосередньо або через проміжні пристрої зв'язані єдиною мережею. Інтерфейси управління здійснюють загальне управління системами Розумний будинок.

Базова концепція

Система управління являє собою сукупність апаратних та програмних засобів, які насамперед націлені на економічність, тобто на зниження можливих розходів (електроенергія, тепло) користувача, а також надає додаткові можливості, наприклад, контроль присутності. Розглянемо всі функції більш детально.

Енергозбереження

Енергозберігаюча система управління освітленням в багатоповерхових будинках (під'їзди, автостоянки, прибудинкові території, підвали, горища) дозволить знизити кількість споживаної електроенергії в 10-15 разів. У цих системах застосовується пристрій управління освітленням з роздільними силовими компонентами, що дозволяє використовувати існуючі лінії електропередач. Енергозберігаюче освітлення починається з намагання упорядкування часу роботи освітлювальних приладів. Ефективний захід енергозбереження - централізація управління освітленням з використанням спеціально розроблених графіків включення і виключення світла. Певну економію можна отримати за рахунок максимального використання всередині приміщення природного світла. Це досягається за рахунок правильного планування будівлі і використовуваних приміщень. Великий ефект дає використання енергозберігаючих ламп. Однак навіть сама «економна» лампа, якщо вона горить в порожньому приміщенні, стане безглуздим джерелом енерговитрат.

Найкраще енергозбереження забезпечують автоматичні вимикачі світла з використанням інфрачервоних та електронних датчиків. Електронні датчики вимірюють рівень освітленості приміщення і, при досягненні заданого значення, видають команду на включення або виключення освітлення (датчики освітленості), або безпосередньо «бачать», що до приміщення увійшов чоловік, і вмикають світло (датчики руху). Світлочутливий елемент блокує ввімкнення освітлення при достатньому природному освітленні. Оскільки на відміну від реле-датчиків часу датчики руху вмикають світло тільки на час фактичного присутності людини в приміщенні, а витрати електроенергії на освітлення можуть бути знижені в кілька разів. Для сходових кліток, коридорів і ліфтових холів економія додатково збільшується за рахунок поетажного управління освітлювальними приладами. В енергозберігаючих вимикачах освітлення застосовуються також інфрачервоні датчики руху з урахуванням планування приміщення. Інші електронні датчики (датчики присутності) здатні визначити знаходження людей в приміщенні і тільки в цьому випадку тримають світло включеним. Інфрачервоний датчик «бачить» тільки рухається людини, хоча цей рух може бути і невеликим - наприклад, помах рукою або кивок головою. При великих часах затримки інфрачервоний датчик працює в режимі датчика присутності, тобто підтримує освітлення при тривалому присутності в приміщенні людей. Малий час затримки вибирається при використанні інфрачервоних датчиків як датчика руху в прохідних приміщеннях. Електронні вимикачі світла можуть використовуватися як автономно, так і в складі автоматизованої системи управління, яку нині називають «розумний дім».

В основі системи енергозбереження лежить температурний контролер і електроконвектори російського і зарубіжного виробництва, що мають сучасний дизайн та доступні ціни. Вони не спалюють кисень, не сушать повітря, пожежобезпечні. Також, замість конвекторів можна використовувати гріють шнури (тепла підлога), інфрачервоні плівки і панелі, електрокотли універсальні і можуть працювати з будь-якими нагрівальними приладами. У традиційних водяних системах опалення датчики можуть управляти кранами з електроприводом або електроклапанами, встановленими на трубах опалення.

У розподільному щиті монтуються автоматичні вимикачі для захисту всіх елементів системи від перевантажень і струмів короткого замикання, а також силові виконавчі пристрої (СИУ-4, СИУ-1).

У системах використовується тільки якісне та надійне електровстановлювальне обладнання провідних європейських фірм, найкращим чином зарекомендувало себе при монтажі та експлуатації. Управляється система температурним контролером за допомогою температурних датчиків і керованих розеток. Монтаж системи управління проводиться телефонним кабелем довжиною до 100 метрів.

Освітлення

В інтелектуальній системі «Розумний Дім» Ви можете керувати світлом натисненням однієї клавіші. За допомогою одного пульта ви зможете налаштувати лампи, люстри, світильники так, як вам подобається. Якщо Ви вирішили запросити гостей і створити їм затишну світлову атмосферу, то система «Розумний Дім» прийде вам на допомогу, Ви

можете одним рухом руки міняти світлову гаму в приміщенні. Датчики руху забезпечують автоматичне перемикання світла, коли ви до них наближаєтеся. Для забезпечення комфорту і затишку у Вашому будинку кожна кімната, хол, зал повинні бути добре освітлені. Без інтелектуальної системи «Розумний Дім» для цього буде потрібно установка великої кількості різних світлових приладів із заплутаною мережею вимикачів.

Система позбавить Вас від необхідності встановлювати безліч вимикачів, Вам представиться можливість замінити їх компактними сенсорними. Так з одного стандартного шести сенсорного вимикача можна управляти дванадцятьма світловими групами. Ви зможете, як плавно регулювати їх яскравість, так просто включити їх або вимкнути. За допомогою сенсорних вимикачів або панелей Ви легко зможете створювати різні світлові сцени, що, безсумнівно, додасть затишку і комфорту Вашого дому, наприклад, сцену «Вечір», при якій одна група світлових приладів включиться на певну яскравість, інша група вимкнеться, штори закриються, а система клімат контролю перейде в комфортний режим. У нічний час світло в коридорах і прихожих буде включатися на частину яскравості автоматично при появі руху. Вам не доведеться шукати вимикач в темряві. Також системою освітлення можна управляти дистанційно з пульта, ноутбука або мобільного телефону. Ви під'їжджаєте до будинку вночі, а він зустріне Вас з включеним освітленням фасаду, підсвічуванням ландшафту і доріжок.

Управління освітленням - одна з найважливіших задач в будинку.[Завдяки інтелектуальному програмування можна заощадити електроенергію та термін експлуатації ламп. Відпадає необхідність шукати вимикачі світла в темряві, а так само вимикати світло при виході з кімнати. Інтелектуальна система вимкне світло, тільки після того як ви заснете і включить м'яке підсвічування, якщо ви прокинетеся вночі, щоб не дратувати очі яскравим світлом. А вранці система вирішить, яке освітлення потрібно в будинку залежно від погоди на вулиці.

Систему автоматизованого управління освітленням можна налаштувати таким чином, що вона буде визначати, в якій частині кімнати знаходиться людина і підсвічувати саме її. У заміському котеджі система може включати вечірню підсвітку двору і декоративне підсвічування фасаду будівлі. Вона зустрічає вас або ваш автомобіль у вечірній час включеним світлом у дворі і гаражі.

Але управління освітленням приносить не тільки комфорт. Розумний будинок може самостійно включати вечорами світло в квартирі, імітуючи присутність людей. Завдяки цьому, майно буде перебувати під подвійним захистом під час Вашої відпустки або тривалої відсутності.

Система клімат-контроль

Така система клімат-контролю працює на підставі закладених у неї алгоритмів, що дозволяють підтримувати встановлені параметри повітряного серед і різних кліматичних зон в приміщеннях при мінімальних затратах енергоресурсів.

Розглянута система дозволяє забезпечувати виконання різних операцій. З її допомогою проводиться нагрів або охолодження. При цьому виключається одночасна робота кондиціонера і системи опалення. Винятком тут може бути наявність теплої підлоги, підтримуючого встановлену температуру в нижній частині кондиціонером приміщення.

Така система забезпечує зниження температури в нічний час в безлюдних приміщеннях і спальнях, що дозволяє створити комфортні умови для сну, а також економити енергоресурси. Крім того, вона дає можливість мінімізувати роботу апаратури і обладнання під час відсутності господарів за допомогою використання режимів роботи «денне відсутність» і «відпустку». При включенні другого режиму проводиться повне відключення системи кондиціонування та вентиляції, а опалювальна система виводиться на мінімальний рівень потужності. Перед поверненням додому можна завчасно встановити в приміщеннях комфортний кліматичний режим шляхом активації системи клімат-контролю по телефону або через інтернет.

Система управління кліматом в приміщенні дає можливість коригувати рівень

температури, вологості, величину притоку свіжого повітря індивідуально для кожного приміщення, управляти роботою системи фільтрації повітря, створювати індивідуальну кліматичну систему для кожного члена сім'ї, погоду в будинку (наприклад, в кімнаті проживання дітей відсутність протягів при постійно свіжому повітрі). У теж час система клімат-контролю, незважаючи на виконання великої кількості функцій, забезпечує економію фінансових коштів і вирішує проблему енергозбереження. Наприклад, систему можна налаштувати таким чином, що у вихідні дні та неробочий час подача тепла в приміщення скорочувалася або відключалася зовсім. Такий режим роботи особливо актуальний для використання в заміських котеджах із застосуванням в них автономних систем опалення. Зазначена система дозволяє дистанційно включати котел опалення або перемикати його в режим економії. З метою більш ефективної і раціональної організації життєдіяльності офісів можливо встановлення контролю над станом комунікацій теплопостачання, електропостачання, водопостачання, створення найбільш комфортних умов роботи для працівників компанії.

Система клімат-контролю «розумного будинку» виключить можливість псування колекції картин, книг або вин шляхом створення найбільш сприятливих умов для їх зберігання.

Для забезпечення коригування параметрів роботи системи застосовуються різні датчики, які фіксують поточні показники мікроклімату в приміщеннях будинку, а також засоби для управління у вигляді перемикачів і панелей. При їх використанні система здатна управляти якістю повітря (температурою, вологістю, озонуванням) відповідно до пори року і доби, режимом провітрювання з використанням автоматичної системи відкривання вікон, змінювати режим роботи радіаторів опалення та теплої підлоги, автоматично підтримувати температуру і вологість у спеціальних приміщеннях, а також аварійно зупиняти систему опалення.

Таким чином, система клімат-контролю «розумного будинку» дозволяє створити здоровий і комфортний мікроклімат для затишного проживання в будинку.

Контроль проникнення

Постановка і зняття квартири з охорони виробляються за допомогою кодової панелі, розміщеної у тамбурі. При відкритті вхідних дверей у людини є 30 секунд на введення правильного коду. Якщо ж код не буде введений розумний будинок включить сирени і відправить СМС повідомлення на кілька телефонних номерів.

Датчики руху, розташовані на кухні, спальні і вітальні дозволять виявити проникнення через вікна.

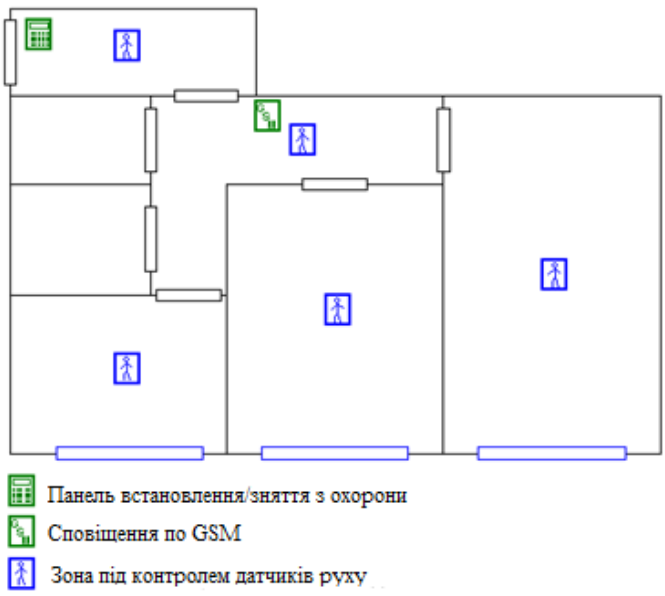


Рисунок 1 - Схема застосування датчиків руху в квартирі інтелектуальна система розумний будинок

При виході з квартири достатньо ввести код на охоронній панелі і розумний будинок не тільки включить сигналізацію, але і відключить освітлення, переведе систему опалення в режим енергозбереження.

Контроль протікання води

Прорив труб водопостачання є дуже неприємною подією у зв'язку з псуванням не тільки свого, але і сусідського майна. Виявити і запобігти витоку води так само допоможе розумний будинок. Контрольованими зонами є санвузли та кухня, тобто ті приміщення, де проходять труби водопостачання.

Прорив труби або перелив води через краї раковини фіксується за допомогою спеціальних датчиків. У випадку протікання розумний будинок перекроїть доступ води в квартиру і відправить СМС повідомлення на задані телефони.

Рисунок 2 – Схема використання датчиків протікання води

Отже, в ході роботи над даним підрозділом було обрано систему управління над розумним домом, яка являє собою сукупність пидсистем управління окремими параметрами та групами датчиків/контролерів.

Розробка структурної схеми

Структурна схема системи – це сукупність об’єктів та частин та взаємозв’язки між ними. Призначенням структурної схеми є наглядне відображення складових частин розробляємої системи, її основних блоків, вузлів та взаємозв’язок між ними.

Структурна схема розробленої системи зображена на рисунку 3 . На ній показано структуру.

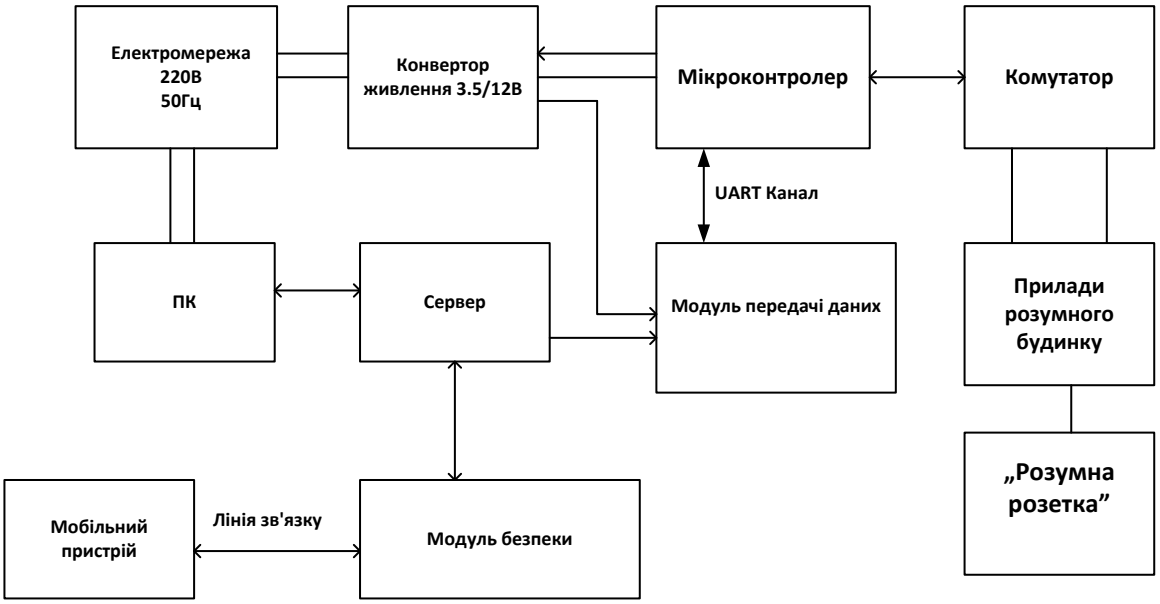


Рисунок 3 – Структурна схема системи «Розумний дім»

Пристрій, побудований за наведеною структурною схемою, як вже було згадано раніше, живиться від електромережі (220В, 50Гц). Змінна напруга на вході пристрою за допомогою бустерного конвертера перетворюється у стабілізовану постійну напругу 3.5В, що живить мікроконтролер DSPIC33FJ16 та Bluetooth Low Energy модуль RN4020 (Microchip). RN4020 забезпечує бездротовий зв’язок пристрою з комп’ютером та передачу даних в обох напрямках. Мікроконтролер DSPIC33FJ16 взаємодіє з RN4020 за допомогою UART каналу, формує допоміжні сигнали, здійснює вимірювання аналогових значень необхідних параметрів роботи електричного приладу, таких як струм, напруга та температура та їх перетворення у цифровий формат. Крім цього мікроконтролер формує сигнали для виконавчого елементу – оптотріаку MOC3023, що виконує комутацію електроприладу. У електричному приладі встановлені датчики напруги та струму, що у вигляді аналогового сигналу (0-3.5В) подаються на входи АЦП мікроконтролера.

Висновок. У статті розглянуто та проаналізовано програмне забезпечення, яке призначено для системи управління розумним будинком з підсистемою безпеки передачі даних. В межах України в недостатній мірі представлені вітчизняні розробки в цій області. У роботі наведені теоретичне узагальнення й рішення наукового завдання дослідження методів управління розумним будинком з підсистемою безпеки передачі даних. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем управління розумним будинком з підсистемою безпеки передачі даних; Досліджена система управління розумним будинком з впровадженням підсистеми безпеки передачі даних; На основі отриманих результатів досліджень створена програмна реалізація системи управління розумним будинком. Розроблені під час виконання роботи алгоритми дозволяють успішно вирішувати завдання управляння системою «Розумний дім». Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудовано алгоритм і обрано середовище розробки. Розроблене програмне забезпечення має простий, дружній та зручний інтерфейс користувача, що забезпечує легкість у освоєнні роботи програмного продукту, зручність у використанні, і не потребує особливих спеціальних знань. При створені програмного забезпечення було використано об’єктно-орієнтований підхід, що відповідає сучасним тенденціям у галузі розробки комерційних програмних систем. Програма реалізована на мові високого рівня C++ та PHP. Дана мова програмування дозволяє найбільш ефективно обробляти дані. Це дозволило мінімізувати строк розробки програмного забезпечення, і, як слід, зменшити витрати на його розробку.

Запропоноване програмне забезпечення ділиться на загальне програмне забезпечення, що поставляється із засобами обчислювальної техніки й спеціальне програмне забезпечення, що спеціально розроблене для даної конкретної системи й включає програми, що реалізують її функції. Для підвищення рівня безпеки запропоновано застосовувати змішану систему шифрування що використовує Base64, AES, RSA. В цілому створене програмне забезпечення підтверджує правильність використаних проектних рішень та повністю відповідає вимогам технічного завдання. Створене програмне забезпечення має потенційну можливість для подальшого вдосконалення і застосування у різних галузях.

Список літератури

1. Смірнов О.А. Програмування комп'ютерних мереж. Основи HTML, CSS, JAVA-SCRIPT. Методичні вказівки. Кіровоград 2007–107 с.
2. Основы информационных и телекоммуникационных технологий: Книга 3: Сетевые информационные технологии. Автор: Попов В.Б.
3. Основы сетей передачи данных. Автор: Олифер В., Олифер Н.
4. Основы построения систем и сетей передачи информации. Учебное пособие для вузов. Автор: Щекотихин В.М., Шестак К.В., Михайлов А.И., Ломовицкий В.В.
5. Компьютерные сети и сетевые технологии. Автор: Спортак Марк.
6. Введение в сетевые технологии. Автор: Иртегов Д. В.
7. Сетевые технологии. Учебник-практикум. Автор: Л. Ф. Соловьева.
8. Информационные технологии. Автор: Б.Я. Советов, В.В. Цехановский.
9. Храмцов П.Б., Брик С.А., Русак А.М., Сурин А.И. Основы web-технологий БИНОМ. Лаборатория знаний, Интернет-университет информационных технологий - ИНТУИТ.ру, 2007.
10. Храмцов П.Б. Видеокурс: Введение в HTML и CSS (2 DVD) Интернет-университет информационных технологий - ИНТУИТ.ру, 2008

УДК 004

В. Нечай, магістр гр. КН-18МЗ-1,4
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ ЕНЕРГОЕФЕКТИВНОГО КОНТРОЛЮ КЛІМАТУ У МОНТАЖНИХ ШАФАХ ЦОД

У статті розроблено програмне забезпечення, яке призначено для системи енергоефективного контролю клімату у монтажних шафах ЦОД. Метою розробки є дослідження та програмна реалізація системи енергоефективного контролю клімату у монтажних шафах ЦОД. Об'єктом дослідження є процес енергоефективного контролю клімату у монтажних шафах ЦОД. Предметом дослідження є методи енергоефективного контролю клімату у монтажних шафах ЦОД. Методи дослідження базуються на методах підвищення рівня енергоефективності ЦОД, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи енергоефективного контролю клімату у монтажних шафах ЦОД. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.
комп'ютерні науки, контроль клімату, монтажні шафи, ЦОД

Постановка проблеми. З надмірності, за якою гналися лише «зелені» компанії, енергоефективність перетворилася в необхідність для будь-яких видів діяльності, де є потреба домогтися економії без зниження продуктивності – через обмеженість бюджетів, компанії прагнуть досягти більшого з меншими витратами.

Складна чутлива електроніка й накопичувачі становлять основу великої кількості промислових рішень, і, щоб захистити це устаткування від несприятливих зовнішніх впливів,

його найчастіше розміщають у монтажних шафах. Залежно від температури й умов навколишнього середовища, шафи необхідно прохолоджувати, попереджаючи тим самим виникнення відмов внаслідок перегріву й забезпечуючи належне функціонування устаткування. Згідно даним дослідницької організації Rocky Mountain Institute, витрати енергії, використовуваної для обігріву й охолодження, можна скоротити на 60%. У даній роботі описуються методи охолодження корпусів, які допоможуть знизити енергоспоживання й заощадити кошти.

Насамперед варто з'ясувати, чи необхідно охолодження в кожному конкретному випадку, і якщо так, те якої потужності. Важливо зробити точну оцінку, щоб не витрачати енергію даремно.

Вибираючи рішення для контролю мікроклімату, потрібно відповісти на три питання: які розміри шафи, скільки тепла виділяється устаткуванням і де буде розміщатися шафа. При наявності всі дані розрахунки можна провести як вручну, так і за допомогою програмного забезпечення.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи енергоефективного контролю клімату у монтажних шафах ЦОД.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи енергоефективного контролю клімату у монтажних шафах ЦОД.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем енергоефективного контролю клімату у монтажних шафах ЦОД.

– Дослідження системи енергоефективного контролю клімату у монтажних шафах ЦОД.

– Програмна реалізація системи енергоефективного контролю клімату у монтажних шафах ЦОД.

Об'єктом дослідження є процес енергоефективного контролю клімату у монтажних шафах ЦОД.

Предметом дослідження є методи енергоефективного контролю клімату у монтажних шафах ЦОД.

Методи дослідження базуються на методах підвищення рівня енергоефективності ЦОД, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Під клімат-контролем розуміється комплекс мір, спрямованих на створення, підтримку оптимального для заданих процесів клімату, а також його контроль і керування.

Для центрів обробки даних (ЦОДів) ці міри реалізуються через системи вентиляції, кондиціювання й зволоження, за рахунок яких забезпечується температура, вологість і запиленість (точніше, незапиленість) у приміщенні.

Найпростіше розібратися з вентиляцією. У приміщенні ЦОДу не передбачається наявність постійного перебування людей, а тому, із числа штатних систем вентиляції присутня лише приточна (підпірна), що має своєю метою створити в об'ємі, що обслуговується, надлишковий тиск щоб уникнути влучення в приміщення повітря ззовні. Це невелика система, звичайно складальна, що забезпечує клас очищення приточного повітря не нижче EU4, є типовий, тому як з погляду вентиляційника, так і з погляду автоматника складностей не викликає.

Окремої уваги заслуговує той факт, що приміщення ЦОД обладнаються системою автоматичного газового пожежогасіння, а, отже, і аварійною системою вентиляції – газовидаленнм. Відповідно до вимог видалення газу виробляється з верхньої й нижньої зон приміщення. Нерідко обсяг під фальшполом виділяється окремо й також обладнається повітрозаборними пристроями. У випадку неможливості забезпечити природний приплив повітря для роботи газовидаленн, застосовується окрема підпірна система.

Інша справа із забезпеченням необхідного тепло-вологісного режиму приміщення. Незважаючи на те, що до кліматичного устаткування з боку обчислювального пред'являються цілком звичні вимоги, найбільш гострим моментом стає можливий діапазон їхньої зміни, за яким ми й звернемося до нормативної документації. Тут букву закону диктують два американських стандарти TIA/ EIA-942 і TIA/ EIA-569-B. Обоє за більше докладними рекомендаціями посилаються на американську асоціацію ASHRAE, що в 2008 році розширила діапазон, що рекомендується, параметрів внутрішнього повітря, увівши наступні критерії (ці розширені, а також існуючі раніше вимоги, показані на рис. 1.):

– температура: 18 – 27°C;

– температура точки роси в межах 5.5 – 15°C (нагадаємо, що температурою точки роси є температура, до якої при постійному вологовмісті необхідно остудити повітря, щоб з'явився конденсат, тобто фактично ця вимога визначає наступний діапазон вологовмісту: 5.5 – 11 г/кг (див. рис. 1));

– відносна вологість не вище 60%.

Спеціально для цих цілей в організації EUROVENT серед 19 сертифікаційних програм є особлива – «Close Control Air Conditioners (CC)» (Кондиціонери точного контролю). Це устаткування класу «прецизійні кондиціонери».

Дійсно, коли мова йде про ЦОДобудування, комфортним кондиціонерам довіряти не рекомендується відразу з кількох причин. Справа в тому, що комфортне (побутове й промислове) кліматичне устаткування призначене, головним чином, для роботи в місцях перебування людей, до того ж з відносно низькою щільністю тепловиділень, чого не сказати про обчислювальні комплекси. Збільшений термін служби, націленість на цілорічну роботу, в 2-3 рази знижене осушення повітря, удвічі збільшений витрата повітря при тої ж холодопродуктивності, а також більше широка лінійка устаткування з різними схемами руху повітря – все це визначає беззастережний вибір на користь прецизійного кліматичного устаткування.

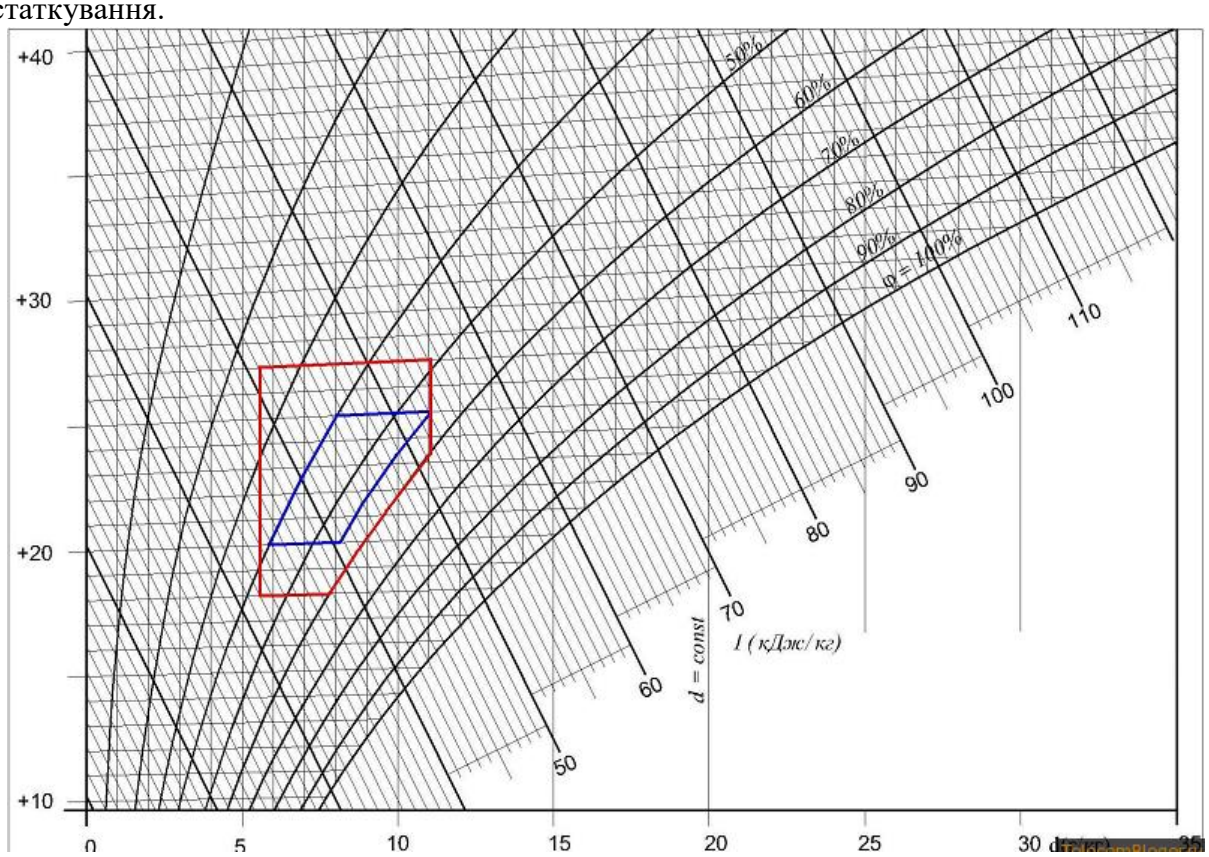


Рисунок 1 – I-d-діаграма вологого повітря й діапазон, що рекомендується, параметрів мікроклімату в ЦОДах: від області, обмеженої синім, перейшли до області, обмеженої червоним

Проблема теплоносія

Як було відзначено вище, техніка за допомогою повітря здійснює тепловідведення. Але як теплоносій повітря не ідеальне, що пояснюється найпростішою термодинамічною формулою (справедливої для випадку нагрівання повітря без зміни його вологовмісту, що й відбувається в IT-стійках):

$$N=C*M*\Delta T,$$

де:

– N – потужність охолодження, кВт;
– C – питома теплоємність теплоносія, кДж/(кг*С);
– M – масова витрата теплоносія, кг/з;
– ΔT – перепад температур теплоносія на вході й виході з устаткування, °С.

По-перше, справа в тому, що для повітряних теплообмінників характерна температура «недорекуперації» (мінімальний температурний напір) порядку 7°С. Це значить, що випарник кондиціонера із середньою температурою 8°С при розумній площі теплообміну зможе остудити повітря до 8+7=15°С, у той же час устаткування в стійці температурою 41°С нагріває повітря до 41-7=34°С. Таким чином, в ідеального теплоносія перепад температур склав би ΔT1= 41-8=33°С, а в повітря як теплоносій перепад дорівнює ΔT2= 34-15=19°С, а виходить, при тих же N і C потрібна витрата теплоносія в ΔT1/ΔT2=33/19=1,7 рази більший.

По-друге, теплоємність повітря відносно низька (1,005 кДж/(кг*С)), у той час як, наприклад, для води вона становить 4,183 кДж/(кг*С), тобто масова витрата води при тих же значеннях N і ΔT (див. формулу вище) був потрібний би в 4,183/1,005=4,2 рази менший. Додамо, що температура недорекуперації для води становить ~2°С, отже, масова витрата знижується ще в ((41-2)-(8+2))/18=1,6 рази, тобто в цілому в 4,2*1,7=7,1 рази, а якщо врахувати, що щільність води в 1000 разів вище щільності повітря, те об'ємна витрата знизиться в 7100 разів. Як видно з характеристик кондиціонерів, на 1кВт тепла необхідно в середньому 200 $м^3$/год повітря, витрата ж води складе всього 0,03$м^3$/год. При прогнозованій через кілька років стійці в 100кВт буде потрібно 3 $м^3$/год води, а потік повітря… видимо, здме стійку.

Таким чином, необхідна заміна повітря як теплоносій на іншу рідку або газоподібну речовину. Звичайно, вода б ідеальної, але одна лише властивість електропровідності викреслює її зі списку претендентів.

На даний момент уже досить широко розвинене рідинне охолодження процесорів і з'являються перші більше принципові результати в позначеному напрямку – компанія Iceotope запропонувала занурювати устаткування в спеціально розроблену рідину – інертний синтетичний охолоджувач (див. рисунок 2). Підвищивши ефективність охолодження таким способом, за даними компанії, стає можливим знизити витрати на охолодження 1000 серверів з майже $800 000 до $50 000, тобто на 93%.

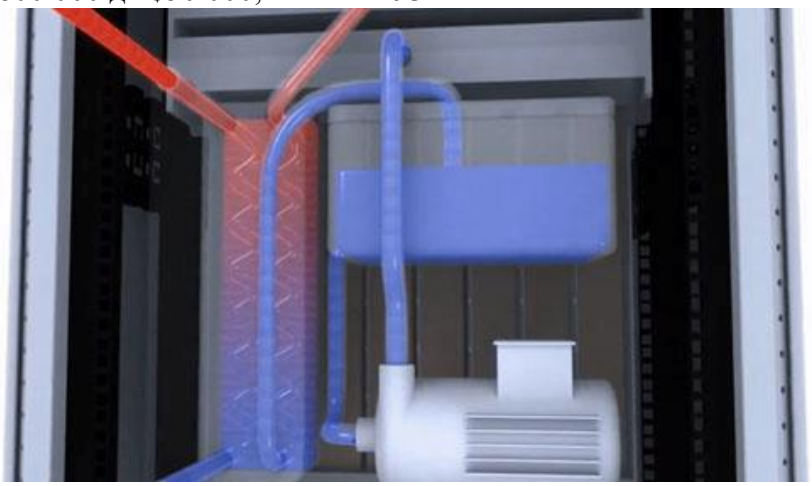


Рисунок 2 – Тильна сторона стійки з розташуванням насоса й колектора для синтетичного теплоносія

У перспективі, якщо врахувати, що енергія фазового переходу речовини нерідко порівнянна з енергією його нагрівання на тисячі градусів, то можна припустити поява синтетичного теплоносія, що міняє агрегатний стан з рідкого на газоподібне при температурах, близьких до 30°С. Цей теплоносій буде скипати при контакті з устаткуванням, у газоподібному виді підніматися нагору, де його чекає більше звична система охолодження, що сточлює його й відправляє знову до устаткування.

Огляд існуючого устаткування

Але, на жаль, масові виробники серверів не переходять на випуск устаткування, що підтримує рідинне охолодження, тому як теплоносій у нашім розпорядженні є тільки повітря, використовуючи який сучасний ринок пропонує ряд рішень.

При використанні прецизійних кондиціонерів забезпечення мікроклімату реалізується на основі трьох існуючих архітектур охолодження виходячи із щільності тепловиділень:

– охолодження на рівні залу;

– охолодження на рівні ряду;

– охолодження на рівні стійки.

Причому, незалежно від обраної архітектури, варто звернути увагу на ключові параметри прецизійних кондиціонерів:

– повна холодильна потужність (холодопродуктивність);

– явна холодопродуктивність;

– витрата повітря, оброблюваного кондиціонером;

– площа кондиціонера в плані.

Розглянемо типи кліматичного устаткування в приміщенні:

Прецизійні спліт-системи звичайно реалізують архітектуру охолодження на рівні залу й використовуються для приміщень із малою щільністю тепловиділень. Як правило, це допоміжні приміщення – ДПЖ, електрощитові й ін.

Широко відома серія кондиціонерів HPS фірми Liebert (Рисунок 3.3). Внутрішні блоки касетного типу оснащені бічним повітрозабором з нижнім видувом і характеризуються рівністю повної й схованої холодопродуктивностей (SHR=1).

Рисунок 3 – Прецизійні спліт-системи компанії Liebert із внутрішнім блоком касетного типу

Таке рішення дуже компактно й не займає досить коштовне місце на підлозі, але за це доводиться платити низкою холодопродуктивністю (від 6.4 кВт до 14.6 кВт). Витрата повітря у випарнику становить від 190 до 240 $м^3$/(год*кВт). Безперечним плюсом є функція вільного охолодження з використанням зовнішнього повітря при непрацюючому компресорі. Тут кондиціонери фірми Liebert вигідно відрізняються наявністю унікальною запатентованою системою плавного переходу на режим вільного охолодження, що використовує обертову керовану електроприводом заслінку. Плавне відкриття заслінки від 0 до 100% дозволяє працювати в змішаному режимі, коли частина холоду генерується холодильним циклом, а частина забирається з навколишнього середовища.

– Існують і **моноблочні шафові кондиціонери**, що відрізняються від попередніх тем, що не вимагають виносного конденсатора (він розташований у моноблоці). Такі системи встановлюються в зовнішню стіну так, щоб лицьова панель із ґратами забору й роздачі повітря перебували в приміщенні, задня панель виходила на вулицю. Тим самим досягається аналог віконного побутового кондиціонера.

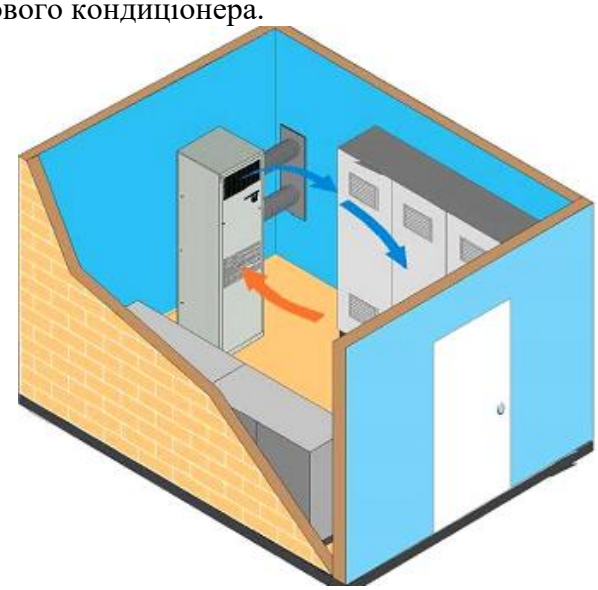


Рисунок 4 – Моноблочні шафові кондиціонери на малих ЦОДах

Можливий режим вільного охолодження. Холодопродуктивність систем досягає 20кВт, і цей тип устаткування ідеально підходить для забезпечення й контролю клімату в маленьких, обмежених приміщень, наприклад, на базових станціях (див. рисунок 4).

– Найбільше широко розповсюджений тип – **прецизійні шафові кондиціонери** (рисунок 5). З їхньою допомогою реалізується архітектура охолодження рідше на рівні залу, частіше ж на рівні ряду. Шафові кондиціонери прохолоджують повітря як за рахунок фреону, так і за рахунок води й мають безліч варіантів виконання виходячи із двох можливих напрямків руху повітря: зверху долілиць і знизу нагору.

Рисунок 5 – Прецизійні шафові кондиціонери фірми Uniflair

Характеристики різних виробників близький друг до друга, тому приведемо усереднені значення для одиниці устаткування:

– Повна холодопродуктивність – від 4 до 160 кВт.
– Явна холодопродуктивність – від 4 до 120 кВт.
– Витрата повітря – від 160 до 260 $м^3$/(год*кВт).

– Площа в плані – від 0.3 до 2.4 м^2.

Заслуговує на увагу широкий вибір комплектуючих для забезпечення необхідної функціональності:

– мікропроцесор для контролю температури й вологості;
– вентилятори що комутируються (EC);
– повітряний клапан з електроприводом;
– парозволожувач (електродний) + осушувач;
– фільтр класу G 3-G5 (EU 3-EU5);
– датчик засмічення фільтра;
– датчик витоку води;
– часова карта;
– опорна рама з віброізоляторами, і ін.

Помітимо, що блоки, що працюють на фреоні, виключають наявність води в ЦОД і обходяться дешевше при потужностях до 100кВт, однак вони мають більші габарити, сильніше навантажують систему ДПЖ і, як правило, не оснащуються функцією вільного охолодження (за винятком кондиціонерів InRef).

На сучасний момент саме на основі шафових кондиціонерів будується найбільше число ЦОДів. Класичним варіантом стало розміщення стійок у ряди з виділенням холодного й гарячого коридорів. Існують рішення з вигороджуванням як холодного, так і гарячого коридорів щоб уникнути змішання різнотемпературних потоків. Роздача холодного повітря кондиціонерами здійснюється під фальшпол, звідки через спеціально передбачені ґрати або панелі активної підлоги повітря розподіляється перед стійками. Тут необхідно враховувати напір убудованого в кондиціонер вентилятора і його витрата. Критичними є наступні величини:

– висота фальшполу. Підпільний простір відіграє роль повітровода, ідеальною швидкістю повітря для якого є величини 1-1.5м/с. Але навіть при більших швидкостях для потужних ЦОДів висота фальшполу досягає півтора метрів, що не завжди дозволяє виконати як висота приміщення, так і конструктивні елементи підлог.

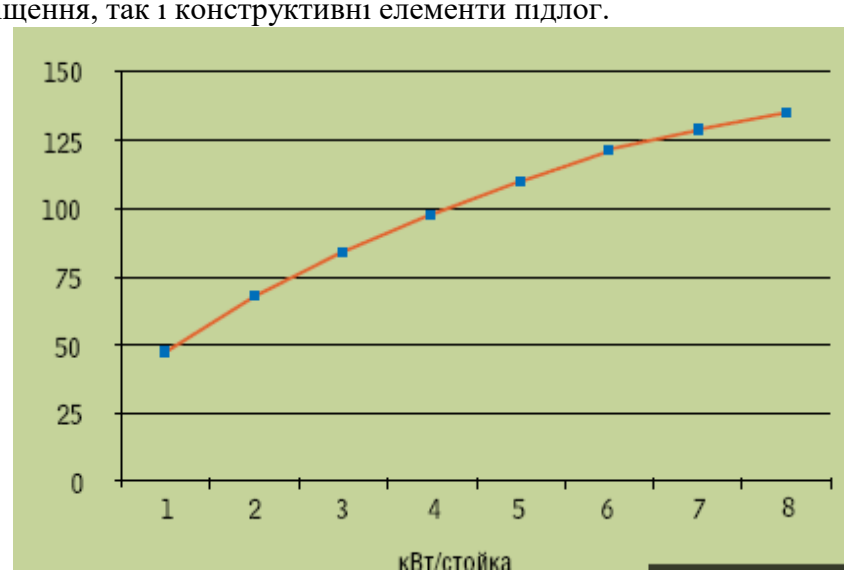


Рисунок 6 – Залежність висоти фальшполу від потужності стійки

Довжина ряду, що обслуговується, становить, як правило, 10-12 метрів.

Результатом обмежень є погіршення топології ЦОДу. Крім того, досвідчені дані показують, що даний спосіб підходить для стійок, тепловиділення яких становлять, наприклад, 10кВт. Деякі типи стійкового устаткування допускають багатобічний повітрозабор і максимальні тепловиділення досягають 25кВт. Подальше збільшення потужності вимагає використання наступного типу кліматичного устаткування.

– **Кондиціонери-доводники.** Тим часом, через постійний ріст потужності обчислювального устаткування, всі частіше використовується архітектура охолодження на рівні стійки. Подібні рішення вже давно з'явилися в провідних виробників кліматичного прецизійного устаткування – Liebert, APC, Rittail і ін.

Суть рішення в установці блоків кондиціонерів безпосередньо в ряді стійок (через одну, дві, три стійки, залежно від співвідношення потужностей), тим самим збільшуючи тепловідведення зі стійки до 40кВт. При цьому знижується електроспоживання кондиціонерів за рахунок меншої потужності вентиляторів у зв'язку з переміщенням повітря на менші відстані.

Компанія Liebert пішла далі, випустивши надстійкові й надкоридорні кондиціонери (див. рисунок 3.7). Додамо ще той факт, що в контурі використовується спеціальний холодоагент, що змінює свій агрегатний стан без реалізації парокомпресійного холодильного циклу й циркулюючий з температурою вище точки роси, а, виходить, явна холодопродуктивність дорівнює повної (SHR =1). Тобто, теоретично, саму густонаселену стійку можна оточити кондиціонерами із трьох сторін – з боків внутрірядними й двома типами блоків зверху й від жодного з них не потрібен відвід конденсату. При цьому для підключення блоків використовуються гнучкі підводки й швидкоз'ємні з'єднання, що дозволяють виконувати роботи без зупинки всієї системи холодопостачання.

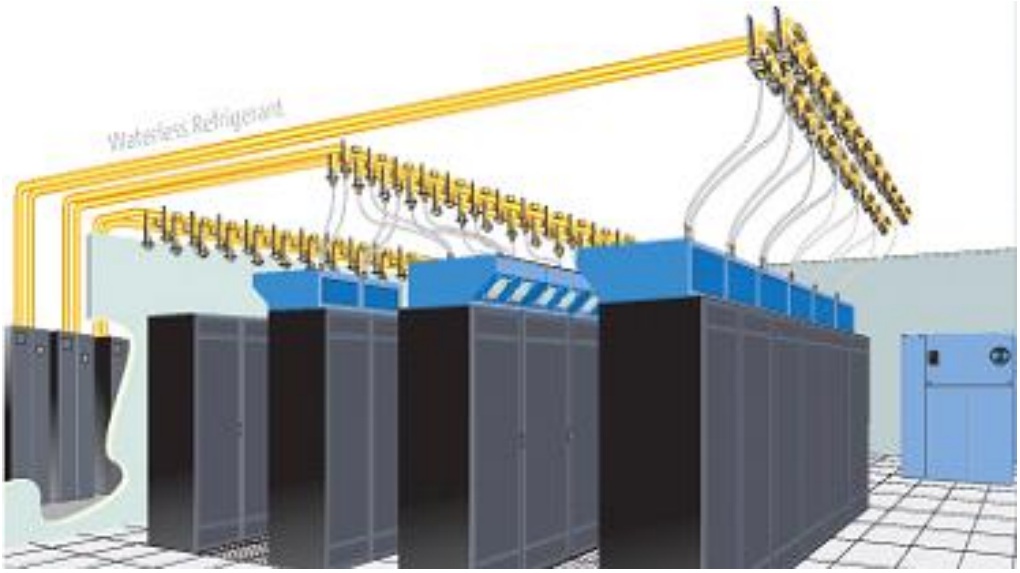


Рисунок 7 – Надстійкові блоки компанії Liebert

– Повна холодопродуктивність блоку – від 9 до 30 кВт.
– Явна холодопродуктивність – від 9 до 30 кВт.
– Витрата повітря – від 140 до 220 $м^3$/(год*кВт).
– Площа в плані – для внутрірядних блоків, як правило, дорівнює 0.3 або 0.6 $м^2$.

У загальному й цілому, відзначимо, що найбільш широкою лінійкою устаткування володіє італійська компанія Uniflair. Її кондиціонери характеризуються наявністю за замовчуванням електронного термо-регулюючого вентиля, низькотемпературного комплекту до – 40°С (що немаловажно для нашої країни), рівністю повної і явної холодопродуктивностей (SHR=1), а також елементами автоматики від компанії Carel. Компактність устаткування Uniflair досягається використанням холодоагенту R410a. Унікальною можливістю також є контроль і регулювання статичного тиску під фальшполом запатентованими засобами Uniflair. Існує гарантований і перевірений варіант відводу 40кВт від стійки.

Компанія APC активно просуває власну масштабовану систему InfraStruXure™, що досягла за вісім років свого існування значних успіхів. Вона поєднує не тільки деякі інженерні системи – засобу живлення й кондиціювання повітря, але й стійки для монтажу

устаткування, а також засобу керування. Розроблено модульні системи для 5 типів IT-середовища, став доступний і простим навіть розрахунок вартості капітальних і експлуатаційних витрат при впровадженні InfraStruXure™.

Гнучким виробництвом, орієнтованим під конкретного замовника, володіє компанія InRef. Завдяки налагодженому зв'язку із заводом є можливість виготовлення устаткування під індивідуальне замовлення. У стандартну комплектацію кондиціонерів входять що комутируються (EC) вентилятори. Лінійка кондиціонерів відрізняється наявністю моделей з інверторним приводом компресора (до 110Гц) і підтримкою прямого вільного охолодження шафовими кондиціонерами. Заводська гарантія становить 2 роки.

Часто встає питання про наявність якісної документації – опису систем, проектних, монтажних і сервісних керівництв. На цьому фронті лідируючі позиції займає Liebert, а також Uniflair із численними фотографіями, що пояснюють.

Окремої уваги заслуговує диспетчерський контроль клімату в ЦОДі. Виробники пропонують відслідковувати й коректувати ситуацію з персонального комп'ютера за допомогою спеціального програмного забезпечення, що дозволяє:

– бачити температуру й вологість повітря, температуру й тиск холодоносія в місцях установки датчиків;

– контролювати й управляти роботою устаткування (кондиціонерів, чіллерів, насосів, клапанів і засувок і ін.), відслідковувати режим роботи теплообмінних апаратів, ступінь їхнього забруднення

– змінювати налаштування роботи системи на відстані;

– здійснювати передачу повідомлень по e-mail і sms;

– мати доступ до ситуації через інтернет;

– поєднувати функції контролю над іншими інженерними системами обчислювальних центрів.

Перспективи

Один з напрямків подальшого розвитку галузі пов'язане з переходом на рідинних теплоносіїв і зачіпалося на початку огляду.

Позначимо й ще одну тенденцію у світі забезпечення клімату, перші кроки якої також потрапили в поле нашого зору при визначенні параметрів мікроклімату. Не далі як в 2008р. асоціація ASHRAE розширила діапазон температур, збільшивши максимальну на 2°C. Не виключені й подальші зміни, тим більше, що експерименти на власних ЦОДах компаній Microsoft, Intel, HP по збільшенню температури в приміщенні привели до економії сотень тисяч доларів у рік. Особливо яскравим є вивід, зроблений у компанії Intel після стійкої 10-місячної роботи ЦОДу при 33°C: «існуючі подання про діапазони температури й вологості варто переглянути». У компанії Sun, наприклад, пропонують за оптимальний діапазон температур прийняти 26-29°C.

Із цією тенденцією добре сполучається пропозиція компанії «Аякс Інжиніринг» використовувати повітро-повітряний роторний теплообмінний апарат високої ефективності, за рахунок якого пропонується позбутися від роботи холодильного контуру при температурі навколишнього середовища до 22°C.

Особливості побудови систем кліматики в МЦОД

МЦОД це представник нового класу модульних рішень ЦОД. Коли вони стали з'являтися на ринку, за ними закріпилася назва «Мобільні ЦОД» (МЦОД), оскільки найбільш помітна відмітна риса такого модуля – можливість переміщення на інше місце експлуатації. Але в міру розвитку розуміння ринком можливостей МЦОД, мобільність стала сприйматися як корисна, але не настільки вже й важлива характеристика, а на перший план вийшла автономність. У результаті, що ведуть виробники стали відмовлятися від терміна «Мобільний ЦОД», заміняючи його на «Модульний», «Портативний» і т.д. Ми пропонуємо нарівні з терміном МЦОД, якому можна розшифрувати і як «Модульний ЦОД», використовувати більше загальний термін – мобільний (автономний) модуль ЦОД.

Від серверних приміщень стаціонарного ЦОД мобільні модулі відрізняються в першу чергу відносно невеликими розмірами. З погляду побудови систем кондиціювання це означає, що в них неможливо встановити фальшпол нормальної висоти, відсутній буферний обсяг повітря над стійками, необхідний для вирівнювання температури гарячих потоків, і, головне, досить невелика відстань від стійок з IT-устаткуванням до зовнішніх стінок конструкції. Також є помітний тепловий потік через стінки конструкції МЦОД назовні. Фактично це означає, що класичну схему компонування систем кондиціювання, що домінує в стаціонарних ЦОД, у мобільних модулях застосувати неможливо.

Тому в них застосовуються компонування систем кондиціювання з тепловими доводниками або оригінальні схеми, наприклад, як у МЦОД Ситроникс «Датеріум 2», де використовується фізичний поділ гарячих і холодних потоків. Переважають рішення на міжстійкових кондиціонерах (Рисунок 8);

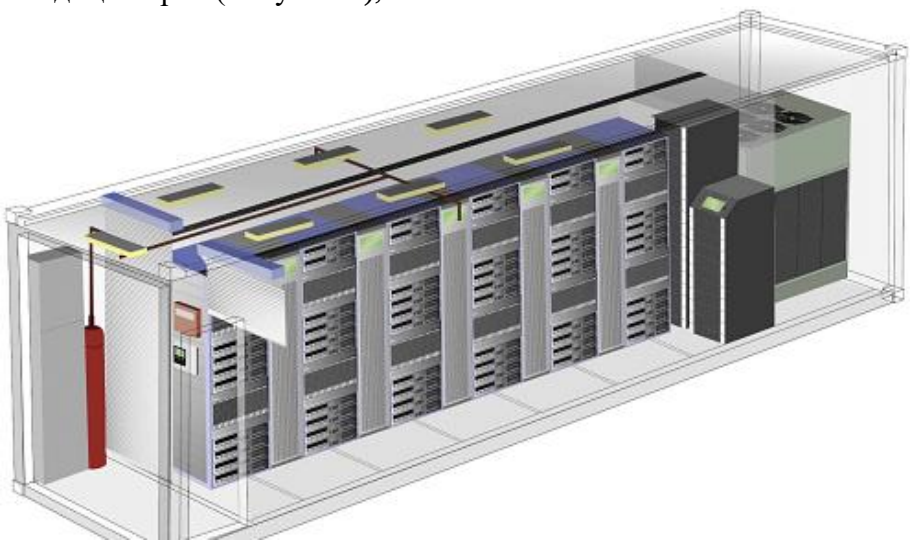


Рисунок 8 – Компонування МЦОД «Датеріум 3» з міжстійковими кондиціонерами

Але зустрічаються й стельові кондиціонери. Вибір цих компонувань обумовлений двома основними причинами. Перша з них виникає з того, що система енергорозподілу й безперебійного електропостачання перебуває відразу, або, у найкращому разі, за тонкою перегородкою. Тому рішення, що використовують як проміжний теплоносій розчини води, тут украй небажані. У цей час гострота даної проблеми знизилася, тому що з'явилися чисто фреонові рішення як в області міжстійкових, так і стельових кондиціонерів. Друга полягає в тім, що ширину мобільного модуля збільшити не можна (модуль стає негабаритним під час перевезення), а глибина стійок росте слідом за збільшенням глибини устаткування. Так, якщо ще 5-7 років тому середні стійки мали глибину 0.6-0.8 м, те зараз стійка глибиною 1 м є стандартної, з'являються стійки глибиною 1,2 м. Частково цю проблему вирішує застосовуваний у всіх МЦОД механізм переміщення стійкового масиву в поперечному напрямку. Він дозволяє оптимізувати ширину коридорів після завершення інсталяції IT-устаткування, але однаково ширина коридорів у робочому положенні не перевищує 0.75 м. Це значення при потужностях стійки в 5-10 кВт уже близько до критичного – у потоці починають утворюватися небезпечні псевдостаціонарні завихрення, що володіють підвищеною температурою. Так, показані на рисунок 3.9 зони підвищеної температури утворювалися в кутах гарячого коридору МЦОД.

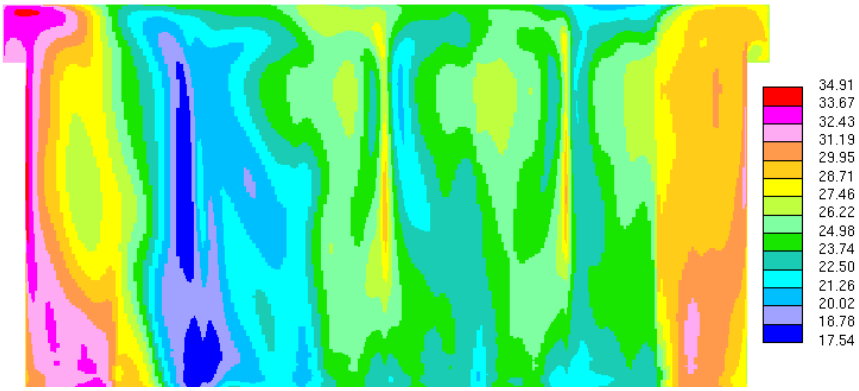


Рисунок 9 – Поле температури в поздовжньому розрізі МЦОД

Основний метод боротьби із цими явищами – ліквідувати будь-які нерівномірності на шляху руху повітря. Особливо кабельні лотки, козирки над стійками, настінні шафи й т.п. Втім, у подібною проблемою в класичних ЦОД зштовхнулися вже давно – це проблема впливу розміщених під фальшполом комунікацій на подачу холодного повітря до стійок. І вирішується вона аналогічно – виносом всіх комунікацій з-під фальшполу.

З ростом питомого споживання стійки з'являється ще одна проблема – можливість ушкодження IT-устаткування потоком прокачуємого через нього повітря. Як уже говорилося вище, ми досягли граничних значень по температурі на вході в стійку й на виході зі стійки. На теплоємність повітря теж поки вплинути не вдається. Залишається тільки підвищувати швидкість продувки. На рисунок 10 показане поле модуля швидкості в поперечному розрізі МЦОД.

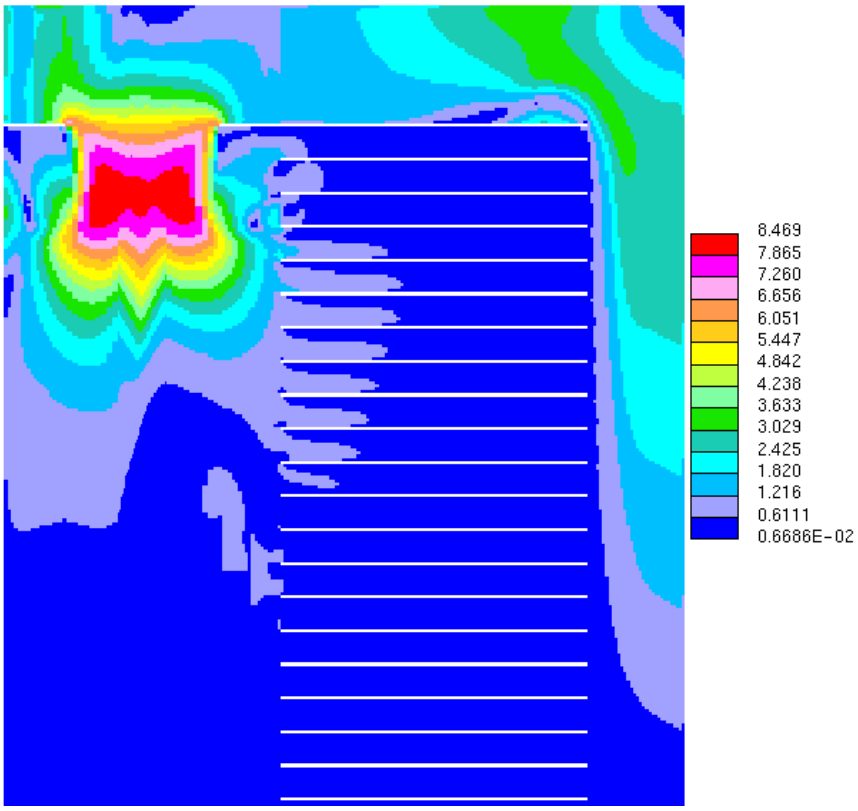


Рисунок 10 – Поле модуля швидкості в поперечному розрізі МЦОД

Видно, що швидкості потоків на вході в окремі сервери досягають 1 м/с. Поки це ще некритично, але адже й потужність стійки тільки 5 кВт. При потужності стійки в 50 кВт швидкість потоку зросте вже до 10 м/с (60 км/год), що приведе як мінімум до руйнування

вентиляторів в IT-устаткуванні. Можна припустити, що цей фактор зупинить ріст питомої потужності стійки на рівні 50-100 кВт.

Але, швидше за все, збільшення питомої потужності стійки припиниться набагато раніше. Справа в тому, що 20 футовий контейнер з потужністю IT-устаткування від 100 кВт перетворюється в «теплову бомбу». При відмові системи охолодження температура усередині контейнера (гермозони) за кілька секунд перевищує 100 градусів. Що фатально не тільки для устаткування, але й випадково що опинився там обслуговуючого персоналу. Тому максимальну потужність стійки можна вважати 12-15 кВт і не очікувати її збільшення найближчим часом.

Що ж стосується теплових втрат від теплопередачі через оболонку мобільного модуля, то при використанні сучасних матеріалів вони становлять 0.5-1.5 Вт/кв.м град. Що для 20 футового контейнера становить величину всього порядку декількох кіловатів і легко компенсується відповідним запасом холодильної (тепловий) потужності.

Так як, вхід у мобільні модулі здійснюється безпосередньо з вулиці, у конструкції МЦОД обов'язково повинен бути присутнім тамбур-шлюз. При використанні в регіонах з жарким і вологим кліматом у тамбур-шлюзі може знадобитися окремий кондиціонер, що працює в режимі осушувача.

Проте, незважаючи на перераховані вище проблеми, теплова ефективність модульних рішень виявляється помітно вище, ніж у традиційних ЦОД.

Це дозволяє значно знизити витрати на експлуатацію модульного ЦОД.

Розробка структурної схеми

Завдання автоматизованого моніторингу й керування кліматичними параметрами актуальний для центрів обробки даних (ЦОД), точних виробництв, а також для ринку так званих “розумних будинків”. Не дивно, що вихід з ладу системи клімат-контролю може викликати лавину проблем пов'язаних з відмовою техніки й зупинкою виробництва.

Опис і архітектура системи

Програмне забезпечення, що розробляється в даній роботі має назва програмна реалізація системи енергоефективного контролю клімату у монтажних шафах ЦОД.

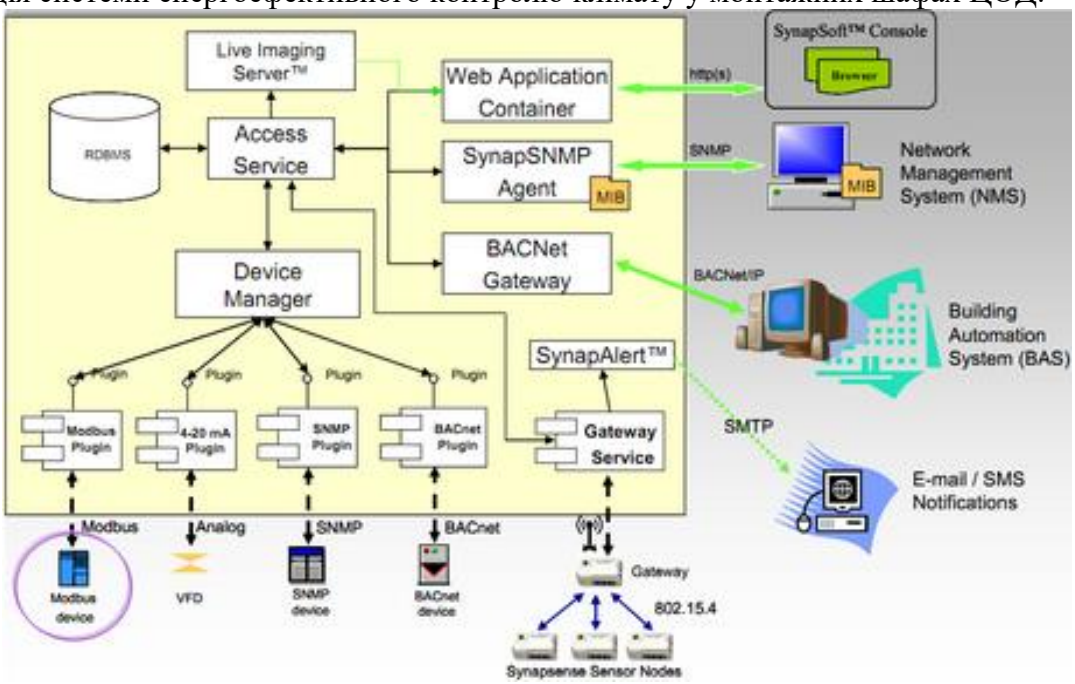


Рисунок 11 – Структурна схема системи

Ядро програмної реалізації системи енергоефективного контролю клімату у монтажних шафах ЦОД складається з керуючих служб, бази даних і менеджера пристроїв. Система плагінів дозволяє підключити до ядра адаптери технологічних протоколів (Modbus,

BACNet, SNMP) і ліній електроживлення. За допомогою цих протоколів відбувається керування вентиляторами, кондиціонерами й іншими пристроями активно впливають на кліматичні параметри. Моніторинг кліматичних параметрів відбувається за допомогою сенсорних пристроїв, що використовують бездротову мережу. Керування системою відбувається за допомогою веб-консолі, а повідомлення про події за допомогою електронної пошти й SMS оповіщень. Як діагностичне рішення використовується стандартний SNMP протокол, що поєднує в собі завдання керування й моніторингу.

Типові проблеми

Ключовою проблемою є широке різноманіття пристроїв і протоколів, що використовуються в системі. Пристрої ґрунтуються на різних стандартах, використовують різні моделі й протоколи керування, використовують різні транспортні механізми й протоколи, містять різні принципи й механізми самодіагностики. При цьому розроблювачі інтегрують свою систему не тільки з активними кліматичними пристроями, але й із системою керування будівлею, що, безсумнівно, додає хаосу у випадку відмов.

Через різноманіття пристроїв розроблювачам довелося створити надлишкова кількість програмного коду, що обертає функціональність кінцевих пристроїв у терміни й абстракції, якими оперує їхня система, для уніфікації процесу керування пристроями. При цьому очевидно частиною функціональності пристроїв було пожертвувано на користь загального універсалізму. Також часто при уніфікації страждають можливості діагностики, коди помилки пристроїв, перетворюються в коди помилок адаптерів, а ті у свою чергу транслюються у виключення вихідного коду ядра. У підсумку за ширмами рівнів абстракцій і адаптерів протоколів губляться щирі причинно-наслідкові зв'язки між відмовою конкретного пристрою й помилкою, текст якого одержав оператор.

Використання протоколу SNMP сильно обмежує можливості діагностики несправностей. По-перше, відсутня можливість викликати штатні процедури самодіагностики, закладені в кінцеві пристрої. По-друге, відсутня можливість протестувати мережні з'єднання і їхня якість, оскільки SNMP має на увазі наявність працездатної мережі. По-третє, SNMP сильно обмежує деталізацію діагностичної інформації, що може надати кінцевий пристрій. По-четверте, використання стандартних засобів SNMP і MIB має на увазі відсутність централізованого тестування й механізмів аналізу діагностичної інформації. Отже, рішення про характер несправності повинен приймати оператор системи, не завжди досконально знаючої особливості її технічної реалізації. У підсумку до людського фактора при ухваленні рішення додається звичайна некомпетентність.

Типові наслідки

Недостатність діагностичної інформації приводить до неправильної діагностики відмови й помилковому вибору шляхи усунення несправності. Найчастіше при усуненні несправності оператори системи мимоволі видаляють всі сліди відмови разом з перезавантаженим або утилізованим функціональним блоком. Що не дозволяє розслідувати реальну причину відмови з метою запобігання несправностей подібного типу в майбутньому. Неефективні способи усунення відмов ведуть до:

- необґрунтованому завищенню вартості експлуатації системи;
- збільшенню часу усунення несправності;
- неможливості з'ясувати реальну причину відмови;
- більше важким наслідкам при розростанні відмови.

Застосування розробленої програмної реалізації системи енергоефективного контролю клімату у монтажних шафах ЦОД

Розроблена програмна реалізація системи енергоефективного контролю клімату у монтажних шафах ЦОД ідеально інтегрується із цією системою, оскільки для рішення вищевказаних проблем і було розроблено. Адаптери технологічних протоколів будуть перетворювати діагностичну інформацію без яких-небудь втрат у діагностичні контейнери. Крім того кожний адаптер буде містити тести самодіагностики кожного кінцевого пристрою, які будуть не тільки викликати функції самодіагностики пристроїв, але й проводити свою

перевірку їхньої працездатності, використовуючи інтерфейс керування пристроєм. Навіть повідомлення SNMP за допомогою відповідного SNMP адаптера будуть перетворені в діагностичні контейнери. У бездротові сенсорні пристрої буде убудована функціональність розробленої програмної реалізації системи енергоефективного контролю клімату у монтажних шафах ЦОД, що перевіряє пристрій зсередини й надає максимально можливу деталізацію діагностики пристрою. Точно також у кожний програмний модуль системи будуть убудовані діагностичні можливості розробленої програмної реалізації системи енергоефективного контролю клімату у монтажних шафах ЦОД, що протоколюють кожну дію, як системи, так і її операторів, і які забезпечують повну самодіагностику за допомогою широкого набору тестів. Експертна база знань буде постачати операторів системи найбільш точними відомостями про відмову й способи його усунення. При цьому розроблювачі системи за допомогою захищеного вилученого доступу можуть у ручному режимі перевіряти правильність висновків експертної системи, правильність функціонування системи клімат-контролю й послідовність дій її операторів.

Що дає розроблена програмна реалізація системи енергоефективного контролю клімату у монтажних шафах ЦОД:

– Одержання достовірної й оригінальної діагностичної інформації від кінцевих пристроїв операторами системи. Це дозволить найбільше точно локалізувати місце й визначити причину несправності.

– Одержання детальної інформації про те, як відмова пристрою вплинула на систему в цілому, які модулі і як були порушені. Це дозволить розроблювачам системи коректувати її архітектуру так, щоб у майбутньому подібні відмови зачіпали б якнайменше модулів. І по можливості модуль, що відмовив, автоматично б замінявся працездатним модулем.

– Наявність деталізованої діагностичної інформації дозволяє експертній системі вибрати найбільш коректний висновок про несправності й спосіб її усунення. Таким чином, мінімізується людський фактор і компенсується відсутність інженерів, що досконально знають систему. Крім того, значно заощаджується час ухвалення рішення й зменшується час відновлення працездатності системи.

– Наявність тестів самодіагностики кожного модуля дозволяє підтвердити первісний діагноз і симптоми несправності. Це збільшує якість діагностики.

– Щоденний запуск процедур самодіагностики всього комплексу дозволяє виявляти пристрої, функціонування яких перебуває під сумнівом, конфігураційні помилки, допущені операторами системи й т.д. Подібні превентивні міри дозволять значно збільшити надійність системи клімату-контролю.

– Значне збільшення надійності системи клімат-контролю веде, відповідно, до значного збільшення надійності центра обробки даних.

Висновок. У статті розглянуто та проаналізовано програмне забезпечення, яке призначено для системи енергоефективного контролю клімату у монтажних шафах ЦОД. В межах України в недостатній мірі представлені вітчизняні розробки в цій області. У роботі наведені теоретичне узагальнення й рішення наукового завдання дослідження методів енергоефективного контролю клімату у монтажних шафах ЦОД. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем енергоефективного контролю клімату у монтажних шафах ЦОД; Досліджена система енергоефективного контролю клімату у монтажних шафах ЦОД; На основі отриманих результатів досліджень створена програмна реалізація системи енергоефективного контролю клімату у монтажних шафах ЦОД. Розроблені під час виконання роботи алгоритми дозволяють успішно вирішувати завдання енергоефективного контролю клімату у монтажних шафах ЦОД. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Розроблене програмне забезпечення має простий, дружній та зручний інтерфейс користувача, що забезпечує легкість у освоєнні роботи програмного продукту, зручність у використанні, і не потребує особливих спеціальних знань. При створені програмного забезпечення було використано об'єктно-орієнтований підхід, що відповідає сучасним тенденціям у галузі розробки комерційних програмних систем. Програма реалізована на мові високого рівня Embarcadero Delphi 10.2 Tokyo. Дана мова програмування дозволяє найбільш ефективно обробляти дані. Це дозволило мінімізувати строк розробки програмного забезпечення, і, як слід, зменшити витрати на його розробку. Запропоноване програмне забезпечення ділиться на загальне програмне забезпечення, що поставляється із засобами обчислювальної техніки й спеціальне програмне забезпечення, що спеціально розроблене для даної конкретної системи й включає програми, що реалізують її функції. Для підвищення рівня безпеки запропоновано застосовувати алгоритм Khufu.

Список літератури

1. Коваленко А.С. Задачи распознавания ситуаций в ERP системах / А.В. Коваленко ., А.А. Смірнов, А.С. Коваленко // Системи обробки інформації. – Х.: ХУПС, 2014. – Вип. 4(120). – С. 161-164.
2. Коваленко А.С. Підсистема технічної діагностики для автоматизації процесів керування в інтегрованих інформаційних системах / А.С. Коваленко , О.А.Смірнов, О.В. Коваленко // Системи озброєння і військова техніка.– Х.: ХУПС, 2014. – № 1(37). – С. 126-129.
3. Коваленко А.С. Анализ эффективности использования экспертной системы технической диагностики с традиционной структурой / А.С. Коваленко, А.А. Смирнов, А.В. Коваленко // Системи озброєння і військова техніка. – Х.: ХУПС, 2014. – № 2(38). – С. 106-108.
4. Коваленко А.С. Разработка структуры экспертной системы технической диагностики интегрированной информационной системы / А.С. Коваленко, А.А. Смирнов, А.В. Коваленко // Наука і техніка Повітряних Сил Збройних Сил України. – Харків: ХУПС, 2014. – № 2(15). – С.154-157.
5. Коваленко А.С. Разработка структуры экспертной системы технической диагностики интегрированной информационной системы / А.С. Коваленко, А.А. Смирнов, А.В. Коваленко // Наука і техніка Повітряних Сил Збройних Сил України. – Харків: ХУПС, 2014. – № 2(15). – С.154-157.
6. Коваленко А.С. Структура системи технічної діагностики інтегрованих інформаційних систем / А.С. Коваленко, О.А. Смірнов, О.В. Коваленко // Збірник наукових праць Кіровоградського національного технічного університету / техніка в сільськогосподарському виробництві, галузеве машинобудування, автоматизація. – Кіровоград: Вид-во КНТУ, 2014. – Вип. 27. – С. 245-251.
7. Коваленко А.С. Дослідження будови інтегрованої інформаційної системи та її елементів / А.С. Коваленко, О.А. Смірнов, О.В. Коваленко // Системи озброєння і військова техніка. – Х.: ХУПС, 2014. – № 4(40). – С. 85-88.
8. Коваленко А.С. Розробка структури бази даних для обліку технічного стану елементів інтегрованої інформаційної системи з урахуванням вимог споживачів інформації / А.С. Коваленко, О.А. Смірнов, О.В. Коваленко // Системи обробки інформації. – Х.: ХУПС, 2015. – Вип. 1(126). – С. 75-79.
9. Коваленко А.С. Обґрунтування набору даних для оцінки технічного стану інтегрованої інформаційної системи / А.С. Коваленко, О.А. Смірнов, О.В. Коваленко // Збірник наукових праць Харківського університету Повітряних Сил. – Харків: ХУПС, 2015. – Вип. 1(42). – С.39-41.
10. Коваленко А.С. Експертна система технічного діагностування інтегрованої інформаційної системи / А.С. Коваленко, О.А. Смірнов, О.В. Коваленко // Системи озброєння і військова техніка. – Х.: ХУПС, 2015. – № 1(41). – С. 106-111.

УДК 004

С. Охотний, магістр гр. КІ-18М-1,4
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ АНАЛІЗУ СТРУКТУРИ ТА КОНТЕНТУ СОЦІАЛЬНИХ МЕРЕЖ

У статті розроблено програмне забезпечення, яке призначено для системи аналізу структури та контенту соціальних мереж. Метою розробки є дослідження та програмна реалізація системи аналізу структури та контенту соціальних мереж. Об'єктом дослідження є процес аналізу структури та контенту соціальних мереж. Предметом дослідження є методи аналізу структури та контенту соціальних мереж. Методи дослідження базуються на методах аналізу графів, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи аналізу структури та контенту соціальних мереж. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення. Розроблено зручний інтерфейс користувача. Наведені інструкції по роботі з програмними засобами. Програму розроблено в середовищі MS Visual Studio з використанням системи керування графової бази даних Neo4j.
комп'ютерна інженерія, аналіз соціальних мереж, соціальний граф

Постановка проблеми. Соціальні Інтернет-мережі (Facebook, VKontakte, Twitter, та багато інших) є основою взаємовідносин у сучасному суспільстві. Чимало людей мають облікові записи відразу в декількох з них. За допомогою соціальних мереж люди знаходять друзів, спілкуються, об'єднуються за інтересами, обмінюються інформацією. Як результат,в наш час соціальні мережі значним чином впливають на поведінку людей. Вони стали інструментом впливу та прихованого контролю над соціумом. Масштаби такого контролю можуть варіюватися від просування різних товарів до організації масових суспільних протестів (Туніс, Гонконг, Великобританія, Україна і т.д.). Таким чином, необхідно розробляти засоби, які дадуть можливість виявляти інформаційні загрози для суспільства, основним джерелом яких є соціальні онлайн мережі.

Проблема інформаційної безпеки населення стала однією з найбільш важливих для України на сьогоднішній день. Наша країна знаходиться під постійним тиском пропаганди агресора, і тому для виявлення розповсюджувачів вірусної інформації в соціальних мережах та ефективній протидії необхідно розробляти відповідне програмне забезпечення. Системи аналізу соціальних мереж дають можливість знаходити найбільш впливових представників мережі та слідкувати за їхньою діяльністю, а також за активністю людей які підпадають під їхній вплив. Також аналіз соціальних мереж дає можливість виявляти ймовірності та шляхи поширення вірусної інформації у суспільстві, знаходити учасників мережі, які намагаються маніпулювати свідомістю інших або потенційно можуть це робити.

У травні 2017 року п'ятий президент України Петро Порошенко указом обмежив доступ до соціальних інтернет-мереж «ВКонтакті», «Одноклассников», пошуковика «Яндекс» з його інструментами і поштового сервісу «Mail.ru». Проте найпоширеніша мережа у світі Facebook, залишилася доступною.

«Дослідник медійних комунікацій, один з керівників інформаційного проекту «Майдан Прес Центр» Алекс Беккер нарікає на брак контролю за повідомленнями на рекламних платформах у соцмережах. Ці платформи перетворені на агітаційні платформи, окремі держави використовують їх як місця для поширення пропаганди та політичної реклами. Негативний вплив таких маніпулятивних дій показали вибори президента США минулого року, цьогорічні вибори у Німеччині та Франції, каже експерт.

у 2014-15 роках проросійські «тролі», маніпулюючи правилами соцмережі Facebook, блокували українських волонтерів та громадських активістів за нібито розпалювання ворожнечі, а фактично – за поширення інформації про бойові дії на сході України, про вторгнення російських військ тощо. Відтак, вважає Беккер, необхідно аналізувати контент соціальних мереж і не допускати поширення пропаганди, брехні тощо [1]».

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи аналізу структури та контенту соціальних мереж.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи аналізу структури та контенту соціальних мереж.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючого програмного забезпечення для аналізу структури та контенту соціальних мереж;

– Дослідження існуючих алгоритмів аналізу графів;

– Програмна реалізація алгоритмів аналізу графів, алгоритмів виділення кластерів в графі, візуалізація даних;

– Розробка програмного рішення системи аналізу структури та контенту соціальних мереж.

Об'єктом дослідження є процес аналізу соціальних мереж.

Предметом дослідження є методи виділення соціальних груп з графу соціальної мережі.

Виклад основного матеріалу. Основним завданням, яке вирішує розроблена програмна система, є збір, зберігання та аналіз даних, які завантажуються з інтернету, а саме з сайту соціальної мережі Facebook.Також система виконує візуалізацію даних.

Для того, щоб отримати дані з сайту соціальної мережі, необхідно скласти ланцюг пошукових запитів. Результат виконання кожного запиту, подається на вхід іншого пошукового запиту. Таким чином можна складати складні вирази для пошуку необхідної інформації в соціальній мережі. Вхідними даними для першого пошукового запиту в ланцюгу є посилання на сторінку сутності, відносно якої виконується запит.

Основними сутностями, які розпізнає програмна система в соціальній мережі, є: користувач, група, пост, сторінка (мається на увазі поняття сторінки у фейсбуці – сутність схожа на групу, але зазвичай представляє, якийсь бренд, компанію або публічну людину).

Між зазначеними сутностями в соціальній мережі існують зв'язки, саме вони представляють найбільший інтерес для аналізу. Пошукова система розпізнає наступні зв'язки:

1) підписник/послідовник – зв'язок між двома користувачами, або користувачем і сторінкою;
2) дружба – зв'язок між двома користувачами;
3) автор – зв'язок між користувачем і постом;
4) член групи – зв'язок між користувачем і групою, або сторінкою і групою;
5) лайк – зв'язок між користувачем і постом.

Кожен запит по суті є пошуком даних за конкретним зв'язком. Наприклад, запит на пошук друзів вказаного користувача або його підписників. Результати пошуку заносяться в базу даних системи. Таким чином відбувається локальне накопичення даних. Це дає змогу пришвидшити виконання ланцюга пошукових запитів за рахунок можливості виконання окремих запитів не на сайті, а на базі даних. Після того як виконається увесь ланцюжок пошукових запитів, програма відобразить результат на графі, де можна буде проаналізувати структуру отриманої мережі й самі дані.

Розроблена програмна система дає можливість виконувати аналіз отриманих даних, а саме визначення трьох типів центральностей: центральності за степенем, центральності за бизькістю та центральності за посередництвом.

Центральності дають можливість оцінити рівень помітності і впливу користувачів (акторів) один на одного.Ідея центральності вершин в графі, а саме їх значення, з'явилася однією з перших в методології аналізу соціальних мереж, і безпосередньо пов'язується з першими спробами Дж. Морено (видатний австрійсько-американський психіатр, соціальний психолог, психотерапевт, соціолог, філософ, засновник психодрами, соціометрії та групової психотерапії) виявити найпопулярніших учасників в групі «соціометричних зірок». Пізніше цей підхід помітності актора в мережі почав називатися центральністю.

Близькість до центру або ступінь центральності – показує, хто є найбільш активним вузлом в мережі. Вимірюється кількістю зв'язків з іншими вузлами в мережі. Центральність показує, наскільки даний вузол близький по відношенню до інших вузлів в мережі.

Центральність за степенем

Центральність за степенем дозволяє виділити акторів, які пов'язані з максимальною кількістю інших учасників мережі (якщо актор володіє великою кількістю вихідних зв'язків, це часто вказує на його владні функції, якщо ж актор має велику кількість вхідних зв'язків це вказує на його популярність в даній мережі).

Актор, який має більше зв'язків з іншими, знаходиться в більш вигідному становищі. Велика кількість зв'язків дає йому більше альтернатив для знаходження ресурсів і розповсюдження свого інформаційного впливу і, водночас, меншу залежність від кожного суб'єкта мережі.

В ненаправлених зв'язках степінь залежить лише від кількості з'єднань з іншими акторами. Для направлених зв'язків слід розрізняти, які зв'язки актора є вхідними, а які вихідними. Суб'єкти, які мають багато вхідних зв'язків мають високий авторитет, тобто багато інших акторів прагнуть мати з ними прямий контакт. Актори, які мають багато вихідних зв'язків мають високу впливовість, бо можуть поширювати свою думку серед великої кількості суб'єктів мережі. Стандартизований індекс центральності за степенем обчислюють за формулою:

$$C_D(n_i) = \frac{d(n_i)}{N}, \quad (1)$$

де N – загальна кількість акторів у мережі;

$d(n_i)$ – ступінь вузла n_i.

Центральність за степенем є ефективною для мереж із "зіркоподібним" розташуванням акторів. Але для лінійних структур її використання може призвести до помилкових висновків щодо впливовості акторів. В таких мережах вимірювання центральності доцільно здійснювати на основі близькості.

Центральність за близькістю

Дослідження центральності за близькістю дозволяє виділити акторів, через яких проходить максимальна кількість найкоротших шляхів, які сполучають між собою інших учасників мережі.

Визначення центральності за близькістю базується на понятті геодезичної (найменшої) відстані між акторами – $d(n_i, n_j)$. Чим меншими є відстані від даного актора до всіх інших акторів, тим більш центральним є його розташування. Найпростішим показником центральності за близькістю є загальна сума найкоротших відстаней даного актора до інших. Стандартизований індекс центральності за близькістю підраховується за формулою:

$$C_i(n_i) = \sum_{i=1}^{N} \frac{1}{d(n_i n_j)} \quad (2)$$

Центральність за близькістю дозволяє виявити користувачів мережі, що мають максимальну незалежність від інформаційних впливів інших учасників мережі.

Центральність за посередництвом

Найбільший інтерес з точки зору інформаційної безпеки являє дослідження центральності за посередництвом. Актори, які мають високий показник центральності за посередництвом слугують єдиною зв'язуючою ланкою між великою кількістю інших учасників мережі. Завдяки цьому вони мають високий потенціал для здійснення впливу на інших учасників мережі та можуть використовувати своє розташування як для розпалювання

конфліктів між іншими учасниками мережі шляхом дезінформації так і для врегулювання конфліктних ситуацій. Найпростішим показником центральності за посередництвом є кількість геодезичних шляхів між акторами *j* та*k*, що вміщують актора *i*: $g_{jk}(n_i)$.

Стандартизований індекс центральності за розташуванням на найменших відстанях має діапазон значень від 0 до 1 і для мереж ненаправлених відношень підраховується за формулою:

$$C_B(n_i) = \frac{C_B(n_i)}{[(N-1)*(N-2)]/2} \quad (3)$$

Для мереж направлених відношень використовується наступна формула обрахунку індексу центральності за розташуванням на найменших відстанях:

$$C_B(n_i) = \frac{C_B(n_i)}{(N-1)*(N-2)} \quad (4)$$

Центральність за посередництвом є мірою контролю мережевих ресурсів актором.

Застосування засобів Neo4j для визначення центральностей

Neo4j – це графова СКБД, однією з найбільших переваг якої є набір вбудованих алгоритмів аналізу графової інформації зокрема є алгоритми які застосовуються при аналізі соціальних мереж, а саме визначення центральностей (степенева центральність, центральність за посередництвом, центральність за близькістю). Також реалізовані алгоритми визначення групи, а саме алгоритми визначення сильно та слабко пов'язаних вузлів, алгоритм визначення коефіцієнту кластеризації, а також розповсюдженості певної інформації (бренду). Крім того є алгоритми з пошуку найкоротшого шляху в графі та алгоритми доступності та якості шляху.

Всі алгоритми представляються у вигляді процедур. Їх можна викликати безпосередньо в Cypher з браузера Neo4j, з cypher-shell, або з клієнтського коду. Для більшості алгоритмів пропонуються по дві процедури: одна з назвою algo.<ім'я>, яка записує результати в граф у вигляді властивостей вузлів та звітної статистики; та інша з назвою algo.<ім'я>.stream, яка повертає результат у вигляді потоку даних, наприклад ідентифікатори вузлів та обчисленні значення. Для великих графів процедура потокового відтворення може повернути мільйони або мільярди результатів, тому зазвичай зручніше зберігати результати алгоритму, а потім використовувати їх з пізнішими запитами.

Приклади Cypher-запитів для визначення степеневої центральності, центральності за посередництвом та центральностіза близькістю,використовуючи процедури потокового відтворення, показано відповідно в лістингу 1, в лістингу 2 та в лістингу 3.

Лістинг 1 – Запит для визначення степеневої центральності з використанням процедури потокового відтворення:

```
CALL algo.pageRank.stream(
  'MATCH (u:User) WHERE exists( (u)-[:FRIENDS]-() ) RETURN id(u) as
id',
  'MATCH (u1:User)-[:FRIENDS]-(u2:User) RETURN id(u1) as source,
id(u2) as target',
  {graph:'cypher'}
) YIELD node,score with node,score order by score desc limit 10
RETURN node {.name, .review_count, .average_stars,.useful,.yelping_since,.funny}, score
```

Лістинг 2 – Запит для визначення центральності за посередництвомз використанням процедури потокового відтворення:

```
CALL algo.betweenness.stream('User','MANAGE',{direction:'out'})
YIELD nodeId, centrality
RETURN nodeId,centrality order by centrality desc limit 20;
```

Лістинг 3 – Запит для визначення центральності за близькістюз використанням процедури потокового відтворення:

```
CALL algo.closeness.stream('Node', 'LINKS') YIELD nodeId, centrality
RETURN nodeId,centrality order by centrality desc limit 20;
```

Приклади Cypher-запитів для визначення степеневої центральності, центральності за посередництвом та центральності за близькістю, використовуючи процедури, які записують результат в граф, показано відповідно в лістингу 4, в лістингу 5 та в лістингу 6.

Лістинг 4 – Запит для визначення степеневої центральності з використанням процедури, яка записує результат в граф:

```
CALL algo.pageRank(
  'MATCH (p:Page) RETURN id(p) as id',
  'MATCH (p1:Page)-[:Link]->(p2:Page) RETURN id(p1) as source, id(p2) as target',
  {graph:'cypher', iterations:5, write: true}
)
```

Лістинг 5 – Запит для визначення центральності за посередництвомз використанням процедури, яка записує результат в граф:

```
CALL algo.betweenness(label:String, relationship:String,
{direction:'out',write:true, stats:true,
writeProperty:'centrality',concurrency:1})
YIELD nodes, minCentrality, maxCentrality, sumCentrality, loadMillis, computeMillis, writeMillis
```

Лістинг 6 – Запит для визначення центральності за близькістю з використанням процедури, яка записує результат в граф:

```
CALL algo.closeness('Node', 'LINK', {write:true,
      writeProperty:'centrality'})
YIELD nodes,loadMillis, computeMillis, writeMillis;
```

Таким чином, Neo4jнадає всі необхідні засоби для проведення аналізу центральностей на основі завантаженої графової інформації.

Розробка структурної схеми

Структурна схема відображає склад і взаємодію частин розроблюваного програмного забезпечення і визначається його архітектурою.

Джерелом інформації для програмної системи є соціальна інтернет-мережа, а саме Facebook. Для взаємодії з соціальною мережею був розробленииий кроулер, який виконує парсинг необіхноїї інформації з сторінок сайту Facebook.Завантажена інформація зберігається в локальній графовій СКБД Neo4j, взаємодія з якою відбувається через менеджер бази даних. Завантажувана інформація з соціальної мережі визначається пошуковим запитом, який відправляється до кроулера менеджером ланцюгів пошукових запитів. Результат роботи кроулера повертається назад(до менеджера пошукових запитів) після чого нові дані надсилаються до бази даних.

Ланцюг пошукових запитів створюється користувачем з допомогою графічного інтерфейсу, після чого він потрапляє до менеджера ланцюгів пошукових запитів, який в свою чергу розбиває ланцюг на окремі запити. Кожен пошуковий запит в залежності від його типу (онлайн або офлайн) відправляється на виконання до кроулера або до локальної бази даних. Тип пошукового запиту обирається користувачем при його створенні за допомогою графічного інтерфейсу програми. Аналіз центральностей виконується аналізатором даних, який відправляє відповідні запити до менеджера бази даних Neo4j, а результати надсилає до графічного інтерфйсу користувача.

На рис. 1 наведено структурну схему розробленого програмного забезпечення.

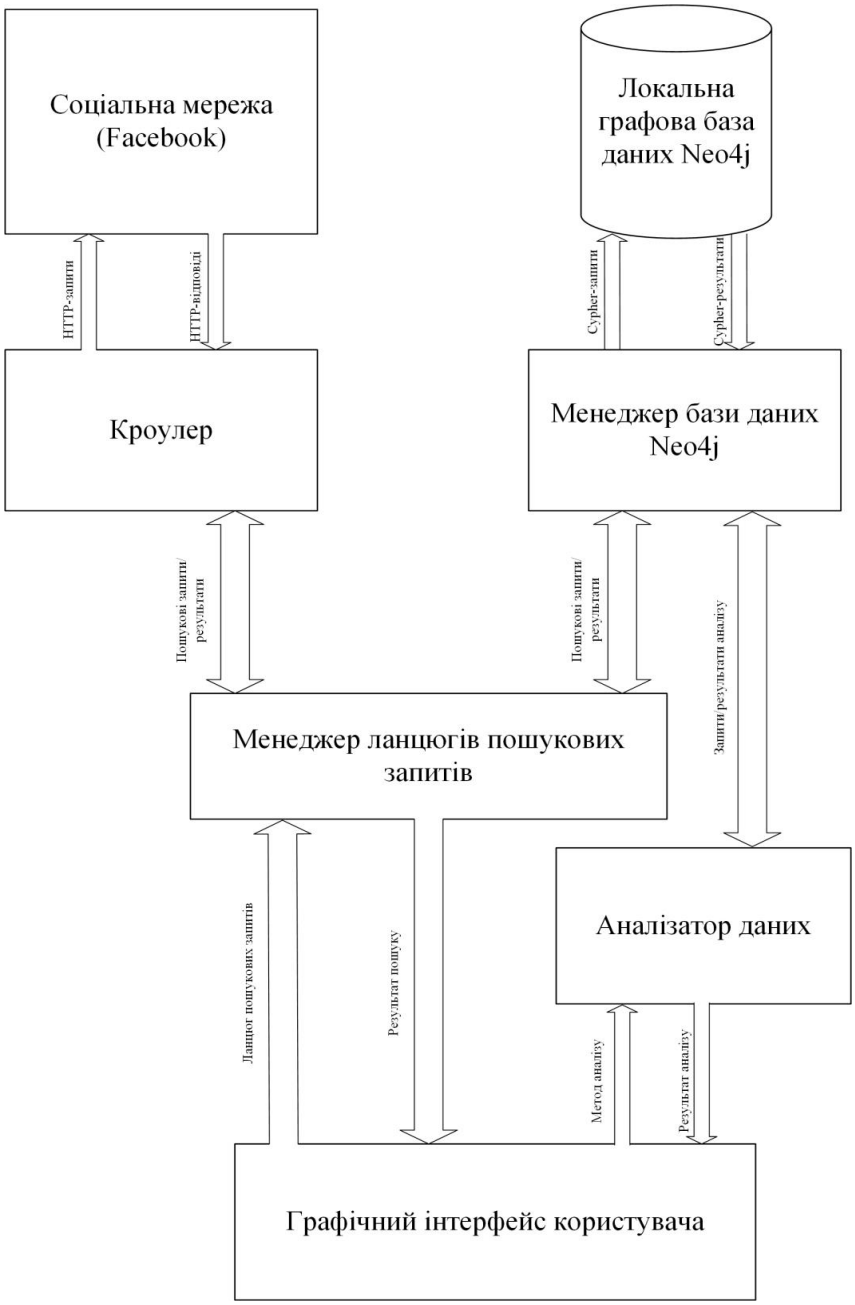


Рисунок 1 – Структурна схема програмної системи

Висновок. У статті розглянуто та проаналізовано програмне забезпечення, яке призначено для проведення збору, збереження та аналізу даних з соціальної мережі facebook. Програмний продукт дає змогу виконувати аналіз завантажених даних, а саме визначення центральностей соціального графу з метою визначення найбільш впливових представників мережі, а також виділення соціальних груп. В подальшому програмне забезпечення можна використовувати для виявлення впливових людей в соціальній мережі, для перевірки розповсюджуваної ними інформації. При створенні ПЗ в якості середовища розробки було використано IDEVisualStudioCommunity 2017. Для збереження даних була використана графова СКБД Neo4j.Для проведення парсингу html-сторінокбуло обрано фреймворк Selenium з веб-драйверами GeckotaPhantomJS. ПЗ реалізовано мовою програмування C# використовуючи платформу .Net, інтерфейс програми реалізовано на мові XAML для графічної підсистеми WPF. Дані мови дають широкий спектр можливостей для ефективної реалізації ПЗ, зокрема XAMLбуло використано для побудови візуального відображення графової інформації на основі патерна MVC. Розроблене програмне забезпечення призначене

для використання на персональних комп'ютерах під управлінням операційної системи Windows 10. Для роботи програмного забезпечення необхідний сервер Neo4j, який необхідно встановити окремо, створити базу даних та користувача. Логін та пароль користувача необхідні будуть під час входу в програмне забезпечення. В цілому створене програмне забезпечення відповідає розробленому технічному завданню та підтверджує правильність використаних програмних рішень. Створене ПЗ має можливості для вдосконалення у майбутньому.

Список літератури

1. Vincent D. Blondel, Jean-Loup Guillaume, Renaud Lambiotte, Etienne Lefebvre, Department of Mathematical Engineering, Universit´e catholique de Louvain, avenue Georges Lemaitre, B-1348 Louvain-la-Neuve, Belgium.
2. Макконнелл С. Профессиональная разработка программного обеспечения. – Пер. с англ. – СПб.: Символ&Плюс, 2006. – 240 с., ил.
3. Соммервилл, Иан. Инженерия программного обеспечения, 6-е издание. : Пер. с англ. – М.: Издательский дом «Вильямс», 2002. – 624 с.: ил. – Парал. тит. англ.
4. Гамма Э., Хелм Р., Джонсон Р., Влиссидес Дж. Приемы объектно-ориентированого проектирования. Паттерны проектирования. – СПб: Питер, 2001. – 368 с.: ил.
5. Каплун, В. А.Захист програмного забезпечення. Частина 2 : навчальний посібник / В. А. Каплун, О. В. Дмитришин, Ю. В. Баришев – Вінниця : ВНТУ, 2014. – 105 с.
6. Amrit C. A Social Network perspective of Conway's Law / Chintan Amrit.
7. Береза А. М. Основи створення інформаційних систем / А. М. Береза.
8. Мазуренко В. В. Огляд моделей аналізу соціальних мереж / В. В. Мазуренко.
9. Гасько Р. В. Інформаційна система аналізу психологічного стану особистості / Р. В. Гасько. – Львів, 2015.
10. Радівілова Т. Огляд видів аналізу соціальних мереж для забезпечення інформаційної безпеки / Т. Радівілова, Л. Кіріченко, Д. Рудченко.

УДК 004

Є. Палєсіка, магістр гр. КН-18-1,4
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ КОНСТРУЮВАННЯ ІГОР-КВЕСТІВ НА ANDROID

У статті розроблено програмне забезпечення, яке призначено для системи конструювання ігор-квестів на Android. Метою розробки є дослідження та програмна реалізація системи конструювання ігор-квестів на Android. Об'єктом дослідження є процес конструювання ігор-квестів на Android. Предметом дослідження є методи конструювання ігор-квестів на Android. Методи дослідження базуються на методах теорії моделювання, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи конструювання ігор-квестів на Android. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення. Розроблено зручний інтерфейс користувача. Наведені інструкції по роботі з програмними засобами.

комп'ютерні науки, ігри-квести, Android

Постановка проблеми. Мобільні телефони давно перестали бути чимось незвичайним і чудово справляються зі своєю функцією, яка є засобом комунікації між людьми. При цьому, смартфони, які зовсім недавно з'явились, але вже міцно увійшли в наше життя, настільки функціональні, що важко сказати чого вони не вміють: це і музичний

програвач, і фотоапарат, і можливість використання Інтернет-ресурсів, та інше. По суті, всі смартфони стали невеликої копією комп'ютера, який постійно можна мати при собі.

У наш час все більше і більше смартфонів, комунікаторів, планшетних ПК і інших видів пристроїв зручних для використання, як в повсякденному житті, так і в ігровій індустрії, випускаються на базі ОС Android.

По-перше, Android підтримує велику кількість пристроїв різних виробників. По-друге, Android характеризується високою доступністю засобів розробки. Засоби розробки для платформи Android безкоштовні, в той час як розробка, наприклад, під iPhone (від компанії Apple) вимагає чималих початкових фінансових вкладень. Крім усього перерахованого вище, перевагою ОС Android є наявність безкоштовних бібліотек для роботи зі сторонніми ресурсами (MapKit, Google Map API, ін.), В той час як для Windows Phone Mobile такі бібліотеки не поширені.

Завдання – розробити програмне забезпечення системи конструювання ігор-квестів на Android, з можливістю створення квестових ігор, запису до бази даних, а також можливістю отримати доступ до цієї бази з будь-якої операційної системи, для виводу квестової гри, яка була створена користувачем. Операційна система Android створена для смартфонів, планшетних комп'ютерів, цифрових програвачів, цифрових фоторамок, годинників, нетбуків та смартбуків, заснована на ядрі Linux. Основною мовою для розробки служить Java, проте існують бібліотеки які дозволяють вести розробку на мові C++, C#, Python, Javascript.

На основі загальних принципів побудови та роботи мобільних застосунків було сформоване технічне завдання, згідно якого розроблене програмне забезпечення системи конструювання ігор-квестів на Android, орієнтоване на використання звичайними користувачами на своїх мобільних пристроях.

Проведений аналіз інтерактивних ігор показав, що вони мають велику популярність і існує багато різних застосунків, але всі вони не мають мобільної можливості створення або конструювання користувачами квестових ігор.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи конструювання ігор-квестів на Android.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи конструювання ігор-квестів на Android.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем конструювання ігор-квестів на Android.
– Дослідження системи конструювання ігор-квестів на Android.
– Програмна реалізація системи конструювання ігор-квестів на Android.

Об'єктом дослідження є процес конструювання ігор-квестів на Android.

Предметом дослідження є методи конструювання ігор-квестів на Android.

Методи дослідження базуються на методах теорії моделювання, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. При аналізі завдання було вирішено використовувати методику ієрархічного поділу системи, так як завдяки цієї методики, можна оптимізувати код, а також відділити візуальну частину від роботи з моделями. Це допоможе в швидкодії застосунку, в його розширюваності і в провадженні нового функціоналу.

Для реалізації проекту необхідно умовно поділити систему на верхній, нижній та проміжний рівень. Нижній рівень є рівнем, який буде відповідати за збір даних та передачу цієї інформації на проміжний рівень. Проміжний рівень буде слугувати для того щоб приймати інформацію з нижнього рівня і записувати прийняті дані у базу даних. Верхній рівень представляє собою візуалізацію прийнятої інформації з нижнього рівня, яка знаходиться у базі даних. Розглянемо більш детально роботу кожного рівня системи.

Нижній рівень представляє собою централізований вузол збору інформації та дочірні вузли збору інформації. Дочірніми вузлами збору інформації виступають класи для роботи з

системою Firebase.

База даних – сукупність даних, які організовані відповідно до концепції, яка описує характеристику цих даних і взаємозв'язки між їх елементами; ця сукупність підтримує щонайменше одну з областей застосування (за стандартом ISO/IEC 2382:2015). В загальному випадку база даних містить схеми, таблиці, подання, збережені процедури та інші об'єкти. Дані у базі організовують відповідно до моделі організації даних. Таким чином, сучасна база даних, крім саме даних, містить їх опис та може містити засоби для їх обробки.

Для централізованих вузлів збору розроблено базу даних, в якій зберігається основна інформація про користувача та історії які створив користувач. Для реалізації цього завдання використана база даних Firebase і створені наступні таблиці: users, stories.

Таблиця users містить основні дані про користувача: авторське ім'я, uid (унікальний ідентифікатор, який використовується для ідентифікації користувача), оцінка.

Таблиця stories використовується для зберігання створених користувачем історій. Вона містить таки дані: uid (ідентифікатор користувача), title, description, background, timestamp.

Проміжний рівень системи використовується для того, щоб приймати інформацію, яка зберігається у централізованих вузлах збору та зберігати її у своїй базі даних. Для організації роботи системи створено базу даних, яка складається з певних таблиць, що відображають логіку створеної системи та серверу, що приймає інформацію та записує її у базу даних.

Верхній рівень представляє собою Android-додаток, який оброблює дані які створив користувач, записує їх в базу під його унікальним uid, а також для візуалізації інформації прийнятої з бази даних.

Виходячи с цього, можна представити шаблон проектування MVP. Model-View-Presenter (MVP) – шаблон проектування, який використовується в основному для побудови призначеного для користувача інтерфейсу. Його принцип роботи зображений на рисунку 1.

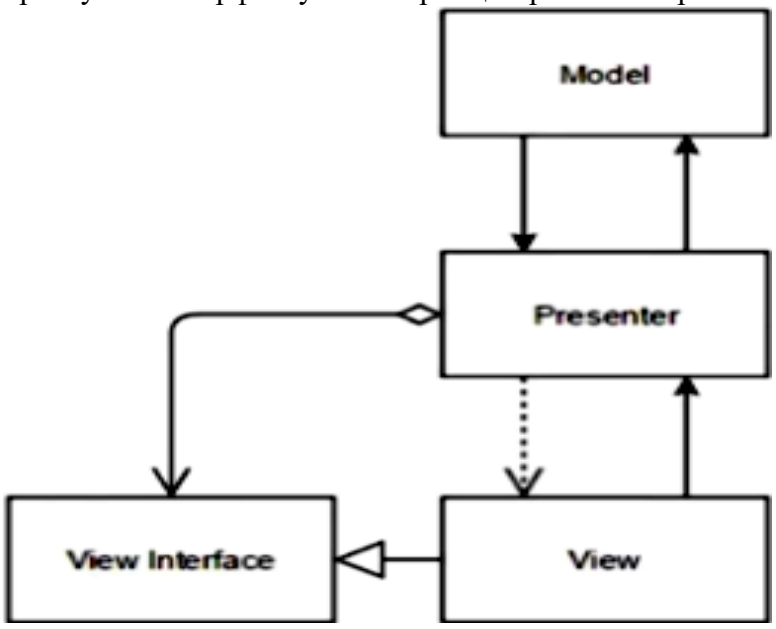


Рисунок 1 – Шаблон проектування MVP

Елемент Presenter в даному шаблоні бере на себе функціональність посередника і відповідає за управління подіями призначеного для користувача інтерфейсу так само, як в інших шаблонах зазвичай відповідає уявлення. В нашому випадку він є проміжним рівнем.

Елемент Model в даному шаблоні зберігає в собі всю бізнес-логіку, при необхідності отримує дані зі сховища і відповідає за оповіщення зміни даних в Presenter. В нашому випадку він є нижнім рівнем.

Елемент View в даному шаблоні реалізує відображення даних (з Моделі), звертається до Presenter за оновленнями. В нашому випадку він є верхнім рівнем.

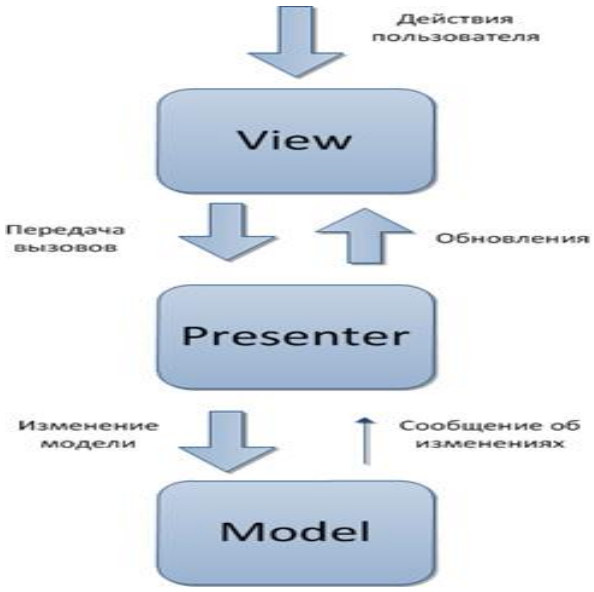


Рисунок 2 – Схема передачі даних в шаблоні MVP

Розробка структурної схеми

Структурна схема – визначає основні структурні частини виробу, їх взаємозв'язки та призначення. Під функціональною частиною розуміють складову частину схеми: елемент, пристрій, структурну групу, функціональну ланку.

Структура програмного забезпечення системи конструювання ігор-квестів на Android складається з трьох ієрархічних рівнів: верхній, нижній та проміжний рівень. Кожен рівень відповідає за свою частину роботи, але залежать від іншого рівня.

Нижній рівень виконує збір інформації з Firebase, зберігає цю інформацію у локальній базі даних Android застосунку та передає цю інформацію на проміжний рівень.

Проміжний рівень приймає інформацію з нижнього рівня та передає цю інформацію на верхній рівень.

Верхній рівень приймає інформацію, зберігає у базі даних та відображає прийняту інформацію за допомогою інтерфейсу.

Як можна побачити зі структурної схеми створеної системи, яка зображена на рисунку 3, кожен рівень спілкується один з одним.

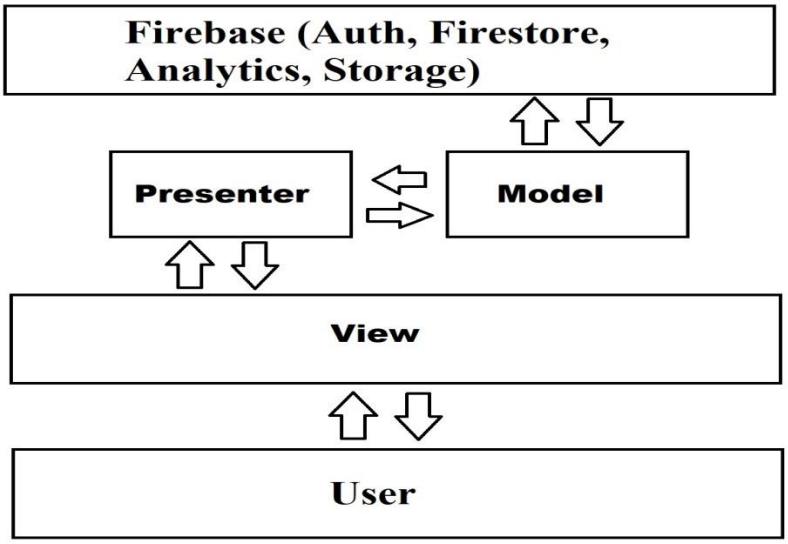


Рисунок 3 – Структурна схема системи

Розроблена структурна схема описує роботу системи і відображає загальну архітектуру програмного забезпечення.

Висновок. У статті розглянуто та проаналізовано програмне забезпечення, яке призначено для системи конструювання ігор-квестів на Android. В межах України в недостатній мірі представлені вітчизняні розробки в цій області. У роботі наведені теоретичне узагальнення й рішення наукового завдання дослідження методів конструювання ігор-квестів на Android. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем конструювання ігор-квестів на Android; Досліджена система конструювання ігор-квестів на Android; На основі отриманих результатів досліджень створена програмна реалізація системи конструювання ігор-квестів на Android. Розроблені під час виконання роботи алгоритми дозволяють успішно вирішувати завдання конструювання ігор-квестів на Android. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки. Розроблене програмне забезпечення має простий, дружній та зручний інтерфейс користувача, що забезпечує легкість у освоєнні роботи програмного продукту, зручність у використанні, і не потребує особливих спеціальних знань. При створені програмного забезпечення було використано об’єктно-орієнтований підхід, що відповідає сучасним тенденціям у галузі розробки комерційних програмних систем. Програма реалізована на мові високого рівня Java, у середовищі розробки Android Studio. Дана мова програмування дозволяє найбільш ефективно обробляти дані. Це дозволило мінімізувати строк розробки програмного забезпечення, і, як слід, зменшити витрати на його розробку. Запропоноване програмне забезпечення ділиться на загальне програмне забезпечення, що поставляється із засобами обчислювальної техніки й спеціальне програмне забезпечення, що спеціально розроблене для даної конкретної системи й включає програми, що реалізують її функції.

Список літератури

1. Дреев А.Н. Использование неравномерного распределения единичных битов для дополнительного сжатия SPIHT кода / А.Н. Дреев, А.А. Смирнов // Информационные системы в управлении, образовании, промышленности: монография. Под редакцией профессора В.С. Пономаренко. – Х.: Вид-во ТОВ «Щедра садиба плюс», 2014. – С. 498.
2. Дрєєв О.М. Дослідження впливу шляху розгортки на ступінь ентропійного стиснення цифрового зображення / О.М. Дрєєв, О.В. Слюсар // Збірник наукових праць Кіровоградського національного технічного університету. Техніка в сільськогосподарському виробництві, галузеве машинобудування, автоматизація. Випуск 21. – Кіровоград: КНТУ. – 2008 – С. 115-118.
3. Дрєєв О.М. Метод розвантаження телекомунікаційного сервера за рахунок кешування зображень / О.М. Дрєєв // Збірник наукових праць Кіровоградського національного технічного університету. Техніка в сільськогосподарському виробництві, галузеве машинобудування, автоматизація. Випуск 25. Ч. І. – Кіровоград: КНТУ. – 2012 – С. 419-424.
4. Дрєєв О.М. Метод прогнозування завантаженості серверу телекомунікаційної мережі / О.М. Дрєєв, О.А. Смірнов, Є.В. Мелешко, О.В. Коваленко // Системи обробки інформації. Випуск 3(101) Том 2. – Х.: ХУПС. – 2012. – С. 181-188.
5. Дрєєв О.М. Оцінка якості стиснення зображень на основі дискретного перетворення Хартлі / О.В. Коваленко, О.П. Доренський, О.М. Дрєєв // Системи озброєння і військова техніка. Науковий журнал 2(34) – Х.: ХУПС – 2013. С. 99-102.
6. Дрєєв О.М. Дослідження впливу ступеня стиснення зображень на оперативність їх доставки у телекомунікаційній системі / О.А. Смірнов, О.М. Дрєєв, О.П. Доренський // Збірник наукових праць "Системи обробки інформації". – Випуск 8(115). – Х.: ХУПС – 2013. – С. 234-239.
7. Дреев А.Н. Сравнение битовых плотностей при использовании различных методов кодирования информации / А.Н. Дреев, А.А. Смирнов // Системи обробки інформації, 2014, випуск 2 (118), том 2 – Харків: ХУПС – 2014. С 64-66.
8. Дрєєв О.М. Моделювання впливу інтенсивності трафіку на оперативність доставляння інформації / О.М. Дрєєв // Науково-виробничій журнал “Зв’язок”. – Київ: ДУТ, 2014. – № 2 (108) С. 24-29.

9. Дреев А.Н. Повышение вероятности доставки сообщений в телекоммуникационных системах и сетях для обеспечения информационной безопасности / А.Н. Дреев, А.А. Смирнов //«Безпека інформації» Том 21, №1 2015 р. – Київ: НАУ – 2015. – С. 22-28.
10. Дрєєв О.М. Узагальнення вейвлету Хаара / О.М. Дрєєв, Г.М. Дрєєва // Збірник тез доповідей Комбінаторні конфігурації та їх застосування, 15-16 жовтня 2010 р. – Кіровоград – С. 58

УДК 004

Б. Палюга, магістр гр. КІ-18М-1,9
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ МЕРЕЖЕВИХ СХОВИЩ НА ОСНОВІ ТЕХНОЛОГІЇ NVR

У статті розглянуто програмне забезпечення, яке призначено яке призначено для мережевих сховищ на основі технології NVR. Метою розробки є дослідження та програмна реалізація мережевих сховищ на основі технології NVR. Об'єктом дослідження є процес реалізації мережевих сховищ на основі технології NVR. Предметом дослідження є методи реалізації мережевих сховищ на основі технології NVR. Методи дослідження базуються на методах Big Data, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація мережевих сховищ на основі технології NVR. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення. Розроблено зручний інтерфейс користувача. Наведені інструкції по роботі з програмними засобами.
комп'ютерна інженерія, мережеві сховища, NVR

Постановка проблеми. Поширення мережевих IP-камер породжує попит на мережеві сховища. Однак у багатьох випадках переважніше використовувати спеціалізовані рішення, такі як мережеві відеореєстратори NVR. Мабуть, ніде проблема зберігання зростаючого обсягу даних не проявляється так гостро, як при записі результатів відеоспостереження. І хоча в деяких сегментах ринку аналогові системи відеоспостереження дотепер популярні, загальна тенденція складається в усі більше широкому застосуванні IP-рішень. А поширення мережевих IP-камер, у свою чергу, породжує попит на мережеві сховища. Однак у багатьох випадках переважніше використовувати спеціалізовані рішення, такі як мережеві відеореєстратори NVR. Запис результатів відеоспостереження становлять майже половину всіх Больших Даних у світі. По оцінці IHS Technologies, щодня додається по 500 Пбайт таких даних, а до 2019 року ця цифра виросте до 2500 Пбайт. Наприклад, у типовому великому міжнародному аеропорті встановлене близько 20 тис. камер, і при частоті 15 кадрів у секунду для формату кадру NTSC одержуємо понад 5 Пбайт щодня. Навіть при скороченні частоти кадрів до трьох у секунду обсяг записів перевищує 1 Пбайт. Звичайно, такі величезні обсяги даних характерні тільки для дуже великих інсталяцій, але вони ростуть – найчастіше навіть більше швидкими темпами – і у випадку менш масштабних рішень, що відбувається за рахунок збільшення кількості використовуваних камер і поширення таких технологічних інновацій, як камери з дозволом 4K. Ситуація збільшується тим, що, відповідно до законодавчих або внутрикорпоративних вимог, ці записи необхідно зберігати протягом тривалого часу, тому перед компаніями встає завдання реалізувати зберігання відеозаписів найбільш ефективним – з економічної й технічної точок зору – способом.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини реалізації мережевих сховищ на основі технології NVR.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація мережевих сховищ на основі технології NVR.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем реалізації мережевих сховищ на основі технології NVR.
– Дослідження мережевих сховищ на основі технології NVR.
– Програмна реалізація мережевих сховищ на основі технології NVR.

Об'єктом дослідження є процес реалізації мережевих сховищ на основі технології NVR.

Предметом дослідження є методи реалізації мережевих сховищ на основі технології NVR.

Методи дослідження базуються на методах Big Data, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу.

Опис функціонування системи

Мережеві сховища для мережевих камер

Незважаючи на те що в деяких сегментах ринку аналогові системи відеоспостереження дотепер популярні, IP-рішення застосовуються усе більш широко. Відповідно, замість спеціалізованих пристроїв для запису відео, таких як цифрові відеорекордери (Digital Video Recorder, DVR), які, незважаючи на свою назву, призначені для захвата зображення з аналогових камер, сьогодні можуть використовуватися звичайні сервери й системи зберігання з необхідним програмним забезпеченням. Однак, якщо компанії потрібна надійна система зберігання, виходить, їй потрібний мережевий реєстратор (Network Video Recorder, NVR).

Одним з головних переваг використання мережевих відеорекордерів є простота їхньої установки й використання. Крім зберігання даних, у них реалізуються й функції керування камерами, тобто забезпечується функціональність VMS. NVR поставляються із передвстановленим програмним забезпеченням і найчастіше оснащуються функціональністю Plug&Play для автоматичного виявлення й підключення підтримуваних відеокамер, тобто встаткування потрібно тільки підключити до мережі.

Втім, використання NVR пов'язане з певними обмеженнями, оскільки будь-яке апаратне рішення є менш гнучким, чим програмне. Так, хоча NVR корпоративного класу й розраховані на масштабування, межу масштабування для них найчастіше виявляється менше, ніж для систем керування відео (Video Management System, VMS). До того ж нарощування можливо лише з фіксованим кроком, що чревате надмірними витратами, наприклад, коли потрібно забезпечити підтримку всього декількох додаткових камер. Скажемо, NVR підтримує 64 каналу, а вам потрібно підключити ще 5 камер понад дане число. У результаті прийде придбати ще один пристрій, ресурси якого по більшій частині не будуть використовуватися.

Таким чином, попит є й на програмні, і на програмно-апаратні рішення – все залежить від конкретної ситуації. При виборі системи потрібно завжди керуватися вимогами й перевагами замовника. Будь-яке рішення має право на існування, якщо воно оптимальним образом справляється з поставленим завданням. А NVR потрібний, коли потрібно «готове рішення з коробки», настроювання й запуск якого здійснюється користувачем за допомогою покрокового майстра, тобто збір «заліза» і установка фірмової ОС із ПЗ вже виконані виробником.

Потенційний ризик у використанні програмних рішень полягає в тому, що часом їх вибирають у прагненні заощадити, тому й устаткування здобувається як можна більше дешеве, а виходить, і надійність невисока. Ніхто не говорить, що якщо використовується програмний NVR або звичайний NAS, те завтра це ПЗ або встаткування вийде з ладу. Неполадки можуть виникнути й через півроку, і через рік-два. Але загальний рівень надійності буде нижче. Ми не раз зіштовхувалися із ситуаціями, коли звичайний комп'ютер

зависав або йшов у перезавантаження через збої в операційній системі. Якщо для замовника випадкова втрата або зупинка відеозапису не є великою втратою, то тоді дійсно має сенс звернути увагу на програмні реєстратори.

Вимоги до СЗД для запису відео

Як і камери, системи зберігання для відеоспостереження стають усе більше інтелектуальними й функціональними. Однак насамперед потрібне забезпечення базових вимог до продуктивності і ємності – запис відео з найкращим дозволом і оптимальною частотою кадрів при необхідній тривалості зберігання записів з найменшими витратами. Устаткування повинне гарантувати необхідний строк зберігання інформації й швидкість доступу до ресурсів, а також відповідати нормам по резервуванню даних і надмірності СЗД (з урахуванням розміру файлів і строків зберігання інформації) відповідно до вимог замовника й законодавства.

Як показало наше опитування, серед всіх вимог постачальники майже одноголосно виділяють надійність. До цілісності даних пред'являються самі тверді вимоги, оскільки при збереженні відеоданих навіть часткова втрата інформації може привести до втрати всього записуваного відеопотоку. Сучасна СЗД повинна забезпечувати стабільну обробку й зберігання ненормованого потоку даних, генеруємого самими різними камерами з дозволом від VGA до Full HD і Ultra HD.

Для забезпечення високого рівня надійності рекомендуємо використовувати системи зберігання, які мають не менш двох контролерів, що працюють в активному режимі це допоможе захистити систему відеоспостереження від позаштатних ситуацій, пов'язаних з апаратними збоями. Сучасна система зберігання повинна легко масштабуватися – як по продуктивності, так і по ємності. У великих інсталяціях, де число встановлених відеокамер велике, потрібна продуктивність дискової підсистеми досягається за рахунок використання дисків SSD у якості кешуючого пристрою для запису й читання даних.

Втім, як уважають в Seagate, про широке застосування флеш-накопичувачів у системах зберігання відеоінформації говорити ще рано. Основна їхня перевага – істотно більше висока швидкість запису – поки не дуже актуально, тому що в більшості випадків цілком достатньо можливостей традиційних дискових накопичувачів. Флеш-накопичувачі має сенс використовувати, коли пристрою працюють при постійній трясці й високих/низьких температурах або застосування дискових накопичувачів утруднений (приклад – накопичувачі у відеокамерах).

Істотний вплив на реалізацію системи зберігання відеоданих, як відзначалося вище, робить необхідний час зберігання записаної інформації – від цього залежать загальна ємність системи і її конкретна реалізація. У багатьох випадках, особливо коли запису необхідно зберігати довго, СЗД варто розділяти на дві підсистеми: оперативну (постійно використовується для запису) і просту архівну (без потокового запису в реальному часі), куди інформація надходить із оперативної у фоновому режимі. Такий підхід дозволяє забезпечити кращі показники за критерієм вимоги/витрати.

Однак, такий поділ на дві системи – не кращий варіант: при побудові системи зберігання відеоданих варто прагнути до консолідації ресурсів. У сучасному світі впровадження окремих СЗД для «гарячих» даних і архівного зберігання недоцільно – як з функціональної, так і з комерційної точок зору. Єдина багатоцільова система керування даними допомагає оптимально розподілити навантаження й заощадити на подальшому масштабуванні інфраструктури.

Зберігання й передача відео 4K

Реалізація у відеокамерах нових технологій впливає на всі інші компоненти системи відеоспостереження. До обробки відеопотоків, переданих камерами надвисокої чіткості (4K и більше), пристрою запису повинні бути готові. Це стосується як необхідної ємності зберігання, так і підтримки відповідних протоколів. NVR записує вступник відеопотік безпосередньо на жорсткі диски, без стиску. Однак для відтворення відео NVR повинен «розуміти» використовуваний камерою алгоритм кодування.

Більшість сучасних NVR розуміють протокол стиску H.264, але для ефективної роботи з камерами 4K потрібна підтримка протоколу H.265. Відповідно до наявних оцінок, H.265 на 50% ефективніше свого попередника при стиску відео високого дозволу й тій же якості зображення. Його використання дозволяє заощадити пропускну здатність мережі і ємність зберігання, однак для стиску й декодування H.265 необхідні могутніші процесори.

Зараз уже нікого не здивувати відеокамерами 4K. Комплектуючі стають доступніше, що веде до збільшення процесорних потужностей відеокамер і, як наслідок, відеореєстраторів. У результаті основною тенденцією зараз є збільшення дозволу відеокамер, що, безумовно, веде до підвищення генеруємого ними потоку. І тоді неминуче виникає необхідність цей потік зменшити без втрати якості. Таким чином, сучасні NVR повинні підтримувати не тільки запис у високому розв'язній здатності, але й різні можливості по скороченню потоку: роботу з кодеком H.265, технології Wisestream, Zipstream і т.д.

Збільшення дозволу веде до збільшення обсягу даних, що, у свою чергу, приводить до підвищеного навантаження як на мережі передачі цих даних, так і на системи зберігання. Однак, у випадку локальних систем відеоспостереження передача даних звичайно не представляє проблеми. Труднощі виникають при використанні хмарних сховищ і віддаленого доступу через недостатню пропускну здатність наявних каналів передачі даних. У зв'язку із цим він призиває звернути увагу на наступні моменти:

– Ефективне використання пропускної здатності, що припускає запис тільки важливих подій і використання «розумних» алгоритмів стиску. Зокрема, кодеки H.264 і H.265, а також їхньої модифікації, наприклад Zipstream від Axis, дозволяють значно скоротити непотрібний трафік.

– Використання потоків з меншим дозволом для перегляду в реальному часі й запис у більше високій розв'язній здатності.

– Резервування зберігання – наприклад, запис на карту пам'яті у випадку обриву з'єднання, що допоможе уникнути втрати даних або хоча б скоротити їх.

Однак, як відомо, будь-яка система надійна настільки, наскільки міцно її сама слабка ланка. Тому для запобігання втрати пакетів, крім достатньої пропускної здатності, необхідно забезпечити відказостійкість (резервування) каналів передачі даних. Сучасна система відеоспостереження повинна володіти підвищеною відказостійкістю, причому це стосується всіх компонентів: камер, систем зберігання й мережевої інфраструктури. Мається на увазі не просте дублювання, хоча для деяких завдань, наприклад для забезпечення електроживлення активних мережевих пристроїв, без дублювання блоків живлення не обійтися. Варто не просто дублювати, а резервувати основні вузли системи, що не тільки підвищить її відказостійкість, але й розширить функціональні можливості.

Розробка структурної схеми

Здобуваючи спеціалізовану систему зберігання для відеоспостереження, таку як NVR, замовник сподівається на те, що вона буде записувати не тільки відео, але й, якщо знадобиться, аудіо, тривожні повідомлення й різні метадані з будь-яких камер, які вже встановлені на його території або з'являться пізніше. Однак у дійсності NVR повноцінно підтримують тільки певний перелік пристроїв. Втім, завдяки зусиллям консорціуму ONVIF по стандартизації інтерфейсу взаємодії мережевих камер і VMS, цей список значно розширився.

Перша специфікація ONVIF з'явилася після створення консорціуму в 2008 році. Однак, як незабаром з'ясувалося, незважаючи на згоду відносно API, кожний виробник по-своєму реалізовував інтерфейс у своїх камерах: розбіжності стосувалися того, які функції варто підтримувати. Для забезпечення уніфікації функцій консорціум ONVIF запропонував концепцію профілів. Перший такий профіль (S) був опублікований в 2011 році. Якщо продукти підтримують його, вони повинні взаємодіяти між собою незалежно від того, хто їх виготовив. З тих пор з'явилося ще кілька профілів: G для зберігання відео, C и A для контролю доступу й Q для спрощення інсталяції.

У цей час на ринку пропонується вже більше 5000 продуктів з підтримкою специфікацій ONVIF, і деякі безіменні виробники стали заявляти про сумісність із ними, у дійсності їх не реалізуючи. Камери, що випускаються ними, нерідко не вдається навіть підключити до NVR. Втім, як показують тести, навіть у випадку продукції відомих виробників не можна бути до кінця впевненим у повній сумісності з ONVIF, зокрема, це стосується детектування руху. До того ж 100-процентна сумісність із ONVIF не гарантує підтримки всіх функцій камери, оскільки найчастіше реалізується безліч додаткових можливостей. Однак ONVIF, принаймні, гарантує базова взаємодія.

Вендорів і моделей камер – безліч, вимог дуже багато, тому абсолютно універсальних NVR немає. Все залежить від ПЗ, за допомогою якого камера й NVR повинні бути повноцінно інтегровані для підтримки всіх функцій при спільній роботі. На жаль, часто виникають ситуації, коли реалізація ONVIF не допомагає домогтися якісної взаємодії через різні підходи виробників камер і використовуваних версій протоколу.

Замовник думає, що в ідеалі всі камери повинні бути сумісні з усіма реєстраторами. Однак це неможливо, і ми змушені застосовувати протокол ONVIF. Він не дозволяє використовувати всі функції камери, тому що кожний виробник закладає в них якісь унікальні речі, а ONVIF є універсальним протоколом. Але доступний набір функцій достатній для одержання якісного відео. Не можна сказати, що це ідеальне рішення, але кращого на даний момент немає. Тому підтримка й розвиток ONVIF повинні розширюватися й набирати популярність.

Якщо споконвічно консорціум ONVIF фокусувався на інтерфейсі для камер відеоспостереження, то тепер він розробляє стандарти й для інших пристроїв фізичного захисту (прикладами можуть служити згадувані вище профілі C и A). Крім того, камери стають частиною Інтернету речей, так що від NVR всі частіше потрібна підтримка не тільки камер. Багато сучасних записуючих пристроїв містять різні датчики, що передають додаткову інформацію про об'єкт у режимі реального часу. Для повноцінної підтримки таких камер необхідна ефективна обробка як потокових, так і випадкових даних. СЗД, у свою чергу, містять у собі нові засоби стиску, можливості розпаралелювання різних відеопотоків і створення багаторівневих сховищ.

Як і в інших сегментах, хмарні послуги відеоспостереження (Video Surveillance as a Service, VSaaS) зараховуються до перспективних напрямків розвитку ринку. Більше того, вони чи розглядаються не в якості ключової його складової – так, згідно із прогнозом Transparency Market Research (TMR), у найближчі десять років ринок відеоспостереження й VSaaS буде щорічно рости на 17%. Провайдери надають різні послуги VSaaS. Насамперед це, звичайно, зберігання записів відеоспостереження. Крім того, у рамках VSaaS часто пропонуються послуги відеоаналітики. Як уважають експерти TMR, подальші перспективи розвитку VSaaS пов'язані з розробками в області штучного інтелекту для рішення таких завданнях, як аналіз міського трафіку.

Однак хмарне відеоспостереження, мабуть, як ніякий інший вид хмарних послуг, відчутно до двох критичних факторів – безпеки й доступності (каналів). Є ряд причин, через які хмарні сервіси використовуються не у всіх випадках. У першу чергу ця відсутність швидкого й надійного каналу зв'язку до хмарного сховища. Другою причиною, звичайно ж, є безпека, оскільки дуже часто відеоматеріали є конфіденційною інформацією й передавати їхній третій стороні неприпустимо.

Більшість замовників не готові розміщати свої корпоративні системи безпеки на хмарних сервісах, тому що бояться, і досить обґрунтовано, що вони можуть бути зламані. Тому, як правило, замовники не зберігають у хмарах всю наявну в них інформацію, а хмарні сервіси частіше використовуються для віддаленого перегляду живого відео або для копіювання частини архіву. Іноді, щоправда, там розміщається частину записів, наприклад за останню добу, щоб у випадку поломки реєстратора не втратити архів. У цілому ж хмарні сховища й сегмент корпоративної безпеки поки не сумісні на 100%.

При хмарній реалізації необхідні швидкісні канали зв'язку між віддаленим об'єктом і ЦОДом. При великій кількості камер і користувачів буде потрібно відповідний NVR корпоративного класу. Як правило, видеоконтент із об'єктів, що належать як часткою користувачам, так і організаціям, вимагає конфіденційного зберігання, тому його відправлення в хмарні сервіси хоча й можлива (особливо у випадку NAS-пристроїв), але використовується рідко, на відміну від локального зберігання або копіювання на власні віддалені сервери.

Безумовно, організація доступу й забезпечення його безпеки – тільки частина проблеми. Перед провайдером встає непросте завдання по створенню ефективної системи зберігання. Для надання послуг хмарного відеоспостереження потрібна СЗД, що здатна забезпечити високопродуктивний і надійний доступ для запису й читання відеоматеріалів. Оскільки запис і читання даних, що надходять із великої кількості джерел, будуть здійснюватися паралельно, СЗД повинна підтримувати використання адаптерів із пропускною здатністю 40 Гбіт/с на порт Ethernet, а в найближчому майбутньому – 100 Гбіт/с.

Як би те не було, інтеграція із хмарою практично завжди корисна, тому що надає можливість швидко й без серйозних фінансових витрат підключити додаткове сховище даних.

NVR під навантаженням

За деякими оцінками, відеодані становлять біля половини всіх даних Інтернету речей. З поширенням камер відеоспостереження, оснащених підтримкою стандартів надвисокої чіткості 4К, потреба в необхідній для їхнього запису ємності зберігання збільшиться в кілька разів, навіть незважаючи на застосування більше ефективних алгоритмів кодування, таких як H.265. У критичних системах для зберігання зростаючих потоків відео доцільно застосовувати спеціалізовані рішення – зокрема, мережеві відеорекордери NVR, розраховані на подібне навантаження.

Рекомендації з організації запису відеоспостереження

Вимоги до системи зберігання дані відеоспостереження залежать від безлічі факторів: кількості встановлених камер, планованої тривалості зберігання інформації, необхідної якості запису (дозвіл зображення й частота кадрів у секунду) і т.д. На основі цих даних можна визначити, який повинна бути ємність зберігання, і скласти первинне уявлення про краще рішення: чи можна реалізувати зазначені вимоги на базі DVR/NVR, буде потрібно чи зовнішня система зберігання даних, чи залишати дані на об'єкті або передавати в хмарне сховище, як буде здійснюватися запис – безпосередньо в систему або із проміжним зберіганням у пам'яті камери й т.п. Наступне уточнення вимог дозволяє скорегувати первісний проект і одержати в результаті надійне рішення.

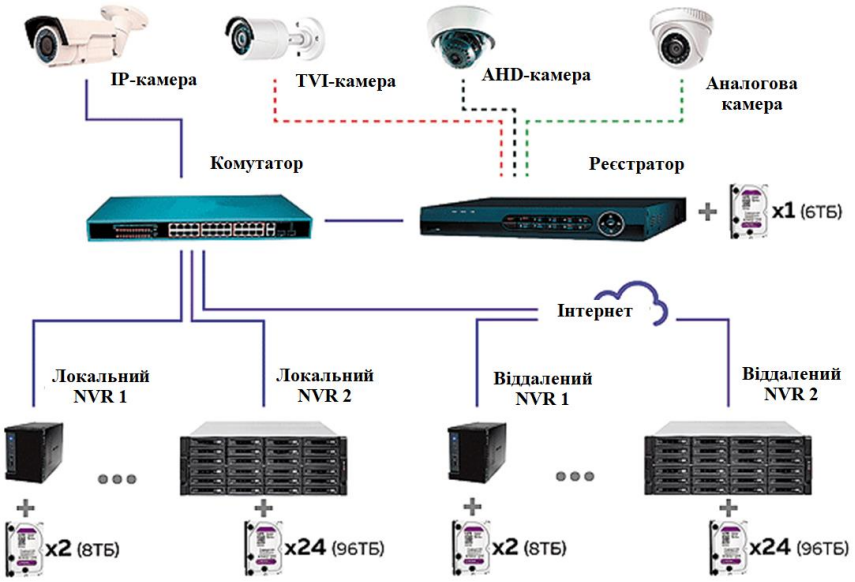


Рисунок 1 – Структурна схема системи

І хоча, як підкреслюють опитані нами вендори, рекомендації прямо залежать від особливостей конкретного проекту, деякі загальні міркування вони висловили.

Про важливість планування. Організація відеоспостереження – це не тільки установка камер, але й зберігання величезної кількості відеоматеріалів, до яких потрібно надати надійний і безпечний доступ. Із цієї причини варто уважно підійти до планування зберігання дані системи відеоспостереження. Як показує практика, добре спланована інфраструктура зберігання даних дозволяє забезпечити високий рівень надійності, безпеки й зручності використання системи в цілому.

Про головні критерії вибору. Кожний об'єкт по-своєму унікальний: на один потрібні цілодобовий запис або кольорове відео найвищого дозволу, а десь досить записувати, що відбувається тільки після спрацьовування датчиків або мати чорно-білу картинку. Крім того, завжди є бюджетні обмеження. Однак, який би сценарій не розглядався, ключовими критеріями вибору залишаються глибина й надійність зберігання.

Про великі проекти. У масштабних проектах рівня «Безпечне місто» або інфраструктурі відеоспостереження на великих підприємствах з більшим числом об'єктів у першу чергу варто домогтися відказостійкісти системи і її безперервної роботи навіть у режимі деградації. Запис повинна здійснюватися без втрат при виході з ладу будь-якого апаратного компонента, а інфраструктура відеоспостереження – підтримувати певний рівень якості обслуговування (QoS), забезпечувати незнижувану продуктивність і потрібну ширину каналу.

Про спеціальне устаткування. Звичайно, насамперед необхідно спеціалізоване встаткування, зокрема реєстратори й диски. Найчастіше замовники хочуть використовувати наявні комп'ютери й для створення системи відеоспостереження, і для запису відео. Це не зовсім вірне рішення, тому що такий набір програмного й апаратного забезпечення не тестувалося на постійний запис і безперебійну роботу 24/7 на відміну від спеціально підібраного програмно-апаратного комплексу відеореєстратора.

Про вибір накопичувачів. При організації запису в DVR/NVR треба уважно поставитися до вибору дискового накопичувача. Варто застосовувати накопичувачі, розроблені саме для систем відеоспостереження, тому що вони розраховані на цілодобовий/круглогодичний режим роботи з розподілом навантаження 90/10 (90% – потоковий запис, 10% – читання) і мають спеціальне внутрішнє програмне забезпечення (прошивання), розраховане на забезпечення потокового запису й використовування особливих технологій для запобігання «випадання» кадрів і підтримки роботи в масивах RAID.

Про розпізнавання для економії. Економія простору на дисках СЗД є однієї з первинних завдань для користувачів систем відеоспостереження через високу вартість засобів зберігання інформації. У системах інтелектуального відеоспостереження, особливо в системах розпізнавання осіб, зберігаються лише журнали подій. Даний підхід, по-перше, дозволяє заощаджувати місце на диску, а по-друге, не вступає в протиріччя із законом «Про захист персональних даних», оскільки зберігаються не дані про людей, а лише результати розпізнавання в зашифрованому виді, що не дозволить стороннім використовувати їх у власних цілях.

Про саме коштовне. Оскільки зміст сховища усе ще є одним із самих витратних компонентів інформаційної системи, варто задуматися про те, що величезна частина інформації у відеопотоці не представляє цінності. Існують різні підходи до скорочення надлишкових даних. Серед них – запис за рухом, за тригером (відкривання дверей, наприклад), за розкладом або використання кодеків з високим коефіцієнтом стиску. У деяких випадках доречне сполучення всіх або деяких підходів.

Висновок. У статті розглянуто та проаналізовано програмне забезпечення, створене в результаті виконання роботи, призначено для мережевих сховищ на основі технології NVR. В межах України в недостатній мірі представлені вітчизняні розробки в цій області. У роботі наведені теоретичне узагальнення й рішення наукового завдання дослідження методів

реалізації мережевих сховищ на основі технології NVR. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем реалізації мережевих сховищ на основі технології NVR; Досліджена система реалізації мережевих сховищ на основі технології NVR; На основі отриманих результатів досліджень створена програмна реалізація мережевих сховищ на основі технології NVR. Розроблені під час виконання роботи алгоритми дозволяють успішно вирішувати завдання реалізації мережевих сховищ на основі технології NVR. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки. Розроблене програмне забезпечення має простий, дружній та зручний інтерфейс користувача, що забезпечує легкість у освоєнні роботи програмного продукту, зручність у використанні, і не потребує особливих спеціальних знань. При створені програмного забезпечення було використано об'єктно-орієнтований підхід, що відповідає сучасним тенденціям у галузі розробки комерційних програмних систем. Програма реалізована на мові високого рівня Embarcadero Delphi 10.2 Tokyo. Дана мова програмування дозволяє найбільш ефективно обробляти дані. Це дозволило мінімізувати строк розробки програмного забезпечення, і, як слід, зменшити витрати на його розробку. Запропоноване програмне забезпечення ділиться на загальне програмне забезпечення, що поставляється із засобами обчислювальної техніки й спеціальне програмне забезпечення, що спеціально розроблене для даної конкретної системи й включає програми, що реалізують її функції. Програма призначена для виконання під управлінням багатозадачної операційної системи Windows XP/Vista/7/8/10. Даються необхідні рекомендації з установки розробленого програмного забезпечення. Для підвищення рівня безпеки запропоновано застосовувати алгоритм DSA.

Список літератури

1. Дреев А.Н. Использование неравномерного распределения единичных битов для дополнительного сжатия SPIHT кода / А.Н. Дреев, А.А. Смирнов // Информационные системы в управлении, образовании, промышленности: монография. Под редакцией профессора В.С. Пономаренко. – Х.: Вид-во ТОВ «Щедра садиба плюс», 2014. – С. 498.
2. Дрєєв О.М. Дослідження впливу шляху розгортки на ступінь ентропійного стиснення цифрового зображення / О.М. Дрєєв, О.В. Слюсар // Збірник наукових праць Кіровоградського національного технічного університету. Техніка в сільськогосподарському виробництві, галузеве машинобудування, автоматизація. Випуск 21. – Кіровоград: КНТУ. – 2008 – С. 115-118.
3. Дрєєв О.М. Метод розвантаження телекомунікаційного сервера за рахунок кешування зображень / О.М. Дрєєв // Збірник наукових праць Кіровоградського національного технічного університету. Техніка в сільськогосподарському виробництві, галузеве машинобудування, автоматизація. Випуск 25. Ч. І. – Кіровоград: КНТУ. – 2012 – С. 419-424.
4. Дрєєв О.М. Метод прогнозування завантаженості серверу телекомунікаційної мережі / О.М. Дрєєв, О.А. Смірнов, Є.В. Мелешко, О.В. Коваленко // Системи обробки інформації. Випуск 3(101) Том 2. – Х.: ХУПС. – 2012. – С. 181-188.
5. Дрєєв О.М. Оцінка якості стиснення зображень на основі дискретного перетворення Хартлі / О.В. Коваленко, О.П. Доренський, О.М. Дрєєв // Системи озброєння і військова техніка. Науковий журнал 2(34) – Х.: ХУПС – 2013. С. 99-102.
6. Дрєєв О.М. Дослідження впливу ступеня стиснення зображень на оперативність їх доставки у телекомунікаційній системі / О.А. Смірнов, О.М. Дрєєв, О.П. Доренський // Збірник наукових праць "Системи обробки інформації". – Випуск 8(115). – Х.: ХУПС – 2013. – С. 234-239.
7. Дреев А.Н. Сравнение битовых плотностей при использовании различных методов кодирования информации / А.Н. Дреев, А.А. Смирнов // Системи обробки інформації, 2014, випуск 2 (118), том 2 – Харків: ХУПС – 2014. С 64-66.
8. Дрєєв О.М. Моделювання впливу інтенсивності трафіку на оперативність доставляння інформації / О.М. Дрєєв // Науково-виробничій журнал "Зв'язок". – Київ: ДУТ, 2014. – № 2 (108) С. 24-29.
9. Дреев А.Н. Повышение вероятности доставки сообщений в телекоммуникационных системах и сетях для обеспечения информационной безопасности / А.Н. Дреев, А.А. Смирнов //«Безпека інформації» Том 21, №1 2015 р. – Київ: НАУ – 2015. – С. 22-28.
10. Дрєєв О.М. Узагальнення вейвлету Хаара / О.М. Дрєєв, Г.М. Дрєєва // Збірник тез доповідей Комбінаторні конфігурації та їх застосування, 15-16 жовтня 2010 р. – Кіровоград – С. 58

УДК 004

Ю. Пархоменко, магістр гр. КІ-17М-1,4
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ ВУЗЛА СИНХРОНІЗАЦІЇ, ПОПЕРЕДНЬОЇ ОБРОБКИ ТА ПЕРЕДАЧІ ДАНИХ ЗАСОБУ ІДЕНТИФІКАЦІЇ ЗЕРНОВОГО ПОТОКУ

У статті розроблено програмне забезпечення, яке призначено для системи вузла синхронізації, попередньої обробки та передачі даних засобу ідентифікації зернового потоку. Метою розробки є дослідження та програмна реалізація вузла синхронізації, попередньої обробки та передачі даних засобу ідентифікації зернового потоку. Об'єктом дослідження є вузол синхронізації, попередньої обробки та передачі даних існуючого апаратного засобу реєстрації та ідентифікації зернового потоку. Предметом дослідження є методи та алгоритми потрібні для обробки зображень вузла реєстрації та передачі їх бінарних кодів до ПК. Методи дослідження - використовувалися методи теорії інформації, інформаційного аналізу, методи теорії формування цифрових кодів та сканування об'єктів при дослідженні засобу ідентифікації зернового потоку, основи теорії цифрових систем автоматичного управління та математичного моделювання. Результат роботи – Розроблено програмне забезпечення вузла синхронізації, попередньої обробки та передачі даних засобу ідентифікації зернового потоку. Розроблені теоретичні положення магістерської роботи покладені в основу реалізації алгоритмів обробки даних та формування бінарних кодів вузла реєстрації. В процесі роботи проведено: аналіз методів обробки зображень в системах технічного зору і визначено шляхи їх практичної реалізації; виконано детальний аналіз існуючих методів та засобів реєстрації дискретних рухомих об'єктів та формування їх цифрових зображень; розроблено методику та алгоритми формування бінарного коду зображень площини контролю вузла реєстрації; розроблено програмне забезпечення блоку синхронізації, попередньої обробки та передачі даних зображення дискретних об'єктів до ПК. Програму розроблено в середовищі Assembler для забезпечення максимальної гнучкості при роботі з апаратними ресурсами контролерів, оптимізації програм по швидкості виконання, оптимізації програм за розміром коду

комп'ютерна інженерія, комп'ютерна інженерія, ідентифікація, зерновий потік

Постановка проблеми. Зерновий сектор України є стратегічною галуззю економіки держави, оскільки вона в останні роки посідає третє місце серед лідерів з експорту зерна на світовому ринку після США та Євросоюзу, а збільшення обсягів ВВП в аграрному секторі забезпечує вдвічі більший ефект порівняно з іншими сферами господарства. В той же час, внаслідок слабкого матеріально-технічного забезпечення та пониженої ефективності праці, які не відповідають світовим стандартам і потребам галузі, урожайність зернових, всупереч усталеним твердженням про високу родючість українських ґрунтів, сьогодні значно поступається провідним країнам.

Одним із основних резервів підвищення продуктивності та якості сівби зернових культур є впровадження цифрових систем контролю та керування процесом висіву. Однак, процес розробки таких систем для зернових сівалок стримується відсутністю надійних, точних і не дорогих засобів реєстрації та ідентифікації зернин в потоці. Діючі системи контролю висіву базуються на використанні простих і дешевих у виробництві, але не точних засобів реєстрації, які контролюють лише інтенсивність формованого висівним апаратом зернового потоку, а не кожну зернину в потоці, що не дозволяє проводити точний висів. Це приводить до значних збитків у галузі. На сьогодні існують дослідні зразки оптико - електронного скануючого датчика зернин в потоці які використовуються для оцінки якості роботи висівних апаратів. Ці пристрої реєстрації виготовлені на апаратному рівні, є громіздкими, складними у виробництві та практичному використанні на сівалках у польових умовах. Низький рівень автоматизації процесу висіву на сьогодні мають зернові сівалки через відсутність надійних і точних засобів ідентифікації формуємого ними зернового

потоку та систем автоматичного управління. Тому розробка цифрових засобів реєстрації та ідентифікації потоку насіння є актуальною задачею.

Перед нами постає проблема детального дослідження вузла синхронізації, попередньої обробки та передачі даних засобу ідентифікації зернового потоку виконаного на аналоговому (апаратному) рівні з метою його програмної реалізації.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні реалізації вузла синхронізації, попередньої обробки та передачі даних засобу ідентифікації зернового потоку.

Мета й завдання дослідження. Метою роботи є дослідження та розробка програмного забезпечення вузла синхронізації, попередньої обробки та передачі даних засобу ідентифікації зернового потоку.

Для досягнення поставленої мети необхідно вирішити наступні завдання:

4. Провести аналіз методів обробки зображень в системах технічного зору і визначити шляхи їх практичної реалізації.
5. Виконати детальний аналіз існуючих методів та засобів реєстрації дискретних рухомих об’єктів та формування їх цифрових зображень.
6. Розробити методику та алгоритми формування бінарного коду зображень площини контролю вузла реєстрації.
7. Розробити програмне забезпечення блоку синхронізації, попередньої обробки та передачі даних зображення дискретних об’єктів до ПК.

Об’єктом дослідження є вузол синхронізації, попередньої обробки та передачі даних існуючого апаратного засобу реєстрації та ідентифікації зернового потоку.

Предметом дослідження є методи та алгоритми потрібні для обробки зображень вузла реєстрації та передачі їх бінарних кодів до ПК.

Виклад основного матеріалу. Як показав аналіз існуючих пристроїв реєстрації дискретних об’єктів в потоці, що формується висівними апаратами зернових сівалок, найбільш придатним для використання у складі САК є двох координатний отикоелектронний, який входить до складу пристрою контролю ЕКПС-03МП (ІП-195).

Оскільки інтенсивність зернового потоку може досягати 450шт/с, а кількість зернин, що одночасно перетинають площину контролю датчика – $5 \div 7$шт, то складність розробки програмного забезпечення датчика полягала як в обмеженні термінів реєстрації і обробки даних, так і в швидкодії елементів схеми: оптронних пар, мікросхем, підсилювачів тощо. Навіть в аналоговому виконанні для досягнення заданих термінів потрібно було використовувати оригінальну технологію (рис. 1). Цю ж проблему потрібно враховувати і вирішувати при проектуванні системи комп’ютерної ідентифікації та визначенні параметрів зернового потоку.

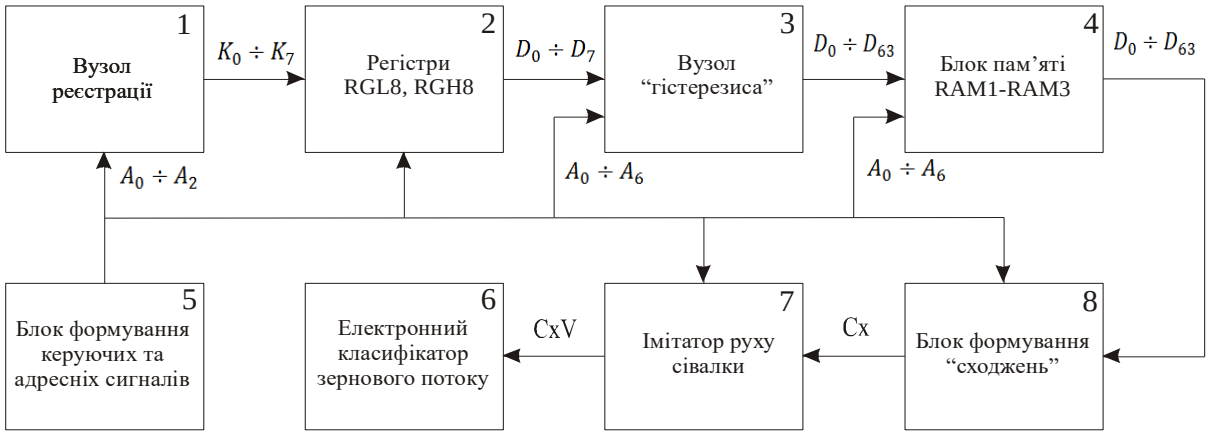


Рисунок 1. - Функціональна схема датчика ПДС 02/03

Синхронізація роботи усіх вузлів датчика ПДС 02/03 задається блоком формування керуючих та адресних сигналів 5. Сканування оптронних пар вузла реєстрації 1 задається адресними сигналами $A_0 \div A_2$ від блоку 5. В кожному такті тривалістю 24мкс засвічуються 8 оптронних пар, аналогові вихідні сигнали $K_0 \div K_7$ з яких одночасно поступають на входи регістрів 2 верхнього $RGH8$ та нижнього $RGL8$ рівнів квантування. Період сканування 64 оптронних пар складає 192мкс. З виходів регістрів 2 дані $D_0 \div D_7$ логічного рівня $A_0 \div A_2$ послідовно подаються на входи вузла «гістерезиса» 3. Сформовані біти зображення рядка $D_0 \div D_{63}$ почергово заносяться в парну $RAM1$ або непарну $RAM2$ пам'ять поточного рядка та в пам'ять $RAM3$ попереднього рядка 4. В результаті послідовного аналізу кодів поточного і попереднього рядків в блоці 8 формуються сигнали сходження об'єкту Cx з площини контролю. Кінцеві сигнали сходження об'єкта CxV, прив'язані до передбачуваної координати місця його падіння на дно борозни завдяки врахуванню швидкості руху сівалки, з виходу імітатора руху сівалки 7 подаються на вхід електронного класифікатора зернового потоку 8. Усі вузли датчика ПДС 02/03 виконані на аналоговому рівні і можуть діяти автономно – незалежно від класифікатора.

На рис. 2. представлено фрагмент комплексної функціональної схеми САК процесом висіву(рис. 2) призначеної для встановлення на зернову сівалку СЗ - 3.6. Цей фрагмент являється уособленою частиною комплексної САК, яка виконує функцію практично незалежної системи комп'ютерної ідентифікації та оцінки якості розподілу зернового потоку вздовж рядка висіву.

Аналогові сигнали $K_0 \div K_7$ з виходу вузла реєстрації 1 поступають на входи блока 2 синхронізації, попередньої обробки, формування та передачі

бінарних кодів $D_0 \div D_{63}$ зображення рядків сканування до блоку розпізнавання образів та формування сигналів їх «сходження » з площини контролю датчика 3. З виходів блоку синхронізації 2 до вузла реєстрації 1 поступають також адресні коди $A_0 \div A_2$ які формують тактові сигнали сканування оптрон них пар.

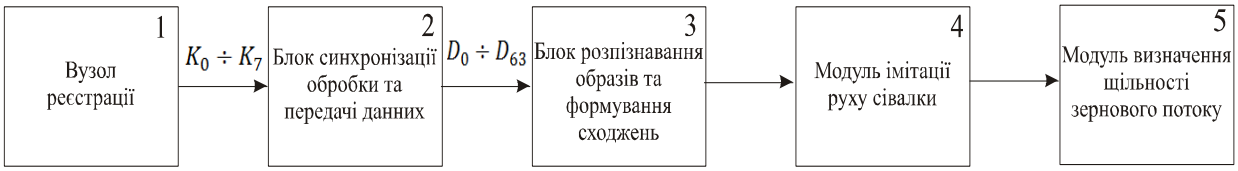


Рисунок 2 - Функціональна схема системи комп'ютерної ідентифікації та оцінки якості розподілу зернового потоку в складі САК

Сформовані сигнали сходження Cx поступають на вхід модуля імітації руху сівалки 4 де формуються кінцеві сигнали сходження об'єкту CxV в яких врахована швидкість руху сівалки. Ці сигнали поступають до модуля 5 визначення щільності розподілу зернового потоку вздовж рядка висіву. Саме ці показники щільності служать основою для керування процесом висіву. Функції блоку розпізнавання 3, модуля імітації 4 та модуля визначення щільності 5 покладено на бортовий комп'ютер. Тому дані з виходу блоку синхронізації 2 повинні передаватися безпосередньо до бортового комп'ютера САК.

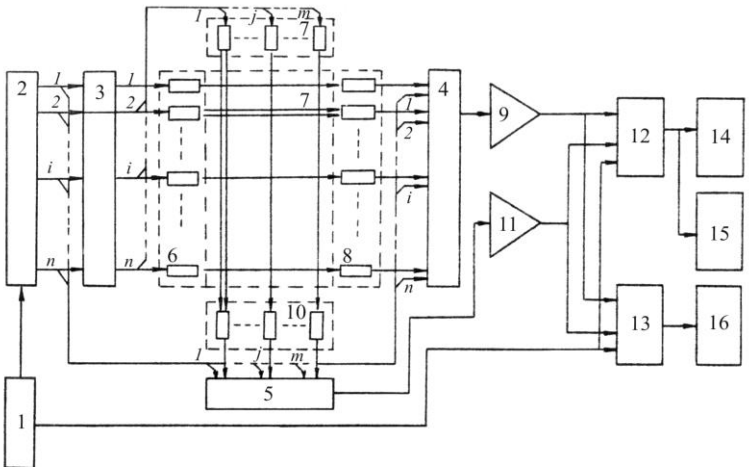


Рисунок 3 - Функціональна схема пристрою реєстрації насіння в потоці

Порівнюючи функціональні схеми датчика ПДС 02/03 (рис. 1) пристрою ІП-195 та системи комп'ютерної ідентифікації та оцінки якості розподілу зернового потоку (рис. 2) проектованої САР приходимо до висновку, що: однаковими у них є лише вузол реєстрації (1); функції регістрів $RGH8$, $RGL8$ (2), вузла «гістерезису» (3) та блоку пам'яті $RAM1 \div RAM3$ (4) покладаються на блок синхронізації, попередньої обробки, формування та передачі даних (2); функції аналогового блоку формування «сходжень»(8), імітатора руху сівалки (7) та електронного класифікатора (6) покладаються на відповідні їм блок 3 та модулі 4,5 реалізовані на програмному рівні.

Розглянемо більш детально роботу вузла реєстрації датчика ПДС 02/03 (рис. 3). Істотною особливістю роботи даного вузла є імітація або фізичне моделювання паралельного світлового потоку по всій площині контролю (розміром 50х100 мм), у вигляді паралельних, спрямованих уздовж координат X,Y, дискретних та таких, що не перетинаються, променів [1,2]. Це забезпечує формування невикривленого зображення проекцій реєстрованих об'єктів.

Реєструюча рамка датчика містить перпендикулярно розміщені лінійки дискретних випромінювачів 5, 6 та фотоприймачів 8, 9 які розташовані один проти одного. Дискретні світлові промені, що скануються з заданою частотою вздовж координат X та У, формують на лінійках фотоприймачів 8, 9 стрічкове вхідне зображення проекцій реєстрованих об'єктів, які перетинають зону контролю 7. Сканування дискретних променів задається адресними сигналами $A_0 \div A_2$, які подаються на входи лічильника–дешифратора 1 через кожні 24мкс. Сформовані на виході дешифратора тактові сигнали $T_0 \div T_7$ керують циклічним почерговим включенням світлодіодів лінійок випромінювачів 5, 6 через ключі 2 та підключенням виходів протилежно розміщених фотоприймачів 8, 9 через ключі 3, 4 до входу відповідного даній координаті підсилювача-формувача 10, 11.

Кожному тактовому сигналу відповідає включення дискретної пари випромінювача та приймача $i-\ddot{i}$ позиції координати X та $j-\ddot{i}$ позиції координати У, що виключає вплив бокових променів інших випромінювачів на формування вихідного сигналу зображення та забезпечує реєстрацію насіння в паралельних променях світла. При кожному такті сканування $T_0 \div T_7$ на виході підсилювачів 10, 11 формуються аналогові сигнали $K_0 \div K_7$ пропорційні інтенсивності променя, що реєструється. Циклічне порядкове сканування дискретних променів вздовж координат X,У забезпечує формування інформаційних рядків проекцій реєструємих насінин у вигляді $n+m$ розрядного двійкового коду, що знімається з виходів

Результати проведених досліджень вказують на: шляхи технічної реалізації блоку синхронізації, попередньої обробки, формування та передачі даних: необхідність більш

детального дослідження термінів виконання окремих операцій, які необхідно враховувати при розробці програмного забезпечення.

Принципи формування дискретних зображень в системах технічного зору

Невпорядкований потік дискретних об'єктів можна розглядати, як потік випадкових явищ: за напрямком, формою зображення, швидкістю, розміщенням та інше. Тому проблеми їх реєстрації та визначення необхідних статистичних та динамічних параметрів складно розв'язати навіть при сучасному рівні розвитку технологій. Принципи формування зображень в системах технічного зору, опису та розпізнавання образів, зниження шумів базуються, як правило, на побудові математичних моделей, розробці алгоритмів і виконанні цілого ряду складних аналітичних, числових і логічних перетворень [3].

Наприклад, при обробці і формуванні зображень, пов'язаних з вирішенням завдань сегментації, використовуються методи обчислення градієнта і оператора Лапласа, теорії графів, стохастичні та ін. Опис зображень пов'язано з визначенням дескрипторів і сигнатур [4]. Для зменшення шумів на апаратному та програмному рівнях використовуються як стандартні методи фільтрації так і деякі спеціалізовані нелінійні процедури: перетворення Фур'є, рекурсивні згладжують фільтри Бьюси-Калмана і ін.. При розпізнаванні образів застосовуються методи порівняння з еталоном, групового обліку ознак, статистичний, синтаксичний та ін. [5].

Доцільність застосування того чи іншого методу визначається характером вирішуваних завдань. Наприклад, при дослідженні та ідентифікації складних об'єктів можливе комплексне використання декількох зазначених вище методів, що супроводжується великим обсягом обчислень. У той же час, в задачах виявлення і реєстрації, не пов'язаних з ідентифікацією або сортуванням об'єктів, процедури обробки можуть бути більш простими. Як показала практика, при дослідженні невпорядкованого потоку дискретних об'єктів, пов'язаного з визначенням параметрів їх розподілу, швидкості руху, розташування, обліку та інших за допомогою оптичних систем, досить сформувати двухградаціонное зображення. У даній роботі розглядаються методи виявлення і формування таких зображень.

Аналітичні методи обробки зображень в системах технічного зору

Системи технічного зору знаходять широке застосування в різних областях науки і техніки. Вони складаються з блоків: реєстрації, попередньої обробки зображень і розпізнавання образів (рис.4)

Джерело зображення, в формалізованому вигляді, представляється функцією яскравості $F(x,y,t,\lambda)$, просторових координат x, y, часу t і довжин хвиль λ. При дослідженні стаціонарних процесів і сталості частотних характеристик випромінювачів яскравість зображення $F_p(x,y)$ на вході оптичної системи (ОС) блоку реєстрації можна розглядати як безперервну функцію просторових координат $F_1(x,y)$.

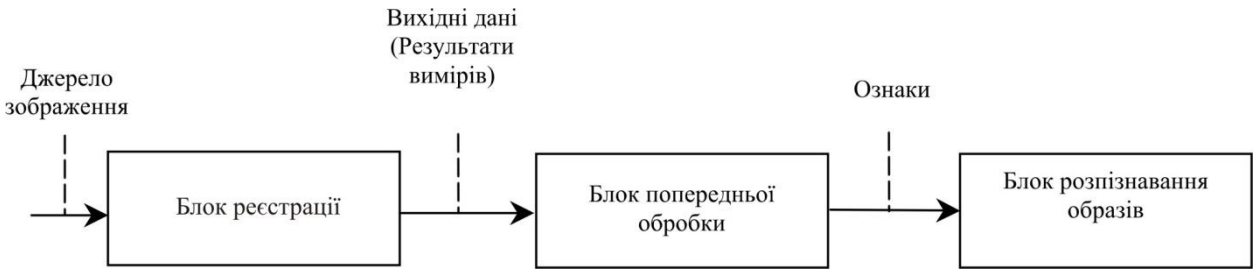


Рисунок 4 – Структурна схема технічного зору

Більшість сучасних оптичних систем використовує принцип сканування відеосигналу з виходів лінійок або матриць фотоприймачів, дискретизовані зображення на вході яких можуть бути представлені як результат модуляції безперервної функції $F_1(x,y)$ і просторово - діскретизуючої функції $S(x,y)$ (1):

$$F_p(x,y) = F_1(x,y) \cdot S(x,y) \qquad (1)$$

Функція $S(x,y)$ може бути отримана при пропусканні кінцевого набору дельта – функцій $\delta(x-i\cdot\Delta x, y-j\cdot\Delta y)$ через лінійний фільтр з одиничним імпульсним відгуком $P(x,y)$, який утворює решітку з кроком $(\Delta x\times\Delta y)$ (3.2):

$$S(x,y)=\sum_{i=1}^{n}\sum_{j=1}^{m}\cdot P(x,y)\cdot\delta(x-i\cdot\Delta x, y-j\cdot\Delta y) \qquad (2)$$

В результаті підстановки функції (3.2) в співвідношення (3.1) отримуємо формулу дискретизованої функції зображень (3.3):

$$F_p(x,y)=\sum_{i=1}^{n}\sum_{j=1}^{m}F_1(x,y)\cdot P(x,y)\cdot\delta(x-i\cdot\Delta x, y-j\cdot\Delta y) \qquad (3)$$

Звідси яскравість зображення на вході i,j -го фотоприймача описується виразом (4):

$$F_{i,j}(x,y)=F_1(x,y)\cdot P(x,y)\cdot\delta(x-i\cdot\Delta x, y-j\cdot\Delta y) \qquad (4)$$

Підсилений відеосигнал зображення U_{ij} на виході i,j-того фотоприймача ОС визначається співвідношенням (5):

$$U_{i,j}=\iint_{\Omega_{i,j}}K_i\cdot U_i\cdot F_{i,j}(x,y)\cdot\omega_{ij}(x-i\cdot\Delta x, y-j\Delta y), R_i\cdot dx\cdot dy\,, \qquad (5)$$

де: i = 1,2, .. n; j = 1,2, .. m; $\Omega_{i,j}$ - площа i,j -го осередку; U_i - напруга, прикладена до дискретного сприймаючого елементу; K_i- передавальна функція i-го підсилювача - формувача; R_i - навантажувальний опір; $\omega_{i,j}(x-i\cdot\Delta x, y-j\Delta y)$ - питома світлочутливість сприймаючої площини фотоприймача.

На рис. 3.5 і рис. 3.6 представлені фрагменти осцилограм відеосигналів, отриманих на виході лінійки фотоприймачів дискретних оптронні пар (ОП).

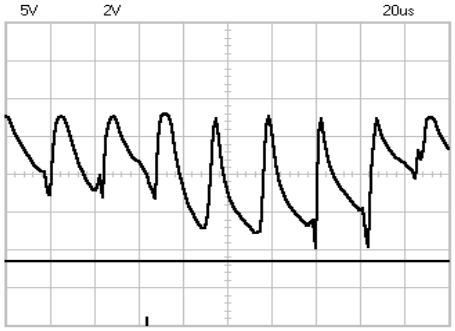


Рисунок 5 – Осцилограма затемнення 4-х ОП

Рисунок 6 - Осцилограма затемнення 2-х ОП

Блок попередньої обробки повинен забезпечувати: зменшення шумів, породжуваних процесом формування, вимірювання, квантування і передачі зображення; завдання порогового рівня; формування числових кодів і сегментацію зображень.

Одним з основних шляхів придушення шумів, підвищення контрастності, розмежування елементів фону і зображення об'єктів є встановлення порогового рівня.

Граничний рівень в загальному вигляді визначається виразом (6):

$$T=T\left[x,y,p(x,y),f(x,y)\right], \qquad (6)$$

де: $f(x,y)$ - яскравість зображення в точці (x,y); $p(x,y)$ - деяка локальна властивість, що впливає на характер зображення в околиці цієї точки, x,y - координата місця встановлення порогового рівня.

Зображення, сформоване пороговим рівнем, задається співвідношенням (7):

$$g(x,y)=\begin{cases}1, если f(x,y)>T\\0, если f(x,y)\le T\end{cases}, \quad (7)$$

відповідно до якого пікселі з рівнем інтенсивності $g(x,y)=1$ відносяться до зображення об'єкта, а пікселі з інтенсивністю $g(x,y)=0$ - до зображення фону. Це справедливо за умови, що інтенсивність об'єкта вище інтенсивності фону, в іншому випадку знаки в нерівностях (7) змінюються.

Якщо граничне значення T залежить тільки від $f(x,y)$, то поріг називається глобальним. Якщо значення T залежить як від $f(x,y)$, так і від $p(x,y)$, поріг називається локальним. Якщо, крім того, T залежить від просторових координат x, y, то такий поріг називається динамічним.

Глобальні пороги застосовуються в ситуаціях, коли є явне розходження між об'єктами і фоном і де освітленість досить однорідна. Методи зворотньоЇ і структурної освітленості, зазвичай дають зображення, які можуть бути сегментовані шляхом застосування глобальних порогів. Але, як правило, довільне освітлення робочого простору призводить до зображень, які, якщо виходити з визначення порогового рівня, вимагають локального аналізу для компенсації таких ефектів, як неоднорідність освітлення, тіні і відображення. відповідно до якого пікселі з рівнем інтенсивності відносяться до зображення об'єкта, а пікселі з інтенсивністю - до зображення фону. Це справедливо за умови, що інтенсивність об'єкта вище інтенсивності фону, в іншому випадку знаки в нерівностях (7) змінюються.

Визначити граничний рівень можна дослідним шляхом, в результаті аналізу відеосигналів зображень. Однак, для вибору оптимального порогу краще скористатися методом побудови апроксимуючої функції розподілу ймовірностей, як лінійної регресії доданків ймовірностей. У разі бімодальною гістограми апроксимуюча її функція задається рівнянням (8):

$$p(u)=F1\cdot f(u)+G1\cdot g(u), \quad (8)$$

де інтенсивність u - випадкова змінна величина, $f(u), g(u)$ - функції щільності розподілу ймовірностей, а $F1, G1$ - апріорні ймовірності, що визначають значимість кожного рівня градації в рівнянні. В даному випадку значення апріорних ймовірностей визначають вірогідність поява двох видів рівнів інтенсивності на образі - світлого і темного. Якщо відомо, що об'єкти складаються з темних пікселів, які займають, наприклад, 30% загальної площі зображення, то завжди апріорна ймовірність рівня темного $F1=0{,}3$ (піксель - елемент растрової решітки розміром $\Delta x\times\Delta y$ з інтенсивністю u). Виходячи з визначення повної ймовірності, апріорна ймовірність рівня світлого $G1=1-F1=0{,}7$.

Введемо наступні апроксимуючі функції розподілу ймовірностей випадкової величини u для рівнів темного $p1(u)$ і світлого $p2(u)$ (9):

$$p1(u)=F1\cdot f(u),\ p2(u)=G1\cdot g(u) \quad (9)$$

З теорії прийняття рішень відомо, що середня помилка визначення пікселя об'єкта в якості фону (і навпаки) мінімізується за допомогою наступного правила: розглядаючи піксель зі значенням інтенсивності u, підставляємо це значення в рівняння (9), потім ми визначаємо цей піксель, як піксель об'єкта, якщо $p1(u)>p2(u)$ або як піксель фону, якщо $p2(u)>p1(u)$.

Виходячи з цього, рівність ймовірностей $p1(u)=p2(u)$ визначає межу розділу між рівнями чорного і білого. Таким чином, значення оптимального порогового рівня інтенсивності $u=T$ визначається зі співвідношення (10) або точкою перетину графіків ймовірностей $p1(u)$ і $p2(u)$.

$$F1\cdot f(u)=G1\cdot g(u) \quad (10)$$

Розглянемо приклад використання даного методу для визначення порогового рівня відеосигналу зображень, отриманих при перетині потоком дискретних об'єктів площини реєстрації двокоординатного скануючого датчика.

Апріорна ймовірність появи затемнених пікселів - зображень об'єктів $F1 = 0{,}05$, апріорна ймовірність появи світлих пікселів – фону $G1 = 0{,}95$. Імовірність затемнення фонового пікселя змінюється по спадаючому експоненціальному закону розподілу $g(u)$ (11), а ймовірність затемнення пікселя, що входить до зображення об'єкта - по зростаючому експоненціальному закону розподілу $f(u)$ (11). При цьому приймаємо, що u - це напруга відеосигналу, величина - обернено пропорційна інтенсивності.

$$g(u) = e^{-(u)}, \quad f(u) = 1 - e^{-(u)} \tag{11}$$

Будуємо графіки апроксимуючих функцій розподілу ймовірностей і $F(u)$ та $G(u)$ (12) (рис.4).

$$F(u) = F1 \cdot \left[1 - e^{-(u)}\right] \quad G(u) = G1 \cdot e^{-(u)} \tag{12}$$

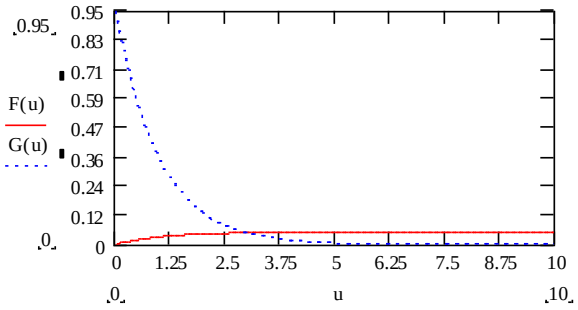


Рисунок 7 – Графіки функцій

Виходячи зі співвідношення (10) оптимальне значення порогового рівня визначається точкою перетину функцій $F(u)$ та $G(u)$. Звідси $T = u = 2.8V$. Отримане значення практично збігається з емпіричним. При цьому похибка у визначенні порогового рівня не перевищує $\pm 3\%$.

Зазначений метод доцільно застосовувати для визначення порогового рівня, якщо відомі закони розподілу інтенсивності $g(u)$ та $f(u)$ при квантуванні за двома рівнями.

Сегментація є одним з етапів в роботі системи технічного зору, так як саме на цій стадії обробки проводиться розмежування елементів об'єкта і фону, з метою їх подальшого розпізнавання. Методи сегментації базуються на двох фундаментальних принципах: розривності і подобі. Перший служить для виділення меж і визначення контурів, а другий - для формування області зображення об'єкта.

Визначення меж може проводитися за допомогою методу градієнта або методу градієнта і оператора Лапласа, як найбільш наочних. В ідеальному випадку ці методи визначають пікселі, що лежать на кордоні між об'єктом і фоном.

Перший метод заснований на обчисленні градієнта зміни інтенсивності або напруги відеосигналу по кожному досліджуваному пікселю зображення і визначається співвідношенням (13):

$$G[f(x,y)] = [G^2{}_x + G_y^2]^{1/2} = [(\frac{\partial f}{\partial x})^2 + (\frac{\partial f}{\partial x})^2]^{1/2} \tag{13}$$

Якщо величина градієнта для даного пікселя $G[f(x,y)] \geq T$, що говорить про крутизну зміни інтенсивності, то цей піксель є граничним між елементами фону і об'єкта або об'єкта і фону. В іншому випадку, якщо $G[f(x,y)] < T$, то цей піксель є елементом фону або об'єкта. Недоліком цього методу є невизначеність у встановленні типу переходу: з фону на об'єкт або з об'єкта на фон.

Наступний метод базується на обчисленні операторів градієнта і Лапласа, що дозволяє виключити вказаний вище недолік, шляхом побудови трирівневого зображення. Введення Лапласіану $L[f(x,y)]$ (3.14) дозволяє ідентифікувати ознаку переходу від фону до об'єкта (-, +), якщо $L[f(x,y)]<0$ і від об'єкта до фону (+, -), якщо $L[f(x,y)]\geq 0$.

$$L[f(x,y)]=\frac{\partial^2 f(x,y)}{\partial x^2}+\frac{\partial^2 f(x,y)}{\partial y^2} \qquad (14)$$

Побудова трирівневого зображення $s(x,y)$ визначається співвідношенням (15):

$$s(x,y)=\begin{cases}0, если G[f(x,y)]<T,\\ +,- если G[f(x,y)]\geq T; L[f(x,y)]\geq 0,\\ -,+ если G[f(x,y)]\geq T; L[f(x,y)]<0\end{cases} \qquad (15)$$

де символи 0, +, - представляють три різних рівня інтенсивності, які визначають пікселі фону, об'єкта і кордони.

Виходячи з цього, зображення сканованих рядків, що містять частини об'єкта, можуть бути описані в такий спосіб:

$(\cdots)(-,+)(+,\cdots,+)(+,-)(\cdots)$,

де: $(\cdots)$ є довільною комбінацією +, - або 0; інші комбінації символів визначають піксель кордону (-), тип переходу з фону на об'єкт $(-,+)$, точки об'єкта $(+,\cdots,+)$, тип переходу з об'єкта на фон $(+,-)$.

Алгоритми **побудови і опису контурів** містять процедури виявлення і простежування кордонів об'єктів з відповідних послідовностей пікселів з оцінкою типу з'єднання (по ребру або діагоналі) і процедури опису із застосуванням ланцюгового коду.

Для визначення і з'єднання точок контуру досліджуваного об'єкта використовується метод послідовного аналізу характеристик пікселів в невеликій околиці (розміром 3x3) кожної, виявленої раніше за допомогою методу градієнтів, граничної точки. Цей метод базується на оцінці наявності, визначенні типу та описі коду зв'язності між центральним і сусідніми елементами досліджуваної околиці. Оцінка наявності зв'язності задається співвідношенням (16):

$$\left|G[f(x,y)]-G[f(x',y')]\right|\leq T, \qquad (16)$$

Де $G[f(x,y)]$ - величина градієнта центральної точки, обчислена за формулою (13); $G[f(x',y')]$ величина градієнта однієї з сусідніх точок; T - пороговий рівень. Таким чином, два сусідніх пікселя з координатами (x,y) і (x',y') зв'язні між собою, якщо різниця між величинами їх градієнтів або інтенсивностей не перевищує оптимального порогового рівня.

Для **визначення типу зв'язності** використовуються поняття четирехсвязності і восьмизв'язності. Під четирехсвязністю мається на увазі зв'язність за чотирма напрямками: вгору, вниз, вліво, вправо, тобто по ребру. Під восьми зв'язністю розуміється зв'язність по восьми напрямках, яка враховує і наявність зв'язності по діагоналі (по дузі).

Ефективність кодування контуру забезпечується застосуванням ланцюгового коду, який дозволяє для будь-якого розглянутого (центрального) елемента зображення задати сусідній піксель контуру.

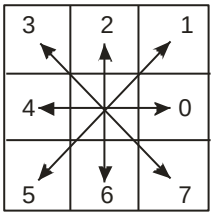


Рисунок 8 – Ланцюговий код

Оскільки черговий піксель контуру є одним з восьми елементів зображення, сусідніх стосовно розглядуваного (при використанні прямокутного растра), для кодування чергового пікселю контуру достатньо використовувати одне число з набору цілих чисел від 0 до 7. Ідея ланцюгового коду проілюстрована рис. 5. За описом контуру в ланцюговому коді можна обчислити ряд ознак, зокрема площу, обмежену контуром, кривизну в певному пікселі контуру, довжину контуру, а також визначити, контур замкнутий чи ні.

При формуванні зображень об'єктів використовується описаний вище метод оцінки зв'язності (16). Подальша обробка отриманих зображень зводиться до операцій стиснення (стирання кордонів), розширення, побудови кістяка і до інших дій, необхідних для виділення ознак і розпізнавання образів.

Розглянуті аналітичні методи, в доступній і теоретично обґрунтовананій формі, пояснюють принципи виявлення і формування зображень, але не завжди знаходять практичне застосування.

Розробка структурної схеми програмного забезпечення блоку СПО та ПД

Розроблюваний програмний продукт вузла СПО та ПД повинен відповідати заданим технічним вимогам і забезпечувати такі терміни виконання операцій, щоб вони не виходили за рамки технологічного процесу, який обробляється.

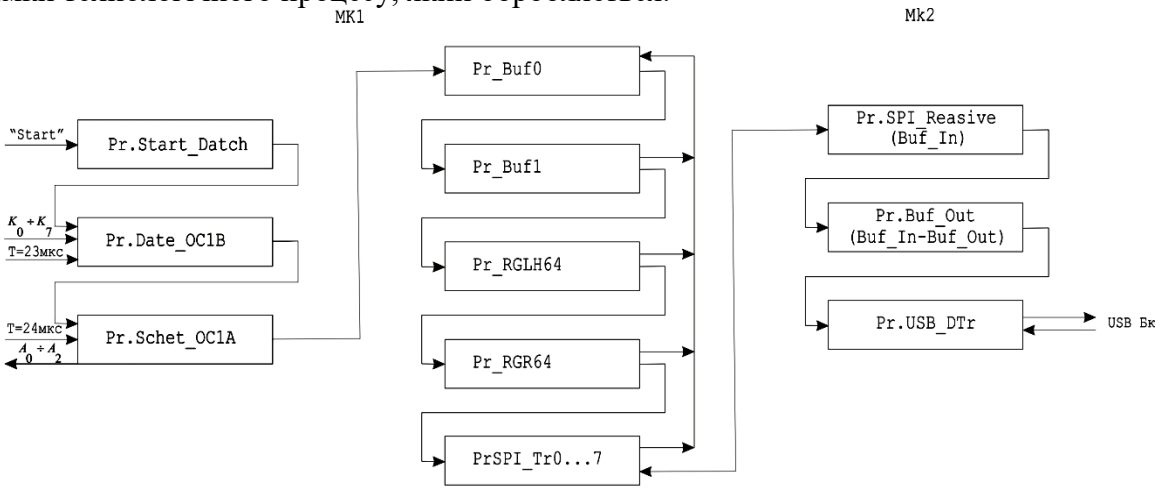


Рисунок 9 - Структурна схема програмного забезпечення вузла СПО та ПД

повноту і послідовність виконання програмами операцій з приймання, попередньої обробки та передачі даних від вузла реєстрації до бортового комп'ютера.

Програма Start_Datch стартує від кнопки «Start/Stop» і запускає роботу головної програми мікроконтролера МК1.

Програма Data_OC1B спрацьовує від вектора переривання OC1B-23мкс, який задається 16 - розрядним таймером/лічильником МК1 на 23мкс кожного 24-х мікросекундного такту. За цією програмою восьми бітні коди даних $D_0 \ldots D_7$ сформовані регістрами нижнього RGL8 та верхнього RGH8 рівнів квантування сигналів $K_0 \ldots K_7$ вузла реєстрації заносяться в порти A і C МК1.

Запуск програми Schet_OC1A здійснюється вектором переривання OC1B-24мкс. За цією програмою виробляються адресні коди $A_0 \ldots A_7$, які формують тактові імпульси сканування площини контролю вузла реєстрації і визначають адресу запису даних в буфер Buf0.

Програми Pr_Buf0, Pr_Buf1 та Pr_RGHL64 формують вихідні коди рядків сканування нижнього RGL64 та верхнього RGH64 рівнів сканування із невпорядкованого потоку вхідних даних.

Програма Pr_RGR64 формує вихідний результуючий код рядка зображення об’єкту RGR64 на підставі сформованих даних RGL64, RGH64 поточного рядка та даних RGR64 попереднього рядка за принципом «гістерезиса» і заносить його в 64-х байтний буфер пам’яті BufTr.

Програми SPI_Tr 0-7 виконують передачу сформованих даних з буфера пам’яті BufTr МК1 в 16-ти байтний вхідний буфер пам’яті BufIn МК2 в режимі Master.

Програма SPI_Reasive МК2 забезпечує приймання 16 байт даних від МК1 в буфер пам’яті BufIn в режимі Slave.

Передача даних з BufIn в 64-х байт ний вихідний буфер памяті BufOut здійснюється програмою Buf_Out. При появі дозволу на приймання даних програма USB_Tr виконує передачу 64 байт даних через канал USART – USB МК2 до бортового комп’ютера.

Висновок. У статті розглянуто та проаналізовано програмне забезпечення, яке призначено для о системи вузла синхронізації, попередньої обробки та передачі даних засобу ідентифікації зернового потоку. В межах України в недостатній мірі представлені вітчизняні розробки в цій області. У роботі наведені теоретичне узагальнення й рішення наукового завдання дослідження методів теорії інформації, інформаційного аналізу, методи теорії формування цифрових кодів та сканування об’єктів при дослідженні засобу ідентифікації зернового потоку, основи теорії цифрових систем автоматичного управління та математичного моделювання. Рішення даного завдання полягало у вирішенні наступних задач: Провести аналіз методів обробки зображень в системах технічного зору і визначити шляхи їх практичної реалізації; Виконати детальний аналіз існуючих методів та засобів реєстрації дискретних рухомих об’єктів та формування їх цифрових зображень; Розробити методику та алгоритми формування бінарного коду зображень площини контролю вузла реєстрації; Розробити програмне забезпечення блоку синхронізації, попередньої обробки та передачі даних зображення дискретних об’єктів до ПК. Розроблені під час виконання роботи алгоритми дозволяють успішно вирішувати завдання по формуванню вихідного бінарного коду рядка зображення та передачі його до ПК. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудовано алгоритм і обрано середовище розробки. Розроблене програмне забезпечення зручне у використанні, і не потребує особливих спеціальних знань. Для забезпечення максимальної гнучкості при роботі з апаратними ресурсами контролерів, оптимізації програм по швидкості виконання, оптимізації програм за розміром коду використовувалась мова програмування Assembler. Запропоноване програмне забезпечення є спеціальним, розроблене для даної конкретної системи й включає програми, що реалізують її функції. Програма призначена для виконання під управлінням мікроконтролерів фірми AVR ATMega16. Даються необхідні рекомендації з впровадження системи в експлуатацію. Для підвищення рівня безпеки запропоновано використання цифрових водяних знаків у вигляді додаткового коду в програмі. В цілому створене програмне забезпечення підтверджує правильність використаних проектних рішень та повністю відповідає вимогам технічного завдання. Створене програмне забезпечення має потенційну можливість для подальшого вдосконалення і застосування у системах ідентифікації в складі САК або СКВ .

Список літератури

1. Пархоменко М. Д. Исследование, разработка, изготовление, испытание электронного преобразователя пропашных и других культур в поток электрических импульсов / М. Д. Пархоменко, А. А. Лукьяненко // Отчёт по НИР, №80032803. – Кировоград: КИСМ, 1985. – 210с.
2. А. с. 1356981 СССР, МКИ3 А 01 С 7/00, G 01 D 9/00. Устройство регистрации семян в потоке / Пархоменко М. Д., Лукьяненко А. А., Крамаренко В. Н., Криворожeнко Э. И. (СССР). - №3888780/30-15; заявл. 25.04.85; опубл. 07.12.87, Бюл. №45.
3. Фурман Я. А. Цифровые методы обработки и распознавания изображений / Фурман Я. А., Юрьев А. Н., Яншин В. В. – Красноярск: Изд-во Красноярского университета, 1992. – 248с.

4. Фор А. Восприятие и распознавание образов: пер. с франц. А.В. Серединского. / А. Фор. – М.: Машиностроение, 1989. – 272с.
5. Путятин Е.П. Обработка изображений в робототехнике / Е.П. Путятин, С.И. Аверин. - М: Машиностроение, 1990. - 320с.
6. Бойко В. І. Основи схемотехніки електронних схем: підручник / Бойко В. І., Гурій А. М., Жуйков В. Я. та ін. – К.: Вища шк., 2004. – 527 с.
7. Бродин В. В. Системы на микроконтроллерах и БИС программируемой логики / Бродин В. В., Калинин А. В. – М.: ЭКОМ, 2002. – 400с
8. Волошин М. Перспективна техніка для посіву дрібнонасінневих культур: сівалки СЗТ – 5,4 та СЗ-5,4-0,6 «Клен» / Волошин М. // Техніка АПК: наук.–технічний журнал. — К.: НВО «Сільгоспмашсистема», 2008. — № 3-4. — С. 36-38.
9. Голубцов М. С. Микроконтроллеры AVR: от простого к сложному / Голубцов М. С. - М.: СОЛОН-Пресс, 2003. - 288с.
10. Гребнёв В. В. Микроконтроллеры семейства AVR фирмы ATMEL / Гребнёв В. В. - М.: ИП РадиоСофт, 2002. - 176с.

УДК 004

Р. Письмений, магістр гр. КІ-18М-1,9
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ ВІДЕОСПОСТЕРЕЖЕННЯ ДЛЯ РЕАЛІЗАЦІЇ СТРАТЕГІЇ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ПІДПРИЄМСТВА

У статті розглянуто програмне забезпечення, яке призначено для системи відеоспостереження для реалізації стратегії забезпечення безпеки підприємства. Метою розробки є дослідження та програмна реалізація системи відеоспостереження для реалізації стратегії забезпечення безпеки підприємства. Об'єктом дослідження є процес відеоспостереження для реалізації стратегії забезпечення безпеки підприємства. Предметом дослідження є методи відеоспостереження для реалізації стратегії забезпечення безпеки підприємства. Методи дослідження базуються на методах теорії кодування відеоданих, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи відеоспостереження для реалізації стратегії забезпечення безпеки підприємства. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення. Розроблено зручний інтерфейс користувача. Наведені інструкції по роботі з програмними засобами.

комп'ютерна інженерія, захист доступу, відеоспостереження

Постановка проблеми. Щоб система відеоспостереження була встановлена не для галочки, а дійсно справлялася зі своїм завданням фіксації подій, проект її реалізації повинен бути ретельно пророблений. Поряд з вибором камер критичне значення має інфраструктура для передачі й зберігання даних.

За числом камер відеоспостереження на душу населення Кропивницькому поки ще далеко до Києва, але їх стає усе більше й більше. Однак значна частина встановлених камер використовується неефективно й не справляється зі своїми завданнями. Більше того, в 80% випадків відеоспостереження нікому не потрібно й про нього згадують тільки при настанні позаштатної ситуації. У багатьох інфраструктурних проектах відеоспостереження чи підключається не в останній день. На таких системах воліють заощаджувати, установлюючи для галочки, але все це доти, поки щось не трапиться: пожежу, пограбування й т.п.

Основними завданнями при установці систем відеоспостереження є забезпечення оперативного реагування на події і їхню фіксацію. Однак вирішити їх можна лише в тому

випадку, якщо вжиті необхідні заходи, зокрема, продумані процеси відпрацьовування вступників сигналів з поста відеоспостереження. Сама по собі система відеоспостереження марна, якщо за нею не стоїть організаційна структура. Тим часом, лише 10% всіх замовників установлюють систему відеоспостереження в рамках реалізації ретельно вивіреної стратегії забезпечення безпеки.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини системи відеоспостереження для реалізації стратегії забезпечення безпеки підприємства.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи відеоспостереження для реалізації стратегії забезпечення безпеки підприємства.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем відеоспостереження для реалізації стратегії забезпечення безпеки підприємства.

– Дослідження системи відеоспостереження для реалізації стратегії забезпечення безпеки підприємства.

– Програмна реалізація системи відеоспостереження для реалізації стратегії забезпечення безпеки підприємства.

Об'єктом дослідження є процес відеоспостереження для реалізації стратегії забезпечення безпеки підприємства.

Предметом дослідження є методи відеоспостереження для реалізації стратегії забезпечення безпеки підприємства.

Методи дослідження базуються на методах теорії кодування відеоданих, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу.

Опис функціонування системи

Якщо ви вирішили придбати систему відеоспостереження, то виникають цілком виправдані питання: як це зробити і яку систему відеоспостереження вибрати? Багато споживачів, найчастіше, жадають від постачальника якісний продукт за мінімальні гроші – це правильне й абсолютно нормальне бажання. Проте вибір – завжди за вами. І він повинен виправдувати витрачені засоби.

При виборі системи відеоспостереження важливо в підсумку одержати те рішення (і, відповідно, придбати встаткування), що гарантовано забезпечить виконання завдань. Якщо коштів на покупку поки недостатньо, те, імовірно, кращим рішенням стане почекати із придбанням або взагалі відмовитися від реалізації даного проекту. Нема рації інвестувати гроші в те встаткування, що себе не виправдає. Необхідно розуміти, що за якість, надійність, довговічність і гарантію відмінної роботи необхідно платити. Ніхто не очікує від старенького й потриманого автомобіля надійної й безвідмовної роботи. Напевно, краще придбати нове авто у фірмовому салоні із заводською гарантією й повним сервісним обслуговуванням. Тому кращою відповіддю на питання «як вибрати систему відеоспостереження?», по-нашій думці, буде відповідь: *найкраще вибирати не систему відеоспостереження, а виконавця (продавця/постачальника).* Відповідно, варто шукати фахівців із систем відеоспостереження й безпеки.

1. На початковому етапі вам необхідно визначити основну мету установки відеоспостереження: для чого необхідна система. Сформулюйте її в письмовому виді. Формулювання можуть бути самими різними, але в кожному разі, вони необхідні особисто вам або вашому підприємству.

2. Знайдіть кілька компаній, що пропонують установку систем відеоспостереження. Запропонуєте їм взяти участь у тендері й повідомите цілі й завдання.

3. Одержите письмове підтвердження про бажання взяти участь у конкурсі.

4. Можна й навіть найчастіше потрібно покладатися на рекомендації знайомих: це вже свого роду гарантія якості наданих раніше послуг. Запросите до участі в тендері

рекомендованих фахівців. При цьому помнете, що ви будете платити гроші й користуватися результатами їхньої роботи.

5. Не напружуйтеся. Не слід занадто заглиблюватися у вивчення різних видів відеокамер, плат відеоспостереження, відеореєстраторів, їхніх параметрів і характеристик: ваше завдання – сформулювати бажаний результат. А потенційні виконавці повинні її уважно вивчити й надати в ПИСЬМОВОМУ ВИДІ не тільки таблиці з розрахунками, але ще й пояснювальну записку, технічне завдання, а також докладні специфікації. При складанні кошторису практично на кожну позицію вимагайте надання специфікації або докладного опису встаткування з характеристиками. На металовироби, стяжки й інші видаткові матеріали специфікацію вимагати не обов'язково, але на відеокамери, плати відеоспостереження або DVR, кабельну продукцію, блоки живлення й інше дороге встаткування – докладна специфікація обов'язкова!

6. Цілком можливо, що від вас зажадають конкретизацію окремих питань. Співробітники деяких компаній можуть попросити вас відповісти на них письмово, інші вислухають і запишуть інформацію з ваших слів – відповіді на ці питання важливі, вони дозволяють більш точно зрозуміти виконавцеві ваші цілі й завдання при розробці проекту.

7. За умови того, що співробітники компанії-інсталятора всі обговорюють тільки в усній формі (і ви відчуєте, що їм важливо поговорити, обговорити, розповісти), можете сміло розставатися з такою компанією. Вимагайте письмових питань, пояснень, роз'яснень на всі ваші питання – це єдино вірне й правильне рішення. Мало того, що письмова інформація збереже ваш дорогоцінний час, вона заощадить кошти, а також забезпечить гарантію досягнення поставленої цілі.

8. Відповіді на будь-які ваші питання виконавці повинні надати в писемній формі. Не соромтеся задавати БУДЬ-ЯКІ питання, наприклад: «Чому пропонована система відеоспостереження така дорога?» Або навпаки: «Чому цей варіант відеоспостереження найдешевший?» «Чим камера відеоспостереження AVZ-12DSF-14-AV відрізняється від пропонованою іншою компанією камери ZAV-140RAS-66-5? Чим обумовлений вибір саме цієї моделі відеокамери? Чому інсталятор уважає, що для цієї зони огляду досить відеокамери 400 ТВЛ?» – помнете, що все це стоїть ваших грошей.

9. Вам не слід соромитися й думати, що спілкування з виконавцем займе багато вашого часу: з'ясовуйте будь-який не зрозумілий вам питання. І якщо у вас залишилися такі (втім, як і будь-якого роду сумніву), сховайте ваш гаманець подалі. Ключові поняття для успішної реалізації будь-якого проекту – це ясність і простота.

10. Якщо вас починають «вантажити» технічними характеристиками, термінами й словами типу «найефективніша», «це оптимальний вибір», «дуже вигідна пропозиція», можете ліниво позіхнути, і задати для почала питання: «*Кому пропоноване рішення дуже вигідно? Продавцеві? Або все-таки мені?*» Якщо вам, то в проекті повинен бути даний чітка і ясна відповідь, чому пропонований варіант є самим вигідним! Надати опис, порівняння й обґрунтований вибір повинен продавець. Покупка системи відеоспостереження повинна бути для вас максимально простій, як поїздка на поїзді з міста «А» у місто «Б». Подумайте, кому цікаві характеристики локомотива, напруга мережі, діаметр коліс, висота рейка або кількість шпал?

Ринок систем відеоспостереження росте з кожним днем. Кількість пропонованого товару просто величезне. Для більше зручного орієнтування для Вас, у море систем відеоспостереження, пропонується наступна класифікація продуктів. Всю продукцію систем відеоспостереження умовно можна розділити на 3 групи.

Група 1 – Системи не потребуючих ПК пристроїв

Дана система працює за рахунок убудованих відеореєстраторів.

Основні переваги:

– Простота й зручність у використання. Якщо немає необхідності розширювати систему, переходити на мережне відеоспостереження, то даний вид відеоспостереження цілком підходить.

– Можливість тривалої безперебійної роботи. Системи, що працюють при підключенні до комп'ютера, дуже часто вимагають перезавантаження, під час яких відеоспостереження припиняється. При використанні реєстраторів дана проблема відпадає.

– Безпека. У силу відсутності ПК пристрою, немає й ризику вірусних атак або зломів.

Недоліки:

– Обмеженість функцій. Дана система «заточена» під вузького функціонала й розширенню не підлягає.

– Неможливо переглядати «живе» і архівне відео одночасно.

На сьогоднішній день система відеоспостереження non-PC помітно поліпшила свої позиції. По-перше, завдяки тому, що вони обзавелися можливістю мережного відеоспостереження.

Група 2 – Системи, що працюють через ПК пристрої

Дані системи відеоспостереження працює винятково через комп'ютери.

Основні переваги:

– Система більше зручна у використанні. Легше перемикатися з однієї камери на іншу. Можна дуже швидко зробити фото зображення й роздрукувати.

– Можливість одночасного перегляду «живого» і архівного відео.

– Можливість модернізації системи. Наприклад, установка додаткових каналів відеоспостереження (камер спостереження). Найчастіше система, інтегрована на базі ПК, використовується при установці більш ніж 16 камер спостереження.

Недоліки:

– Потрібна часте перезавантаження комп'ютера, під час якої відеозапис зупиняється.

– Високий ризик атаки вірусів і зломів системи.

При виборі даної системи відеоспостереження бажано звертатися до перевірених постачальників, оскільки ринок зараз затоплений неліцензійними товарами без гарантії на роботу системи.

Група 3 – IP відеоспостереження

Дана система так само працює через підключення до персонального комп'ютера, однак у цьому випадку ПК необхідний тільки для виводу картинки. Даний тип відеоспостереження є найбільш новим і усе ще розвивається. IP система найчастіше використовується для налаштування мережного відеоспостереження або спостереження через інтернет. IP система відеоспостереження використовує, у якості складових, IP-камери й IP-відеореєстратори. Для передачі відеопотоків використовується стек протоколів TCP/IP. У даний момент це саме динамічно, що розвивається напрямок, ринку, чому сприяє неухильно, що знижується вартість, що становить системи.

Основні переваги:

– Проста система налаштування, досить мати мережа LAN або просто модем. Для початку роботи необхідно підключити IP камеру в мережу, щоб система початку функціонувати. До кожної камери в цьому випадку привласнюється своя IP адреса. Перевага IP камер у високій якості зображення.

– Немає необхідності проводити додаткові кабелі (можливий підключення без кабелю, через бездротової адаптер).

– Можливість автономної роботи системи, без використання ПК. Необхідна тільки комп'ютерна мережа.

– Можливість перегляду зображення й керування IP камерою дистанційно в режимі реального часу. Досить мати доступ до інтернету. До речі, при установці необхідних налаштувань, можна здійснювати відеоспостереження на телефоні. Зараз ринок удосталь пропонує програми, які дозволяють одержувати картинку з камер спостережень на смартфон.

– Необмежена кількість камер спостереження.

– Висока розв'язна здатність, обмежена лише пропускною здатністю мережі й параметрами використовуваного встаткування.

– Відстань передачі відеопотоку від IP-камери відеоспостереження не обмежено межами локальної мережі. У такий спосіб досягається масштабованість системи. IP-відеореєстратор здатний записувати відеопотоки від IP-камер що перебувають, наприклад, в іншому місті.

– Можливість використання для передачі відеопотоків існуючі комп'ютерні мережі.

– Можливість тонкого налаштування параметрів IP-відеокамер через web-інтерфейс. Настроїти можна як параметри зображення, такі як: яскравість, контрастність, колірний баланс, так і вибрати кодек для роботи з відеозображенням, виставити зони зображення по яких камера видасть сигнал об виявлення руху, указати e-mail або параметри ftp сервера, на який будуть відправлені кадри у випадку виявлення руху в кадрі й багато чого іншого.

– Завдяки технології TCP/IP стала можливим побудова бездротових систем HD і Full HD відеоспостереження що використовують Wi-Fi камери.

– Розв'язна здатність IP камер і реєстраторів не обмежується дозволом HD і Full HD. Бюджетний сегмент ринку завойовують камери й реєстратори підтримуючий дозвіл 4 Мп і все більше застосування знаходить устаткування розв'язної здатності 4k (8 – 12 Мп).

Мережний відеореєстратор (NVR) вхідний у комплект для IP відеоспостереження виконує роль сервера запису відеопотоків від камер. Його завдання – забезпечити надійний запис на жорсткий диск, надати зручний і швидкий пошук потрібного відео в архіві за інтересуючим вас критерієм, будь те пошук за часом доби або по тривожній події, такому як рух у кадрі. Крім того, до NVR можна одержати доступ із клієнтського ПЗ, для віддаленого перегляду живого відео й архівів на смартфонах, планшетах або за допомогою віддалених стаціонарних PC.

Недоліки:

– Висока вартість продукції. У порівнянні з аналоговою продукцією вартість IP камер вище в 5-10 разів.

IP система дає тільки стисле зображення, яких необхідно декодувати.

HDCVI

HDCVI (High Definition Composite Video Interface) – один зі стандартів систем HD відеоспостереження, що використовують передачу відеосигналу по коаксіальному кабелі. На першому етапі технологія HDCVI поєднувала два дозволи в прогресивному скануванні – 1080p (1920x1080) і 720p (1280x720). В 2016 році компанія Dahua (основоположник формату й основний виробник устаткування для відеоспостереження формату HDCVI) випустила камери й відеореєстратори HDCVI з розв'язною здатністю – 4 Мп (2560x1440), а до 2017 г устаткування з дозволом 8 Мп. Крім того, у відмінності від конкурентів, з 2015 року на ринку присутні камери відеоспостереження з можливістю передачі звуку разом з відеосигналом по одному кабелі.

Переваги:

– Розв'язна здатність камер: 8 Мп (3840x2160), 4 Мп (2592x1520), 1080 p (1920×1080) і 720 p (1280×720).

– Аналогова модуляція.

– Відсутність компресії й інтермодуляції.

– Передача по коаксіальному кабелі або кручений парі (за допомогою широкополосних пасивних або активних приймачепередатчиків).

– Надійна передача від джерела до приймача без тимчасової затримки.

– Максимальна дальність передачі сигналу HDCVI з дозволом 4 Мп у нових камерах Dahua становить 700 м. по коаксіальному кабелі 75 Ом діаметром 6mm і 300 м. по UTP кабелі.

– Композитний сигнал відео/аудіо/PTZ – по одному кабелі передається не тільки відео, але й додаткові сигнали, такі як аудіо сигнал і сигнали керування трансфокатором і поворотним пристроєм.

– Двостороння передача даних.

Ціна HDCVI системи відеоспостереження нижче вартості IP систем.

HD-TVI

HD-TVI (High Definition Transport Video Interface) – один зі стандартів передачі аналогового HD і Full HD відео по коаксіальному кабелі. Комерційна назва формату – Turbo HD. Даний формат одержав свій розвиток завдяки компанії Hikvision. К 2017 камери спостереження HD-TVI досягли розв'язної здатності 5 Мп (2592x1920).

Переваги:

– Розв'язна здатність камер: 5 Мп (2592x1920), 3 Мп (1920x1538), 1080 p (1920×1080) і 720 p (1280×720).

– Аналогова модуляція.

– Відсутність компресії й інтермодуляції.

– Передача по коаксіальному кабелі або кручений парі (за допомогою широкополосних пасивних або активних приймачепередатчиків).

– Надійна передача від джерела до приймача без тимчасової затримки.

– Дальність передачі в розв'язній здатності 1080 p (1920x1080) і 720 p (1280×720) – 500m по коаксіальному кабелі 75 Ом діаметром 6 mm.

– Композитний сигнал відео/аудіо/PTZ

– Двостороння передача даних.

– Висока завадостійкість Turbo-HD камер. Поширення сигналу без паразитних високочастотних випромінювань і зображення, вільне від перешкод і зриву синхронізації.

Ціна HD-TVI (Turbo HD) системи відеоспостереження приблизно дорівнює вартості HDCVI систем.

AHD

AHD (High Definition Transport Video Interface), подібно HDCVI і HD-TVI (Turbo HD), є композитним інтерфейсом за допомогою якого передається аналоговий відеосигнал у розв'язній здатності 4 Мп, 3 Мп, Full HD (1080 p) і HD (720 p). Формат AHD, як і його два конкуренти, забезпечує відмінну якість HD картинки й передачу відеосигналів на ті ж 300 – 500 м по якісному коаксіалу.

– Розв'язна здатність устаткування: 4 Мп, 3 Мп, 1920H (1920×1080) і 1280H (1280?720).

– Аналогова модуляція.

– Відсутність компресії й інтермодуляції.

– Передача по коаксіальному кабелі або кручений парі (за допомогою широкополосних пасивних або активних приймачепередатчиків).

– Надійна передача від джерела до приймача без тимчасової затримки.

– Завдяки потужному еквалайзеру досягається дальність передачі Full HD сигналу на відстань 500 м. по коаксіальному кабелі 75 Ом діаметром 6 mm.

HD-SDI

HD-SDI інтерфейс (High-Definition Serial Digital Interface) був розроблений для використання в телебаченні високої чіткості. Інтерфейс описується стандартом SMPTE 292M і має на увазі передачу відеоданих з параметрами 720p і 1080i з бітрейтом 1,485 Гбіт/с по одному коаксіальному кабелі із хвильовим опором 75 Ом на відстань до 100 м. без додаткових підсилювачів або більше 100 м. з використанням підсилювачів HD-SDI.

Інтерфейс 3 G-SDI описується стандартом SMPTE 424M і має на увазі передачу відеоданих з параметрами 1080p з бітрейтом 2,970 Гбіт/с по одному коаксіальному кабелі із хвильовим опором 75 Ом на відстань до 100 м. без додаткових підсилювачів або більше 100 м. з використанням підсилювачів 3G-SDI.

Переваги:

– розв'язна здатність до 1080 p (Full HD).

– відсутність затримки поширення відеоданих.

– повна відсутність наведених перешкод.

Недоліки: відстань передачі аналогового сигналу без додаткових пристроїв – до 100 м. по якісному коаксіальному кабелі. для передачі на більші відстані застосовуються ретранслятори HD-SDI або передавачі сигналу HD-SDI по оптоволокну.

Слід зазначити, що HD-SDI формат використовується в якості студійного для цифрової передачі Full HD відео без наведених перешкод на помірні відстані. Застосування в системах відеоспостереження стримується його підвищеними вимогами до ліній передачі (якісний коаксіал до 100м.).

Розробка структурної схеми

Якщо не приділяти належну увагу всій системі відеоспостереження, у тому числі інфраструктурі, по якій дані будуть передаватися, то належного рівня ефективності домогтися не вдасться. Сучасні комплекси відеоспостереження висувають свої вимоги й до мережі передачі даних. З урахуванням обсягів переданого трафіку мережа повинна забезпечувати високу пропускну здатність, бути надійною, захищеною й досить інтелектуальною, щоб самостійно реагувати на погрози й підтримувати свою працездатність. Це важливо, тому що містити штат персоналу для цілодобового контролю за роботою кожного пристрою в мережі мало хто може собі дозволити.

Часто в мережі підприємства присутні дві відособлені інфраструктури: мережа підприємства й мережа безпеки (для відеоспостереження). Однак, сьогодні в більшості проектів використовуються цифрові камери, інформацію з яких можна передавати по мережі передачі даних, що обслуговує саме підприємство. Це дозволяє дві відособлені мережі замінити однією. Таке об'єднання приводить до оптимізації витрат і при побудові, і при обслуговуванні мереж. А завдяки використовуваній технологічній базі співробітники служби безпеки можуть бути впевнені в тім, що вони стануть одержувати стабільний, високоякісний відеопотік, доступний у режимі 24/7. У той же час така ж надійна й продуктивна робота гарантується й для інших відділів – бухгалтерії, кадрів, розробки й т.п., при цьому доступ до різних даних і сервісів буде розмежований і захищений.

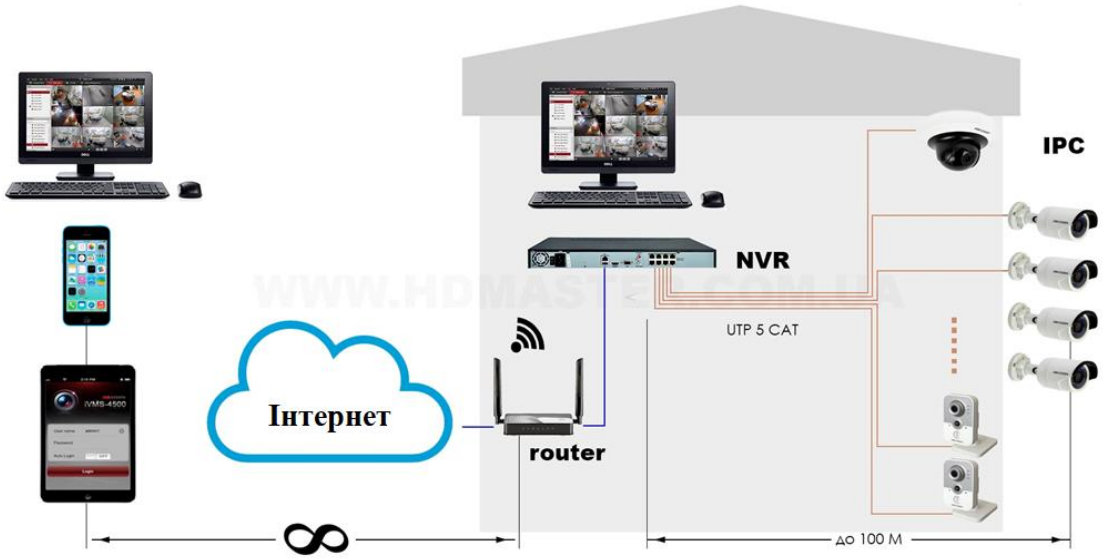


Рисунок 1 – Структурна схема системи

При використанні IP-камер, замість двох окремих мереж – для відеоспостереження й передачі даних – досить однієї.

Для японського виробника мережного встаткування система відеоспостереження відеоспостереження – особливий ринок. Компанія дуже багато інвестувала в розвиток цього напрямку й активно співробітничає з постачальниками відеокамер, зокрема Axis і Panasonic, здійснюючи, наприклад, спільне тестування для забезпечення найкращої передачі відео. Компанія пропонує рішення для побудови мереж різного масштабу – від невеликих на 10-20 камер і середніх на 50-200 камер до масштабних мультисервисних мереж, які звичайно

проектуються з перспективою розширення й збільшення кількості відеопристроїв з урахуванням потреб замовника. До кожної із цих топологій пред'являються свої технологічні вимоги, і кожна з них має унікальну архітектуру.

У невеликих мережах популярністю користуються недорогі, прості й функціональні рішення, які, будучи один раз настроєні, уже не вимагають уваги – «настроїв і забув». У відповідь на подібні запити система відеоспостереження пропонує реалізувати мережа на базі одного комутатора, до якого підключаються робочі місця й камери, – «рішення в одній коробці». Найчастіше як такий комутатор використовуються високопродуктивні пристрої серії AT-x930 і AT-x510 з підтримкою живлення по Ethernet (PoE+). Завдяки неблокуємій архітектурі комутаторів можна безболісно додавати камери й робочі місця без втрати в продуктивності й відмовостійкості. Більше того, на комутаторі реалізовані механізми контролю доступу, є убудований сервер RADIUS і підтримується потрійна автентифікація (802.1x, MAC, Web). Це дозволяє заощадити на придбанні окремого сервера безпеки. Якщо споконвічно в мережі були встановлені комутатори серії AT-x510 (комутатор другого рівня), при розширенні інфраструктури й необхідності формування ядра мережі їхня функціональність може бути розширена з L2 до L3 за рахунок додаткової програмної ліцензії.

Промислові комутатори система відеоспостереження IE3000 здатні забезпечити живлення підключених пристроїв потужністю до 60 Вт.

Масштабні мережі мають багаторівневу структуру. У мережі, де встановлено кілька десятків камер, уже є й рівень доступу, куди підключаються камери, і рівень агрегації, куди сходяться потоки, а далі виробляється запис на пристрої зберігання. Більші розподілені мережі споконвічно розраховані на масштабування – вони здатні підтримувати нелімітована кількість камер. Для забезпечення надійної роботи передбачається необхідний ступінь резервування й надмірності, при цьому камери можна підключати вживу – мережа буде зберігати працездатність. Подібні мережі застосовуються у великих проектах аж до таких, як «Безпечне місто».

Для побудови мережної інфраструктури системи відеоспостереження рекомендується використовувати гігабітні комутатори серії x510. При їхньому створенні за основу був узятий комутатор третього рівня старшого класу, з якого виключили функціональність динамічної маршрутизації, досить рідко використовувану в мережах відеоспостереження. Це дозволило здешевити пристрій, хоча воно підтримує такі необхідні функції, як живлення PoE+. Серед інших можливостей, затребуваних при побудові мереж відеоспостереження, – технології резервування й стекування, у тому числі віддаленого, коли комутатори можуть територіально перебувати в різних місцях, а управлятися як один пристрій.

Технологія Ethernet Protection Switched Ring (EPSRing) дозволяє відновити з'єднання у випадку розриву мережі за мінімальний час – менш чим за 50 мс. Ця затримка, якщо брати потік відео, непомітна людському оку. Раніше ця технологія була доступна на пристроях старшого класу (комутатори третього рівня) і використовувалася у великих проектах, таких як «Безпечне місто», а тепер вона підтримується й на бюджетних комутаторах L2 і тому зустрічається навіть у проектах організації відеоспостереження в торгових центрах. Інший спосіб забезпечення відмовостійкості мережі – застосування механізмів стекування.

Система відеоспостереження підтримує як локальний, так і віддалений стеки. У першому випадку два комутатори, що перебувають в одному місці, можуть бути об'єднані в стек спеціальним кабелем, при цьому навантаження розподіляється між ними динамічно. При виході одного з ладу другий відразу візьме навантаження на себе. Система відеоспостереження використовує підхід до стекуванню Active-Active, коли обоє пристрою постійно працюють, тому немає небезпеки, що при відмові одного із пристроїв інше не запуститься. При побудові кампусної мережі комутатори можуть бути об'єднані за допомогою механізмів віддаленого стекування через SFP-модулі. Керування комутаторами в стеці теж здійснюється як одним пристроєм.

Сучасну систему відеоспостереження неможливо представити без живлення по Ethernet (Power over Ethernet, PoE). Це дозволяє обійтися без ще однієї мережі – для забезпечення живлення камер. Як правило, для камер досить менш 30 Вт, тобто PoE+, але деяким потрібна потужність до 60 Вт. Не дуже давно система відеоспостереження випустила комутатори з підтримкою поки не стандартизованої технології High PoE. Це промислові комутатори серії AT-IE300, вони призначені для ситуацій, коли потрібно забезпечити віддалене живлення камер у складних умовах. «При виборі комутатора встає питання про сумарний бюджет PoE, від якого залежить максимальна кількість камер, що живляться. У цей час спостерігається тенденція оптимізації камер по споживанню живлення, тому, на наш погляд, що існують стандарти 802.3af і 802.3at, або PoE і PoE+, залишаться актуальними й достатніми».

Зберігання записів

Ще один наріжний камінь системи відеоспостереження – система для запису й зберігання даних. Перше ніж IP-камери одержали поширення, організація відеоспостереження припускала придбання й установку дорогих пристроїв DVR для запису відео, до яких камери підключалися прямо. З поширенням IP-камер на зміну цифровим відеорекордерам (Digital Video Recorder, DVR) прийшли мережні (Network Video Recorder, NVR). Однак проблема зберігання зроблених записів тільки збільшилася зі збільшенням доступності й затребуваності відповідних рішень.

У порівнянні з іншими типами дані обсяги відеоданих ростуть найбільше швидко. Згідно із прогнозами аналітичної компанії IHS, цього року камерами відеоспостереження буде згенеровано більше 6000 Пбайт даних, а до 2019 року сукупний щогодинний обсяг відеоспостереження складе 3,3 трлн годин. Крім того, строки зберігання відеозаписів усе більше подовжуються. Це зв'язано як з жорсткістю нормативного регулювання, так і з усе більше активним використанням записів не тільки для забезпечення безпеки, але й для аналітичних завдань, що стає причиною висування додаткових вимог до функціональності NVR.

У своїх проектах InPrice Distribution використовує рішення Synology, що з 2007 року пропонує рішення для зберігання відеозаписів. У той час камери були переважно аналоговими, але вже тоді Synology зуміла оцінити потенціал нового ринку, що дозволило цієї компанії рости разом з ним і вдосконалювати свої рішення. Всі випускаємі нею NAS поряд з функціями файлового сервера, принт-сервера, поштового сервера й інших можливостей підтримують і відеореєстратор – незалежно від моделі функціональність пристроїв однакова. Крім продуктів для SOHO і SMB, Synology пропонує рішення для корпоративного сегмента. Моделі серій XS і XS+ призначені для сегмента SME і здатні підтримувати запис із 70 і 100 камер відповідно. У них можна встановлювати диски ємністю до 10 Тбайт.

NAS мають можливість збільшення дискового простору за рахунок кошиків, що підключаються. У деяких випадках можливо більш ніж дворазове масштабування. Установивши необхідну кількість дисків, потім можна додавати й інші без зупинки робочих процесів. Максимальна можлива ємність зберігання, складова 1,8 Пбайт при установці 180 дисків по 10 Тбайт, досягається у випадку моделей RC18015xs+ (з 15 модулями розширення RXD1215sas) і RS1816xs+ (з 14 модулями розширення RX1216sas). При цьому є обмеження по тому й розділі: максимальний розмір одного тому – 200 Тбайт.

При використанні модулів розширення й дисків ємністю 10 Тбайт максимальна ємність зберігання Synology RackStation RC18015XS+ становить 1,8 Пбайт.

В Synology є й спеціалізована модель: NVR216 з підтримкою перегляду й запису відео від дев'яти IP-камер. Її основна відмінність – наявність можливості прямого підключення монітора/ТБ і керуючих периферійних пристроїв без використання ПК. Пристрій поставляється із чотирма безкоштовними ліцензіями й можливістю розширення їхнього числа до дев'яти камер. В NVR216 установлюються два HDD, при підключенні модуля

розширення DX513 їхнє число можна збільшити до семи. Таким чином, базова конфігурація оптимізована під потреби більшості малих і середніх офісів або крапок роздрібної торгівлі.

Убудовані функції Surveillance Station дозволяють заощадити дисковий простір при записі. Це можна зробити різними способами – наприклад, записувати відео тільки при детектуванні руху. У версії 8.0 додалася функція Advanced Continuous Recording: коли нічого не відбувається, запис ведеться в низькому розв'язній здатності, а при виявленні руху здійснюється перемикання на інший потік з більше високим дозволом. Як тільки дія закінчується, відбувається повернення до низького розв'язної здатності.

Підтримка багатоадресної передачі дозволяє знизити навантаження й на NAS, і на мережу. Трансляція відео декільком клієнтам в одному потоці дозволяє, наприклад, службі охорони переглядати відео в реальному часі одночасно з декількох місць. Для виводу зображення на екран можна скористатися терміналом VS360HD. Це вузькоспеціалізований пристрій для візуалізації зображення з камер без можливості нецільового використання (охоронцеві не вдасться пограти в комп'ютерні ігри). VS360HD оснащений потужним відеодекодером і може зчитувати «живий» відеопотік з Surveillance Station або прямо з камери й виводити його на пристрої HDMI.

За допомогою правил на Surveillance Station можна набудовувати різні варіанти подій і дій. При настанні таких подій, як виявлення руху, поява/зникнення об'єкта, розфокусування/загоражування камери й т.п., можуть ініціюватися пошук в архіві, запис зображення з камери (у тому числі з підвищенням розв'язної здатності), вивід окремої таблиці подій на монітор оператора, відправлення push-повідомлень і повідомлень по SMS і електронній пошті й т.д. Наприклад, якщо одна із установлених поворотних камер ламається, можна заздалегідь задати параметри другій камері, щоб вона змінила позицію й знімала заданий сектор постійно або за розкладом доти, поки перша не буде відновлена.

Якщо одна із установлених поворотних камер виходить із ладу, то можна заздалегідь задати параметри другої камери, щоб вона змінила позицію й знімала заданий сектор постійно або за заданим розкладом.

Для забезпечення гарантованої доступності Synology пропонує рішення Synology High Availability. Воно припускає використання двох ідентичних серверів NAS, які об'єднані в кластер (як тимчасова міра можлива підключення різних серверів). Один із серверів у кластері є активним, інший перебуває в резерві. Всі дані з дисків активного пристрою копіюються на другий сервер. У випадку відмови основного запасний берет на себе виконання його функцій. Однак, така конфігурація обходиться у два рази дорожче.

Нова версія програмного забезпечення підтримує конфігурацію з виділеними серверами (N+M): один (або декілька) перебуває в резерві, і після відмови запис із камер, які обслуговував сервер, що вийшов з ладу, триває на резервний. При відновленні дані переносяться назад. Один резервний сервер може бути з'єднаний з декількома основними, і навпаки – один основний з декількома резервними. Очевидно, у такій конфігурації архів записів на несправному сервері буде недоступний до його відновлення, зате нові записи не будуть загублені. Такий варіант резервування, природно, обходиться дешевше, ніж дублювання кожного NAS окремо.

Розгортання сотень IP-камер являє собою трудомістке завдання. Для проектів розподіленого відеоспостереження з декількома площадками Synology пропонує Synology Central Management System (CMS). Реалізація цього рішення припускає наявність виділеного головного сервера (host server), що здійснює контроль за всіма серверами запису на різних площадках. CMS дозволяє організувати відеоспостереження філій при їхньому з'єднанні, наприклад через Інтернет. Один хост-сервер здатний контролювати до 300 віддалених площадок і 5000 камер. Таким чином, із центрального офісу можна стежити за станом і переглядати архіви як локальних камер, так і віддалених – у філіях.

Висновок. У статті розглянуто та проаналізовано програмне забезпечення, створене в результаті виконання роботи, призначено для системи відеоспостереження для реалізації стратегії забезпечення безпеки підприємства. В межах України в недостатній мірі

представлені вітчизняні розробки в цій області. У роботі наведені теоретичне узагальнення й рішення наукового завдання дослідження методів відеоспостереження для реалізації стратегії забезпечення безпеки підприємства. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем відеоспостереження для реалізації стратегії забезпечення безпеки підприємства; Досліджена система відеоспостереження для реалізації стратегії забезпечення безпеки підприємства; На основі отриманих результатів досліджень створена програмна реалізація системи відеоспостереження для реалізації стратегії забезпечення безпеки підприємства. Розроблені під час виконання роботи алгоритми дозволяють успішно вирішувати завдання відеоспостереження для реалізації стратегії забезпечення безпеки підприємства. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки. Розроблене програмне забезпечення має простий, дружній та зручний інтерфейс користувача, що забезпечує легкість у освоєнні роботи програмного продукту, зручність у використанні, і не потребує особливих спеціальних знань. При створені програмного забезпечення було використано об’єктно-орієнтований підхід, що відповідає сучасним тенденціям у галузі розробки комерційних програмних систем. Програма реалізована на мові високого рівня Embarcadero Delphi 10. Дана мова програмування дозволяє найбільш ефективно обробляти дані. Це дозволило мінімізувати строк розробки програмного забезпечення, і, як слід, зменшити витрати на його розробку. Запропоноване програмне забезпечення ділиться на загальне програмне забезпечення, що поставляється із засобами обчислювальної техніки й спеціальне програмне забезпечення, що спеціально розроблене для даної конкретної системи й включає програми, що реалізують її функції. Програма призначена для виконання під управлінням багатозадачної операційної системи Windows XP/Vista/7/8/10. Даються необхідні рекомендації з установки розробленого програмного забезпечення. Для підвищення рівня безпеки запропоновано застосовувати алгоритм NTRU.

Список літератури

1. Дреев А.Н. Использование неравномерного распределения единичных битов для дополнительного сжатия SPIHT кода / А.Н. Дреев, А.А. Смирнов // Информационные системы в управлении, образовании, промышленности: монография. Под редакцией профессора В.С. Пономаренко. – Х.: Вид-во ТОВ «Щедра садиба плюс», 2014. – С. 498.
2. Дрєєв О.М. Дослідження впливу шляху розгортки на ступінь ентропійного стиснення цифрового зображення / О.М. Дрєєв, О.В. Слюсар // Збірник наукових праць Кіровоградського національного технічного університету. Техніка в сільськогосподарському виробництві, галузеве машинобудування, автоматизація. Випуск 21. – Кіровоград: КНТУ. – 2008 – С. 115-118.
3. Дрєєв О.М. Метод розвантаження телекомунікаційного сервера за рахунок кешування зображень / О.М. Дрєєв // Збірник наукових праць Кіровоградського національного технічного університету. Техніка в сільськогосподарському виробництві, галузеве машинобудування, автоматизація. Випуск 25. Ч. І. – Кіровоград: КНТУ. – 2012 – С. 419-424.
4. Дрєєв О.М. Метод прогнозування завантаженості серверу телекомунікаційної мережі / О.М. Дрєєв, О.А. Смірнов, Є.В. Мелешко, О.В. Коваленко // Системи обробки інформації. Випуск 3(101) Том 2. – Х.: ХУПС. – 2012. – С. 181-188.
5. Дрєєв О.М. Оцінка якості стиснення зображень на основі дискретного перетворення Хартлі / О.В. Коваленко, О.П. Доренський, О.М. Дрєєв // Системи озброєння і військова техніка. Науковий журнал 2(34) – Х.: ХУПС – 2013. С. 99-102.
6. Дрєєв О.М. Дослідження впливу ступеня стиснення зображень на оперативність їх доставки у телекомунікаційній системі / О.А. Смірнов, О.М. Дрєєв, О.П. Доренський // Збірник наукових праць "Системи обробки інформації". – Випуск 8(115). – Х.: ХУПС – 2013. – С. 234-239.
7. Дреев А.Н. Сравнение битовых плотностей при использовании различных методов кодирования информации / А.Н. Дреев, А.А. Смирнов // Системи обробки інформації, 2014, випуск 2 (118), том 2 – Харків: ХУПС – 2014. С 64-66.
8. Дрєєв О.М. Моделювання впливу інтенсивності трафіку на оперативність доставляння інформації / О.М. Дрєєв // Науково-виробничій журнал “Зв’язок”. – Київ: ДУТ, 2014. – № 2 (108) С. 24-29.

9. Дреев А.Н. Повышение вероятности доставки сообщений в телекоммуникационных системах и сетях для обеспечения информационной безопасности / А.Н. Дреев, А.А. Смирнов //«Безпека інформації» Том 21, №1 2015 р. – Київ: НАУ – 2015. – С. 22-28.
10. Дрєєв О.М. Узагальнення вейвлету Хаара / О.М. Дрєєв, Г.М. Дрєєва // Збірник тез доповідей Комбінаторні конфігурації та їх застосування, 15-16 жовтня 2010 р. – Кіровоград – С. 58

УДК 004

Л. Поліщук, магістр гр. КН-18МЗ
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ ХМАРНОГО СЕРВІСУ КЕРУВАННЯ ОБ'ЄКТАМИ ТЕХНОЛОГІЧНИХ ПРОЦЕСІВ

У статті розроблено програмне забезпечення, яке призначено для системи хмарного сервісу керування об'єктами технологічних процесів. Метою розробки є дослідження та програмна реалізація системи хмарного сервісу керування об'єктами технологічних процесів. Об'єктом дослідження є процес забезпечення системи хмарного сервісу керування об'єктами. Предметом дослідження є методи й алгоритми забезпечення системи хмарного сервісу керування об'єктами. Методи дослідження базуються на методах і алгоритмах побудови систем хмарного сервісу, методах теорії ймовірності, теорії масового обслуговування й імітаційного моделювання. Результат роботи – програмна реалізація системи хмарного сервісу керування об'єктами. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення. Розроблено зручний інтерфейс користувача. Наведені інструкції по роботі з програмними засобами.
комп'ютерні науки, системи хмарного сервісу

Постановка проблеми. За останні кілька років роль інформаційних систем (ІС) і технологій (ІТ) в вітчизняній та світовій промисловості істотно зросла. Впровадження ІС стало необхідною умовою підвищення мобільності, гнучкості та ефективності системи управління АСУТП і складними технічними системами. Підприємства, в яких формалізовані процеси для збирання інформації та її внутрішньому розподілу, можуть краще спрогнозувати динаміку ринкових тенденцій і діяти більш оперативно, більш впевнено і обґрунтовано приймати рішення. На сьогоднішній день ситуація на українському ринку така, що більшість підприємств, не залежно від розміру бізнесу, готові йти по шляху інновацій в сфері розвитку ІС і ІТ для оптимізації основних і допоміжних технологічних процесів.

Витрати на традиційні форми використання ІС і ІТ бувають значними. Сюди, як правило, включені витрати на оновлення основних модулів програмної оболонки, амортизація і ремонт обладнання, заробітна плата обслуговуючому персоналу, втрати при відмові інформаційної системи. Взагалі, при автоматизації будь –якої сфери діяльності частіше за все враховуються тільки явні витрати - на розробку і впровадження ІС, - і менше уваги приділяють наступним, прихованим витратам (експлуатаційні витрати). Витрати на експлуатацію ІС можуть досягати 70% від загальної вартості, тоді як витрати на створення і впровадження інформаційної системи в середньому складають близько 30%.

У зв'язку з цим запропонована альтернативна віртуальна форма ІТ інфраструктури, основу якої складають хмарні технології. Хмарні інформаційні технології являють собою модель повсюдного і зручного мережевого доступу до загального пулу конфігурації обчислювальних ресурсів (сервери, додатки мережі, системи зберігання та сервіси), які можуть бути швидко надані і звільнені з мінімальними зусиллями по управлінню.

Проведені дотепер дослідження створили міцну науково-методологічну базу для проектування структур управління промисловими й технологічними об'єктами. Однак

впровадження нових, усе більше досконалих технологій, ставить і ряд нових завдань, що вимагають свого рішення.

В останні кілька років у розвитку промислових мереж чітко виявилися наступні тенденції: відбулася відмова від традиційних схем побудови з вираженим ядром, у якому зосереджені основні обчислювальні потужності, а до виконавчого устаткування тягнеться безліч кабельних з'єднань. Такі рішення не задовольняють сучасним вимогам по масштабуванню мережі, надійності й відмовостійкості, забезпеченню безпеки, а саме головне – не гарантують виконання вимог за швидкодією для трафіку реального часу – передачі голосу, відео- і команд управління, обсяг якого постійно зростає; відбувся перехід до розподіленої обробки інформації з активним використанням промислових локальних мереж, що перепрограмовуються в процесі роботи мікроконтролерів, мікропроцесорів і інтелектуальних датчиків; для управління виробничими й технологічними процесами активно використовується мережа Internet, у тому числі й у режимі реального часу; для побудови центральної частини цифрових промислових систем (ЦПС) великих підприємств і складних технічних комплексів використовуються найсучасніші високошвидкісні канальні технології, такі як технологія синхронної цифрової ієрархії SDH/SONET, технологія ущільненого хвильового мультиплексування DWDM, технології 10 Gigabit Ethernet і Metro Ethernet. Для підвищення швидкості передачі маршрутизатори мережі Internet працюють по новій високошвидкісній технології MPLS; на середньому й нижчому рівнях ЦПС стали активно використовуватися хмарні технології; впровадження в ЦПС вищевказаних нових мережних технологій обумовило появу в мережі нових видів інформаційних потоків:

– інформації від відеокамер, призначених для спостереження за ходом випробувань складних виробів, за ходом технологічного процесу, переміщенням роботів і т.п.;

– передачі екстрених голосових повідомлень; передачі в реальному часі шифрованої мови й відео;

– відеокліпів, файлів великої довжини від цифрових фотоапаратів, програм оперативного перезавантаження флеш-пам'яті керуючого устаткування й т.д.;

– додаткове навантаження на мережу створюють розподілені по мережі компоненти інформаційного захисту, деякі з яких також генерують потоки реального часу, наприклад при передачі екстрених повідомлень про ознаки виявлення атак зловмисників; все більші масштаби приймає впровадження комплексних рішень великих фірм – системних інтеграторів, наприклад проект SCADA TRACE MODE 6. Системи такого роду характеризуються дуже великою функціональністю, інтегрують роботу всіх служб великого підприємства, а в методологічному плані вписуються в концепцію CALS-технології.

Впровадження цілого ряду технологічних новацій породило й цілий ряд проблем. Чисто механічне з'єднання різних мережних технологій може привести й до небажаних наслідків. Без більших витрат на впровадження нових технологій однаково не обійтися, але який при цьому буде досягнутий ефект, не завжди ясно.

Найбільш важкою проблемою є забезпечення в ЦПС суперечливих вимог до параметрів якості передачі інформаційних потоків з різною структурою. Передача даних характеризується великим ступенем пульсації трафіку, що неприпустимо для мови, аудіо- і відео- інформації, для яких установлені тверді обмеження на загальну затримку й варіацію величини інтервалів між пакетами. У той же час при передачі даних перекручування й втрати пакетів неприпустимі, а при передачі мови, аудіо- і відео- інформації невеликий відсоток втрат пакетів допускається. Інформаційні потоки не є постійними в часі. Тому комутація й маршрутизація таких потоків можлива тільки при виконанні попереднього дослідження їхньої структури в межах деякого інтервалу часу. Така процедура, обумовлена як профілювання трафіку, є необхідною для управління ресурсами мережі з метою досягнення встановлених показників якості її роботи.

Для досягнення необхідних показників якості потрібно оптимізувати структуру комп'ютерної мережі. Дане завдання є надзвичайно складним, оскільки на показники якості мережі впливають такі основні параметри протоколів передачі, як час доступу до загального

середовища передачі (для неперенавантаженої мережі), величина тайм-ауту непідтверджених пакетів, установлене значення максимальної довжини кадру в проміжній мережі MTU, частка службової інформації в пакеті, час життя пакета TTL і т.д. Якщо ці величини брати як варіації змінних, то завдання оптимізації мережі стає чисто комбінаторним з експонентним часом рішення. Спроба вирішити його шляхом натурального моделювання, приречена на невдачу, тому що зміна тільки одного з параметрів вимагає перезавантаження комп'ютера. Параметрами цільової функції є основні показники якості для найбільш важливих застосунків, наприклад, середній час затримки при передачі пакетів і її варіація, середнє значення й варіація інтервалів між пакетами й т.д.

Найпростіший, і самий дорогий, шлях рішення цих проблем – це пряме збільшення продуктивності каналів зв'язку й комутаційного устаткування. Однак в умовах твердої конкуренції на ринку мало хто з мережних інтеграторів іде цим шляхом. До останнього часу використовувалися переважно дві стратегії управління потоками в мережі DiffServ і IntServ. Перша з них забезпечує: профілювання трафіку (поділ потоків трафіку на класи) по алгоритму "дірявого відра", його синхронізацію по алгоритмах типу "відро токенів", що зменшує величину черг у комутаторах і маршрутизаторах, а також різні способи пріоритетної обробки в проміжних комутаційних пристроях. Показники якості мережі забезпечуються "по можливості", але не гарантуються. Однак перевагою стратегії DiffServ є те, що вона простіше реалізується на практиці. Стратегія IntServ передбачає гарантоване забезпечення смуги пропущення багатьох користувачів, зокрема гарантованої середньої швидкості передачі, передачі пульсацій трафіку протягом погодженого, щодо невеликого інтервалу часу. При цьому виконуються й інші показники якості, такі, як вимоги до затримок окремих пакетів, вірогідності передачі, часу включення резервного устаткування й т.д. Реалізувати таку стратегію на практиці дуже складно.

Останнім часом рішення проблем забезпечення показників якості в мережах реального часу намітилося в рамках високошвидкісної технології комутації міток MPLS. Ця технологія повинна поєднати переваги мережі Internet з розвиненими можливостями її застосунків, таких, як Web-, електронна пошта й широкі можливості масштабування, і переваги мереж з віртуальними каналами, таких як frame relay і ATM з їхньою високою швидкістю передачі й захищеністю. Мережі такого роду повинні забезпечувати резервування смуги пропущення, інжиніринг трафіку, що забезпечує паралельну й збалансовану передачу трафіку через маршрутизатори MPLS по багатьом шляхам, і, в остаточному підсумку – рішення завдання оптимізації мережі, з урахуванням варіювання параметрів протоколів в окремих ланках мережі. Рішення цієї проблеми покладається на розташовані поза мережею автоматизовані комплекси, що мають у своєму складі засоби імітаційного моделювання.

Навіть короткий аналіз особливостей передачі в ЦПС трафіку й попереднього розгляду показників якості говорить про те, що в цих мережах виникають такі ж проблеми оптимізації, що й у мережах MPLS і Metro Ethernet. Більше того, окремі сегменти, як MPLS, так і Metro Ethernet можуть використовуватися в центральній частині ЦПС.

Можна констатувати той факт, що технологічний ривок в області створення нового покоління ЦПС відбувся, але адекватні йому засоби моделювання й оптимізації ЦПС ще не створені. Тому завдання розробки спеціалізованого математичного забезпечення, методів і інструментальних засобів моделювання й оптимізації цифрових промислових мереж, поставлене в даній магістерській роботі, є досить актуальним.

В останні роки системи хмарного сервісу зайняли міцні позиції в повсякденному житті. Згідно з документом IEEE, опублікованим у 2008 році, «Хмарні обчислення — це парадигма, в рамках якої інформація постійно зберігається на серверах у мережі інтернет і тимчасово кешується на клієнтській стороні, наприклад на персональних комп'ютерах, ігрових приставках, ноутбуках, смартфонах тощо». Активний ріст числа хмарних технологій висуває в ряд першочергових завдань розробку методів оптимізації їхньої роботи, розробку нових алгоритмів функціонування таких мереж, а також оцінку їхньої продуктивності. Проблемам розробки математичних моделей мереж передачі даних присвячена значна

кількість робіт. Особливості хмарних сервісів при оцінці їхньої продуктивності досить повно відбиті в ряді робіт, однак недоліками цих робіт є, слабка увага, що приділяється механізмам адаптивного централізованого управління, хоча саме ці механізми націлені на рішення основної проблеми промислових мереж – проблеми „прихованих станцій". Таким чином, завдання аналізу, розробки й оптимізації механізмів адаптивного динамічного управління є однієї з найважливіших для розвитку промислових мереж передачі даних. Крім цього, потрібно розробити комплекс аналітичних і імітаційних моделей механізмів централізованого управління для одержання адекватних оцінок показників продуктивності й оптимізації пристроїв промислової мережі.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи хмарного сервісу керування об’єктами технологічних процесів.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи хмарного сервісу керування об’єктами технологічних процесів.

Для досягнення цієї мети необхідно вирішити наступні проблеми:

– виконати аналіз функціонального наповнення й структури цифрової промислової мережі, і оцінити характер переданого в ній трафіку;

– розробити методи поліпшення синхронізації процесу передачі пакетів при використанні хмарних сервісів передачі даних;

– розробити загальні підходи до оптимізації трафіку реального часу, критичного до затримок;

– знайти процедури проведення процесу оптимізації протоколів, алгоритмів і програм цифрової промислової мережі при заданих часових обмеженнях на час оптимізації;

– розробити методи забезпечення необхідних ймовірносно-часових характеристик передачі інформації, критичної до затримок, при впливі перешкод у цифровій промисловій мережі;

– виконати експериментальну перевірку розроблених методів і алгоритмів у реальних умовах.

Завдання досліджень. Для досягнення цілей магістерської роботи необхідне рішення наступних завдань:

1. Визначення загальних підходів і розробки методик параметричної оптимізації алгоритмів і програм цифрових промислових мереж при передачі трафіку реального часу. Це дозволяє підвищити показники якості телекомунікацій і зменшити матеріальні витрати на мережне устаткування.

2. Розробки методів забезпечення синхронізації переданих потоків реального часу, що дозволяє зменшити випадкове розкидання інтервалів між пакетами при передачі з використанням хмарних сервісів, що, в остаточному підсумку, приводить до підвищення якості передачі інформації.

3. Розробки методів підвищення надійності при забезпеченні ймовірнісно-часових характеристик алгоритмів і програм передачі інформації за рахунок введення контрольних точок.

4. Проведення експериментів на реальних системах для перевірки коректності розроблених теоретичних положень, методів і рекомендацій.

Об'єктом дослідження є процес забезпечення системи хмарного сервісу керування об’єктами.

Предмет дослідження – методи й алгоритми забезпечення системи хмарного сервісу керування об’єктами.

Виклад основного матеріалу. Промислові хмарні платформи

Шляхи інтеграції компонентів систем управління з хмарними платформами передусім залежать від вибору платформи, служб, які вона надає і відповідно протоколів, які підтримуються цими службами. Серед передових гравців на ринку хмарних платформ, які займаються просуванням Інтернету речей та пропонують відповідні продукти слід виділити

наступні: Amazon Web Service, Microsoft Azure та Google Cloud Platform. Названі хмарні платформи належать до публічних і швидко розвиваються у напрямку Інтернету речей. З огляду на це, кожен з вище згаданих, надає засоби для реалізації та впровадження Інтернету речей, в тому числі і промислового Інтернету речей, який є невід'ємною частиною розвитку Індустрії 4.0. Amazon Web Service пропонує комплексне рішення для реалізації Інтернету речей, а саме AWS IoT Core – це керована хмарна платформа, яка дозволяє підключеним пристроям просто і безпечно взаємодіяти з хмарними додатками та іншими пристроями. Крім того, що хмарні сервіси надають значний функціонал для об'єднання пристроїв в загальну мережу та віддалене управління ними, важливим фактором для інтеграції з виробничим обладнанням та програмним забезпеченням є підтримуванні цими службами протоколи. AWS IoT Core підтримує протоколи HTTP, WebSockets і спрощений протокол зв'язку MQTT, спеціально спроектований для підтримки нестабільного підключення і роботи в мережах з низькою пропускною здатністю. Microsoft Azure в свою чергу пропонує комплексне рішення для Інтернету речей Azure IoT Suite. Компонент цього рішення буде розглянуто більш детально нижче. Рішенням від Google Cloud Platform виступає Google Cloud Web of Things (IoT) Core – це повністю керована служба для безпечного підключення та керування пристроями IoT.

Вище згадані платформи відносяться до споживчих хмарних платформ. Існують також промислові хмарні платформи, які набагато глибше фокусуються на операційних технологіях (OT) – технологіях автоматизації промислових процесів та виробництв. Вони розроблені таким чином, щоб забезпечувати збір та обробку даних під час функціонування виробничих процесів з метою підвищення продуктивності а також прогнозуючого обслуговування. Серед них GE Predix від General Electric та MindSphere від Siemens AD. Ці рішення є комерційними, мають чітке промислове спрямування, простіші з точки зору використання, але можуть виявитися більш дорожчими, ніж звичайні споживчі хмарні платформи. Крім того, враховуючи, що більш застосовані споживчі платформи вже надають ресурси для реалізації промислових рішень, їх використання може бути більш доречним. Зокрема MS Azure вже надає можливість реалізації рішень націлених на виробництво. Слід відмітити, що індустріальну платформу GE Predix теж можна розгорнути в інфраструктурі Azure і наразі Microsoft та General Electric ведуть переговори щодо співпраці, яка в майбутньому дасть змогу додаткам розгорнутим засобами MS Azure обмінюватися даними з Predix.

MS Azure вже зараз надає ресурси для реалізації промислового Інтернету речей та має дуже розвинену інфраструктуру. Крім того MS Azure підтримує технологію OPC UA, яка знаходиться на етапі становлення як передового стандарту для інтеграції промислового обладнання в єдину мережу. Слід зазначити що Microsoft тісно співробітничає з компаніями в світі промислової автоматизації. Крім GE, MS співпрацює з COPA-DATA, яка займає передові місця в сфері розробки програмного забезпечення HMI/SCADA. Це спонукало до зосередження деталізації в дослідженні на інтеграції існуючих АСУТП з хмарними сервісами саме Microsoft Azure.

Значна кількість виробників апаратних та програмних засобів для АСУТП на хвилі розвитку застосування промислового Інтернету речей, мають намір залишатися конкурентоспроможними та не втрачати позиції на ринку. На етапі цифрової революції неможливо уникнути об'єднання операційних та інформаційних технологій, тому для передових розробників технічного та програмного забезпечення, яке застосовується в операційних технологіях, важливо швидко адаптуватися до змін в промисловому світі. Наразі розглядаються нові інструменти в SCADA-програмах, які дозволяють інтеграцію з хмарними сервісами, для того щоб забезпечувати віддалений моніторинг процесу, менеджмент активів, предиктивне обслуговування, аналіз історичних даних. Як приклад, COPA-DATA для своєї SCADA zenon пропонує використання сервісів MS Azure для розгортання мобільних застосунків HMI клієнтів та веб-сайтів для віддаленого моніторингу. Крім того в хмарі можна розмістити інструментальний засіб для побудови звітів zenon

Analyzer, що забезпечить скорочення локальних обчислювальних ресурсів та відкриту можливість доступу до звітів усім стейкхолдерам. Таке рішення вимагає самостійного використання платформи MS Azure як системи типу PaaS. Schneider Electric пропонує своє рішення для збору, візуалізації та аналізу промислових даних, яке представляє собою систему типу SaaS, побудовану засобами MS Azure. Це рішення – Wonderware Online InSight, яке дозволяє інтегруватися з такими продуктами як Wonderware InTouch HMI, Wonderware System Platform, Wonderware Historian.

Однак не всі SCADA-програми мають вбудовані засоби інтеграції з хмарними платформами. Крім того, наявність великої кількості проваджень потребують інших технологій інтеграцій. Тому в дослідженні нас цікавили технології, які б надавали можливість об’єднати більшість рішень з хмарними платформами.

Найбільш сучасною інтеграційною технологією в промисловій автоматизації є OPC UA, яка крім того є базовою комунікаційною технологією Індустрії 4.0. Не зважаючи на те, що OPC UA є наступницею OPC Classic, вона є крос-платформною і більше не застосовує технологію DCOM. OPC UA заснований на архітектурі SOA, яка об'єднує всі функціональні можливості окремих специфікацій OPC Classic в одну розширювану структуру. До недавнього часу існували обмежені можливості для інтеграції OPC UA з MS Azure. Зараз вже існує кілька можливих варіантів підключення OPC UA та MS Azure через програмний шлюз. Запуск програмних шлюзів можливий на різноманітних операційних системах та апаратних пристроях, включаючи віртуальні машини у хмарах. З боку MS Azure рекомендується використовувати такі служби: IoT Hub, Event Hubs, Azure Service Bus. Вони підтримують протоколи AMQP 1.0, MQTT 3.11 і HTTP і побудовані для отримання даних у великій кількості. IoT Hub, крім того, забезпечує управління пристроєм та двостороннє спілкування.

Розглянемо деякі пропозиції щодо інтеграції OPC UA з MS Azure.

Першим можливим варіантом реалізації передачі даних в хмарну платформу MS Azure зі SCADA-програми або PLC, які підтримують OPC UA, є розробка власного програмного шлюзу. Написання власного шлюзу OPC UA є відносно нескладною задачею завдяки відкритій версії OPC UA.NET Standard library та прикладам, що надає OPC Foundation. Крім того є відкриті бібліотеки AMQP для багатьох мов програмування. Тим не менше це вимагає від інтегратора наявність програмістів з відповідними компетенціями в об’єктно-орієнтованому програмуванні.

Другим варіантом реалізації шлюзу є використання Azure IoT Edge Gateway [1]. Azure IoT Edge Gateway є крос-платформним і використовує модульну архітектуру. У відкритому доступі знаходять різноманітні модулі, в тому числі OPC UA Publisher. Перевага підходу Azure IoT Edge Gateway полягає в тому, що при цьому використовується проект із відкритим кодом, який підтримують (включаючи Microsoft) та застосовують інші користувачі, а також даний підхід реалізує масштабовану, розширювану крос-платформну архітектуру.

Приклад реалізації даного підходу інтеграції наведений на рисунку 1. В даному варіанті розглядається взаємозв’язок між компонентами системи, а саме SCADA-програмою та службою MS Azure IoT Hub. SCADA-програма має інтегрований OPC UA сервер, служба IoT Hub зберігає та оброблює дані від різних пристроїв, забезпечує підтримку протоколів AMQP 1.0, MQTT 3.11 і HTTP поверх TLS (протокол з шифруванням), а також надає різні можливості для оперування отриманими даними (проведення аналітики) та їх подальшого використання іншими службами, наприклад, розгортання OPC UA клієнтів в хмарі. Такий взаємозв’язок реалізується за допомогою встановлення програмного пакету Azure IoT Edge Gateway з боку функціонування SCADA-програми. Так як шлюз має модульну структуру, то для встановлення зв’язку шлюзу з OPC UA сервером необхідно в його програмний код включити модуль OPC UA Publisher, який функціонує на базі стеку OPC UA.NET Standard library. Azure IoT Edge Gateway вже включає бібліотеки AMQP 1.0, MQTT 3.11 і HTTP, тому передача даних реалізовується за допомогою цих протоколів.

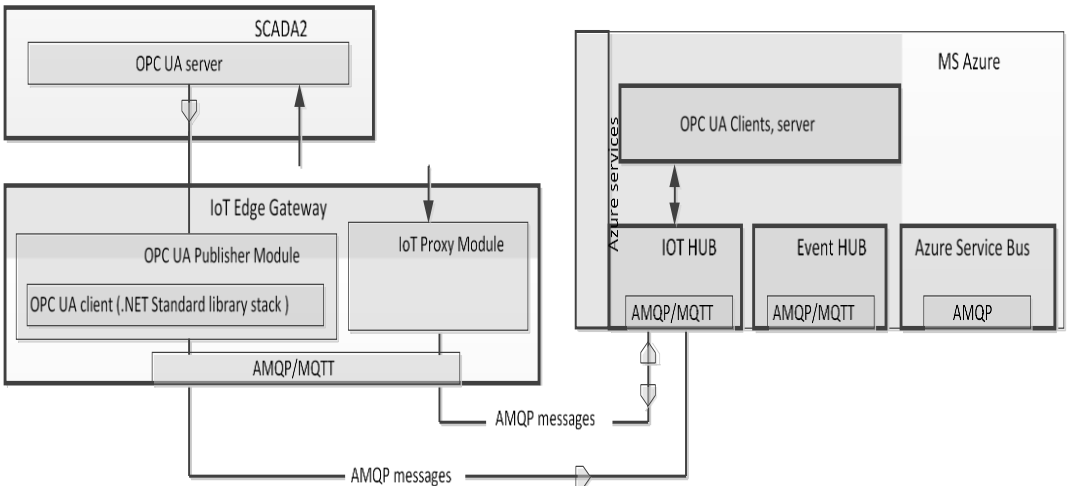


Рисунок 1 – Взаємозв'язок між компонентами SCADA-програми та службою MS Azure IoT Hub

Також замість модуля OPC UA Publisher можна використовувати модуль Azure IoT Edge OPC Reverse Proxy для реалізації двостороннього зв'язку. Якщо програмні засоби (SCADA) або пристрої не підтримують OPC UA можна використовувати готові програмні шлюзи OPC DA/UA. Наприклад, UaGateway Wrapper & Proxy v1.4.6 дозволяє підключати будь які COM/DCOM клієнти до UA серверів, або навпаки - UA клієнтів до COM/DCOM серверів всіх класичних специфікацій. UAGateway є додатком, що працює в операційній системі Windows (XP, Vista, Win7). Незабаром очікується версія, що буде підтримувати протоколи AMQP і MQTT. Це дозволить публікувати дані OPC UA та класичних OPC в хмарні сервіси та різноманітні IoT платформи. Альтернативою відкритим програмним шлюзам є комерційні шлюзи з закритою архітектурою (чорна скринька), де постачальник сам реалізовує і підтримує шлюзування між SCADA-програмою та службою MS Azure. Основна перевага використання комерційних шлюзів – це їх підтримка постачальниками.

Поряд з OPC SCADA-програми тим чи іншим способом обслуговуються відкритими технологіями ODBC, OLEDB та ADO.NET для обміну з СУБД. Механізми передачі даних зі SCADA-програм в локальні бази даних SQL зокрема через MS SQL Server є достатньо відпрацьованими. У цьому випадку задача інтеграції зводиться до переміщення даних з локальної бази даних MS SQL у базу даних SQL Azure. Існує рішення, яке дозволяє зв'язувати дані між локальним сервером MS SQL та базою даних SQL Azure шляхом їх синхронізації. Засіб управління, що надається для синхронізації даних Microsoft SQL Data Sync Agent, передбачає вибір бази даних і таблиці, які необхідно синхронізувати, а потім створює завдання служби агента SQL Server для автоматичної синхронізації даних з SQL Azure за розкладом. При цьому максимальна частота синхронізації може досягати 5 хвилин. Ця технологія дозволяє розширити існуючу локальну інфраструктуру для роботи в хмарі. Завдяки зв'язуванню локальних даних з хмарною інфраструктурою можна легко налаштувати обмін інформацією з мобільними користувачами, віддаленими джерелами даних, при цьому використовуючи переваги нових служб в хмарі. Ця технологія також створює міст, який забезпечує взаємодію між локальними і віддаленими програмами.

Вище були представлені шляхи інтеграції SCADA-програм з хмарною платформою MS Azure, проте впровадження підходів Індустрії 4.0 передбачає участь всіх активів в єдиній загальній мережі. Активними учасниками процесу управління в АСУТП є програмований логічний контролер (ПЛК), який може підтримувати різноманітні промислові протоколи, такі як Profibus, EtherCAT, Modbus, EtherNet/IP, CAN, CANopen і т.п. Для встановлення зв'язку з хмарною платформою такою як MS Azure, яка підтримує AMQP, MQTT та HTTPS, необхідно використовувати проміжний пристрій – апаратний шлюз – який налаштує зв'язок, представлення та передачу даних між різними кінцевими вузлами. Використання програмних

шлюзів значно спрощує інтеграцію будь яких пристроїв з хмарою та мінімізує затрати часу на написання додаткового коду. Тому виникає необхідність в правильному підборі обладнання. В якості апаратного шлюзу, як готового рішення можна використовувати продукти, які пропонує Microsoft, Advantech або Intel.

Протоколи AMQP, MQTT підтримуються хмарною платформою MS Azure та багатьма іншими. Протокол MQTT (Message Queuing Telemetry Transport) – це простий відкритий протокол, який розроблений для обміну типу «машина-машина», тому його обчислювальні вимоги є мінімальними. Крім використання апаратних шлюзів, програмовані логічні контролери можливо інтегрувати з хмарними сервісами, реалізувавши протокол MQTT безпосередньо в контролері. Для цього необхідно написати, наприклад, функціональні блоки, в яких реалізуються методи протоколу, такі як: Connect, Disconnect, Publish, Subscribe, Unsubscribe. Бібліотека таких блоків вже є реалізованою та знаходиться у відкритому доступі для ряду контролерів, наприклад, Siemens S7-300/S7-400 в середовищі програмування Step7. Маючи відкритий код неважко перенести його на інші платформи, що мають відкритий стек TCP/IP, наприклад з підтримкою CoDeSys.

Враховуючи, що OPC UA набирає обертів як передовий стандарт IIoT комунікації, його все більше впроваджують на рівні контролерів. Велика кількість виробників, наприклад, ABB, Bosch Rexroth, B&R, CISCO, General Electric, KUKA, National Instruments (NI), Parker Hannifin, Schneider Electric, SEW-EURODRIVE та TTTech оголосили про співпрацю під егідою IIC та OPC Foundation. Ці компанії прагнуть до відкритої, уніфікованої, заснованої на стандартах комунікації в режимі реального часу між промисловими контролерами і хмарою. Вони приймають стандарт OPC UA як єдиний для промислової автоматизації та зв'язку IIoT. На сьогоднішній день вже в багатьох контролерах інтегровано OPC UA server: Siemens S7-1500, Modicon M241 та M251 від Schneider Electric, PACSystems RX3i 320 CPU від General Electric та інші. У якості шлюзу до MS Azure може використовуватись програмно-апаратний засіб, зроблений наприклад на Raspberry Pi.

В якості ще одного інструменту інтеграції PLC та MS Azure можна використовувати інструмент потокового програмування – Node-RED. Він надається редактором налаштування потоків, який працює на основі браузера та дозволяє зручним способом зв'язати пристрої, які мають різні комунікаційні можливості, між собою. Node-RED побудований на легкій та ефективній програмній платформі Node.js, що дозволяє використання Node-RED як на недорогих апаратних пристроях таких як Raspberry Pi, так і в хмарі. В бібліотеці на сайті Node-RED можна знайти різні «nodes», за рахунок яких можна забезпечити встановлення зв'язку між пристроями, що використовують різні протоколи.

Розробка структурної схеми

Завдяки хмарним технологіям дані з різноманітних систем або окремих пристроїв доступні всім зацікавленим особам (стейкхолдерам). Збір максимального обсягу інформації та можливість своєчасно оперувати нею є важливим критерієм побудови сучасних автоматизованих системах управління технологічними процесами (АСУ ТП).

Під автоматизацією промисловості розуміють заміну ручної праці машинною, будь то роботи, автоматичні прилади або програмне забезпечення. Автоматизація полягають в тому, що на лінії виробництва робочий процес і деякі його компоненти (операції) виконуються не людьми, а спецтехнікою або інформаційними системами. Вже сьогодні автоматизоване виробництво може повністю замінити людину на багатьох видах робіт і це доведено системою MES.

Підвищення продуктивності і бажання отримати конкурентну перевагу, як правило, є основною причиною для старту проекту по автоматизації на багатьох підприємствах. Інші причини автоматизації можуть бути обумовлені не «надіями на майбутнє», а наявністю конкретних причин - наприклад, небезпечним робочим середовищем або високою вартістю людської праці. Деякі підприємства автоматизують процеси з метою скоротити час виробництва, збільшити гнучкість виробництва, скоротити витрати, усунути людські помилки або заповнити нестачу робочої сили.

Автоматизована система управління технологічними процесами (АСУ ТП) являє собою комплекс засобів технічного, інформаційного, математичного і програмного забезпечення для управління технологічними об’єктами, який забезпечує оптимальний при заданій структурі і технічних засобах рівень автоматизації збору й переробки інформації для формування управляючих сигналів і передачі їх без збитків й викривлення на виконавчі механізми з метою досягнення ефективної роботи технологічного об’єкта управління в цілому.

Процес створення конкретних АСУ ТП починається зі складання технічного завдання, де визначаються:

– призначення й мета створення системи;

– характеристики об'єкта автоматизації;

– вимоги до системи;

– склад і зміст робіт зі створення АСУ ТП;

– вимоги до документування й ін.

При створенні системи визначається структурна схема АСУ ТП, проводиться вибір технічних засобів: сервера(ів), АРМа (ів), контролера (ів), а також програмного забезпечення.

У даній магістерській роботі розроблено й впроваджено високотехнологічну систему АСУ ТП, починаючи з автоматизації керування окремими процесами на підприємстві і виробництві, аж до створення системи комплексної автоматизації.

АСУ ТП – автоматизована система управління технологічними процесами, яка має 2 або 3 рівні, виконує наступні функції:

– збір інформації;

– підтримка технологічних параметрів на заданих значеннях;

– контроль за технологічними параметрами, для яких не виконуються функції регулювання;

– сигналізація;

– блокування управлінь, які є результатом помилкових дій технологічного персоналу;

– протиаварійний захист при виникненні аварійних ситуацій.

Структурна схема розробленої системи зображена на рисунку .2. На ній показано структуру автоматизованої системи управління технологічним процесом з використанням системи хмарного сервісу.

Перший (нижній) рівень АСУ ТП є рівнем датчиків, виконавчих механізмів і контролерів, які встановлюються безпосередньо на технологічних об’єктах. Їхня діяльність полягає в отриманні параметрів процесу, перетворенні їх у відповідний вигляд для подальшої передачі на вищий ступінь (функції датчиків), а також у прийомі управляючих сигналів і у виконанні відповідних дій (функції виконавчих механізмів).

Задачами рівня є:

– збір інформації про вимірювані технологічні параметри процесу;

– випрацювання управляючих дій на технологічний процес з метою підтримки технологічних параметрів на заданих значеннях або зміни їх до певних законів;

– сигналізація про вихід їх за задані межі;

– блокування помилкових дій персоналу і управляючих пристроїв;

– протиаварійний захист процесу за фактом аварійних подій.

Підсистеми цього рівня підтримують параметри технологічного процесу на заданих значеннях і можуть бути реалізовані з використанням «традиційних» методів регулювання динамічними об’єктами.

Другий (середній) рівень – рівень виробничої ділянки (цеху). Його функції:

– збір інформації, що надходить з нижнього рівня, її обробка і зберігання;

– випрацювання управляючих сигналів на основі аналізу інформації;

– передача інформації про виробничу ділянку на вищий рівень;

– обчислення параметрів, що не вимірюються, зокрема, показників якості продукції, техніко-економічних показників;
– зведення матеріальних балансів;
– архівування інформації;
– генерація звітів;
– діагностика і захист від збоїв в елементах підсистем нижнього рівня;
– визначення налаштувань управляючих пристроїв і уставок локальних регуляторів підсистем І рівня;
– зміна структури локальних підсистем (переконфігурація, включення/виключення, перехід у ручне управління).

На даному рівні проводиться оптимізація технологічних процесів за технологічними показниками.

Третій (верхній) рівень у системі автоматизації займає так званий рівень управління і відноситься до системи управління підприємством (АСУП). На цьому рівні здійснюється контроль за виробництвом продукції, оптимізація за техніко-економічними і економічними показниками. Цей процес включає збір даних, що надходять з виробничих ділянок, їх накопичення, обробку й видачу управляючих директив нижнім ступеням.

Завдання управління даного рівня:

– оптимізація економічних показників виробництва;

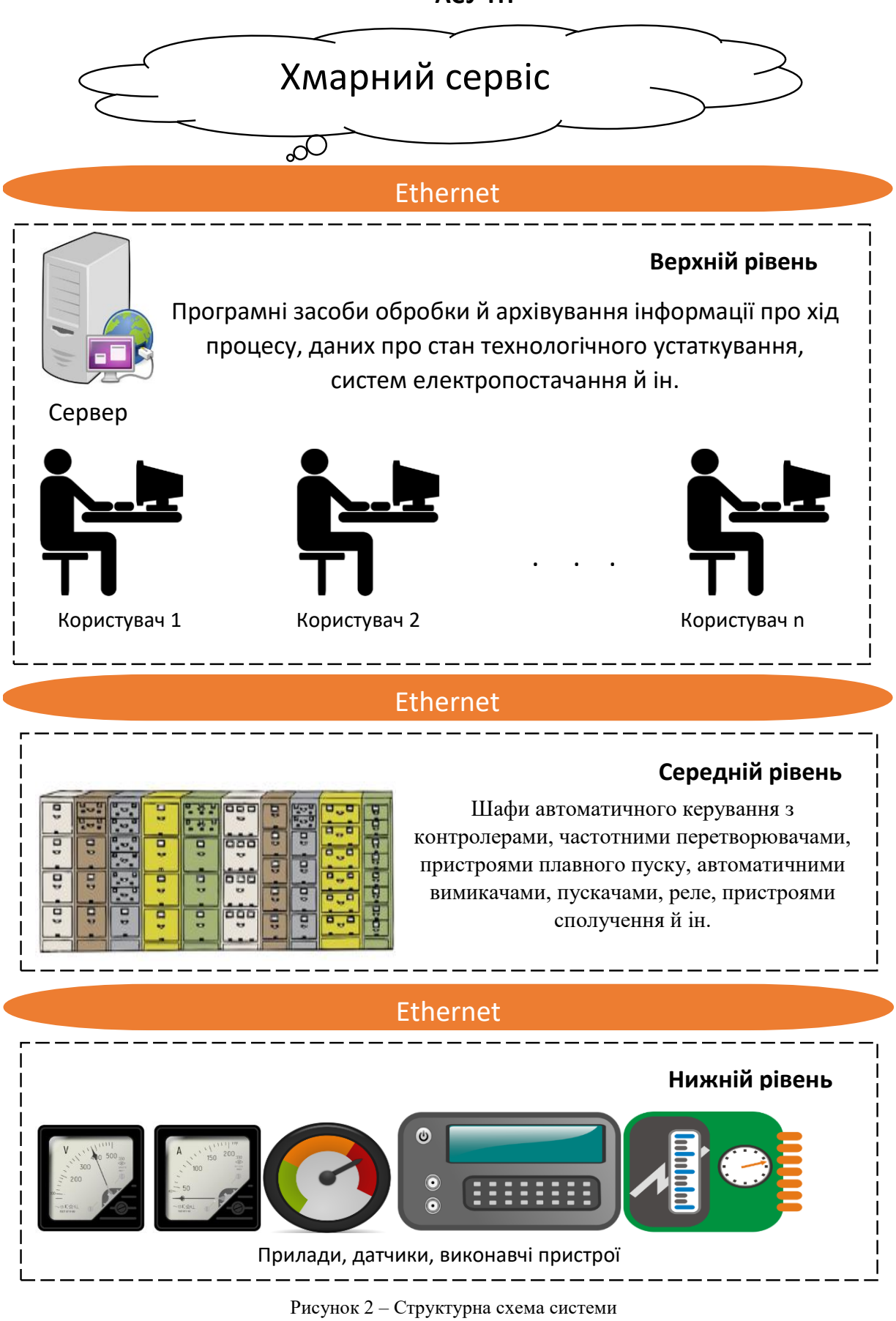


Рисунок 2 – Структурна схема системи

– управління економічними і техніко-економічними показниками;

– зведення матеріальних балансів;
– архівування інформації;
– складання виробничих планів і так далі.

Слід зазначити, що деякі завдання другого і третього рівнів перекриваються та в ряді випадків ці два рівні об’єднуються в один.

Розроблена, під час виконання магістерської роботи, АСУ ТП забезпечує:

– роботу в реальному часі;
– у темпі з технологічним або виробничим процесом;
– наявність автоматичної системи збору і передачі інформації;
– відсутність громіздкого документообігу, властивого АСУП;
– значну складність задач алгоритмічного і програмного забезпечення,
– наявність ряду операцій централізованого контролю й обробки інформації;
– певну локальність і стабільність задачі управління об’єктом.

Для інформаційного зв'язку всіх підсистем використовуються промислові мережі.

При побудові АСУТП використовується ієрархічна інформаційна структура з застосуванням на різних рівнях обчислювальних засобів різної потужності.

На самому нижньому рівні датчики, виконавчі пристрої та модулі розподіленого введення/виведення встановлюються безпосередньо на технологічних об'єктах.

На середньому рівні використовуються контролери з операційними системами реального часу для збирання і обробки інформації з об'єктів нижнього рівня та подачею управляючих сигналів. Інформація з контролерів прямує в мережу диспетчерського пункту.

На верхньому рівні АСУТП розміщені потужні комп'ютери, що виконують функції серверів баз даних і робочих станцій та забезпечують аналіз і зберігання всієї інформації, що надійшла за певний заданий інтервал часу. Також візуалізацію інформації, та організацію потоку даних і документації між відділом управління і виробничими одиницями.

При реалізації інформаційних АСУТП використовується архітектура «клієнт-сервер». Так звана головна станція, що служить сервером, виконує функції зберігання архівних даних. Ця станція - найпотужніша в контурі АСУТП, що реалізує основний обсяг роботи. Інші станції «клієнти» в контурі АСУТП здійснюють візуалізацію технологічного процесу, збір даних з контролерів, первинну обробку вхідних сигналів.

Централізоване зберігання отриманих даних здійснюється в базах даних під управлінням «MS SQL Server». Крім того, на сервері зберігаються конфігураційні файли, що описують архітектуру АСУТП, встановлені програми, що забезпечують роботу за конфігурацією АСУТП.

Вихід з ладу головної станції за відсутності її дублювання призводить як мінімум до деградації системи. Дублювання ж головної станції вимагає великих матеріальних витрат на додаткове обладнання і програмне забезпечення. Дублювання станцій-клієнтів вимагає значно менших витрат через обмеженість вимог до комп'ютерів і ПЗ. Для контролю технологічного процесу оперативний персонал реалізує функції візуалізації поточного стану технологічного обладнання, технологічної сигналізації та реєстрації аварійних подій, які реалізовані на станціях-клієнтах і працюють при відмові станції сервера. Необхідно також забезпечити збереження архівних даних на період відмови головної станції.

Станції візуалізації в контурі типової конфігурації дубльовані. Для підвищення надійності системи в частині оперативного контролю дублюються станції збору даних.

Надійність верхнього рівня типової конфігурації АСУТП і конфігурація з дубльованими станціями збору даних та модифікованим програмним забезпеченням реалізує функціонування оперативних завдань АСУТП при відмові головною станції,

АСУТП використовує TRACE MODE6 програмну шину і механізм збереження архівних даних. Для передачі вхідних даних в АСУТП використовується нецентралізована шина. Всі станції в мережі рівнозначні. Тому вихід з ладу сервера не впливає на передачу даних між станціями збору даних і станціями візуалізації.

Для збереження архівних даних на час відмови сервера в АСУТП, реалізована «тимчасова історія», тобто на час відмови головної станції накопичення отриманих даних проводиться в кільцевому буфері на станції збору даних. Кільцевий буфер забезпечує збереження отриманих даних на максимальний час для відновлення сервера. При відновленні працездатності головної станції дані з кільцевого буфера переносяться в базу даних історії. Цим забезпечується цілісність архівних даних.

Висновок. У статті розглянуто та проаналізовано програмне забезпечення, яке призначено для реалізації програмного забезпечення системи хмарного сервісу керування об'єктами технологічних процесів. В межах України в недостатній мірі представлені вітчизняні розробки в цій області. У роботі розроблені механізми адаптивного динамічного централізованого управління в широкосмугових цифрових промислових мережах передачі інформації, а також проведене дослідження й оптимізація цих механізмів за допомогою комплексу аналітичних і імітаційних моделей. Зокрема: 1. Сформульовано принципи побудови й особливості широкосмугових цифрових промислових мереж; 2. Розроблено нові механізми адаптивного централізованого управління в промислових мережах; 3. Розроблено аналітичні моделі адаптивного централізованого управління на основі застосування моделей систем хмарного сервісу; 4. Запропоновано комплекс імітаційних моделей, що дозволяє розраховувати характеристики широкосмугових промислових мереж з адаптивним динамічним централізованим управлінням. Рішення деяких, поставлених у цій роботі, задач виконано автором самостійно, рішення деяких проблем було взято із джерел. Постановка задач, вибір підходів до їхнього рішення й обговорення отриманих результатів і переваг нових розроблених підходів до даної задачі були проведені автором разом з науковим керівником. Розроблене програмне забезпечення має простий, дружній та зручний інтерфейс користувача, що забезпечує легкість у освоєнні роботи програмного продукту, зручність у використанні, і не потребує особливих спеціальних знань. При створені програмного забезпечення було використано об'єктно-орієнтований підхід, що відповідає сучасним тенденціям у галузі розробки комерційних програмних систем. Програма реалізована на мові високого рівня Delphi. Дана мова програмування дозволяє найбільш ефективно обробляти дані. Це дозволило мінімізувати строк розробки програмного забезпечення, і, як слід, зменшити витрати на його розробку. Запропоноване програмне забезпечення ділиться на загальне програмне забезпечення, що поставляється із засобами обчислювальної техніки й спеціальне програмне забезпечення, що спеціально розроблене для даної конкретної системи й включає програми, що реалізують її функції. Для підвищення рівня безпеки запропоновано застосовувати алгоритм Khufu.

Список літератури

1. Юдін О. К. Хмарні технологій організації інтегрованих корпоративних мереж / О. К. Юдін, Р. В. Зюбіна, Т. В. Зюбін. Інформаційна безпека. 2013. Т. 11, №. 3. С. 112–127.
2. Смирнов А.А. Усовершенствованный алгоритм управления доступом к «облачным» телекоммуникационным ресурсам / Мохамад Гани Абу Таам, А.А. Смирнов, Н.С. Якименко, С.А. Смирнов. Збірник наукових праць "Системи обробки інформації". Випуск 1(126). Х.: ХУПС, 2015. С. 150-153.
3. Смирнов А.А. Исследование эффективности метода управления доступом к облачным антивирусным телекоммуникационным ресурсам / Мохамад Гани Абу Таам, А.А. Смирнов, С.А. Смирнов. Наука і техніка Повітряних Сил Збройних Сил України. Випуск 3(19). Х.: ХУПС, 2015. С. 134-141.
4. Смирнов А. А., Смирнов С. А., Дидык А. К. Разработка и реализация метода безопасной маршрутизации метаданных в облачные антивирусные системы. Securitea informationala 2015-2016: Conferenta internationala (editia a XII-a), Chisinau, Moldova, 3 martie 2016, Chisinau: ADSEM, 2016, С. 90-96.
5. GERT-моделі технології хмарного антивірусного захисту / О.А. Смірнов та ін. Кібербезпека: освіта, наука, техніка. Київський університет ім.Бориса Грінченка, Т. 2, № 2, С. 6-30, Груд. 2018. doi:10.28925/2663-4023.2018.2
6. Метод формування антивірусного захисту даних з використанням безпечної маршрутизації метаданих / С.А. Смірнов та ін. Кібербезпека: освіта, наука, техніка. Київський університет ім.Бориса Грінченка, Т. 3, № 3, С. 63-87, Бер. 2019. doi:10.28925/2663-4023.2019.3.6387

7. Jose M. Alcaraz Calero, Nigel Edwards, Johannes Kirschnick, Lawrence Wilcock & Mike WrayClouds: Toward a multi-tenancy authorization system for cloud services / IEEE Security and Privacy, 2010, pp. 16-122.
8. Chou D.C. & Chou A.Y. Software as a Service (SaaS) as an Outsourcing Mode / An Economic Analysis, 2007, pp. 386-391.
9. Jun Feng, Yu Chen. Bridging the Missing link of Cloud data storage security in AWS / IEEE conf. on CCNC, 2010.
10. I. Iankoulova, M.Daneva: Cloud Computing Security Requirements: a Systematic Review / Sixth International Conference on Reseatch Challenges in Information Science, 2012, pp.1-7.

УДК 004

О. Раков, магістр гр. КН-18М-1,9
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СЕРВІСУ МОНІТОРИНГУ ТА КОНТРОЛЮ СТАНУ ІТ

У статті розглянуто програмне забезпечення, яке призначено для сервісу моніторингу та контролю стану ІТ. Метою розробки є дослідження та програмна реалізація сервісу моніторингу та контролю стану ІТ. Об'єктом дослідження є процес моніторингу та контролю стану ІТ. Предметом дослідження є методи моніторингу та контролю стану ІТ. Методи дослідження базуються на методах надійності, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація сервісу моніторингу та контролю стану ІТ. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

комп'ютерні науки, моніторинг та контроль стану ІТ

Постановка проблеми. Традиційний підхід до моніторингу ІТ-інфраструктури не відповідає її складності, мінливості й ступеню впливу на роботу всієї організації. Це ставить під погрозу всі рівні підтримки ІТ-інфраструктури: від планування до оперативного обслуговування. Найчастіше компанії починають реагувати на таку невідповідність тільки в тому випадку, коли воно приводить до вкрай хворобливих наслідків. Що можна зробити вже сьогодні, щоб ці проблеми залишилися в минулому?

Якісна підтримка сучасної ІТ-інфраструктури – багатоплановий процес, складний для будь-який середньої й вже тим більше великої компанії. На цьому шляху необхідно перебороти чимало перешкод, щоб досягти стабільно високих результатів, але виходить це далеко не в усіх. Серед багатьох проблем виділяється одна – відсутність цілісного підходу до моніторингу ІТ-інфраструктури. А тим часом на основі такого підходу вибудовується вся система реагування на інциденти і їхнє запобігання.

Із цією проблемою постійно зіштовхуються більшість компаній незалежно від їхнього розміру й сфери діяльності. Причому її важливість і навіть наявність не завжди усвідомлюються, тому боротьба йде з наслідками, а не із причиною. Результат – нестабільність і низька якість роботи не тільки самої ІТ-інфраструктури, але й інформаційної системи (ІС) у цілому. Більше того, під погрозою виявляються основна діяльність, фінансове становище й репутація організації. На щастя, сьогодні проблему можна не тільки ідентифікувати, але й ефективно вирішити. Цьому й присвячений дана робота.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини сервісу моніторингу та контролю стану ІТ.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація сервісу моніторингу та контролю стану ІТ.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем моніторингу та контролю стану ІТ.
– Дослідження сервісу моніторингу та контролю стану ІТ.
– Програмна реалізація сервісу моніторингу та контролю стану ІТ.

Об'єктом дослідження є процес моніторингу та контролю стану ІТ.

Предметом дослідження є методи моніторингу та контролю стану ІТ.

Методи дослідження базуються на методах надійності, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу.

Опис функціонування системи

Моніторинг ІТ систем є складовою частиною керувань інформаційною інфраструктурою підприємства, що полягає в постійному спостереженні й періодичному аналізі ІТ об'єктів з відстеженням динаміки змін, що відбуваються з ними. Ключовим завданням систем моніторингу ІТ є одержання, збереження й аналіз інформації про стан підконтрольних елементів ІТ структури компанії. Спеціальна програма дозволяє оперативно відреагувати на виниклу проблему в роботі ІТ сервісів, а також ефективно запобігати виникнення неполадок.

Постачальники даної послуги виділяють 2 рівні ІТ моніторингу:

– ІТ інфраструктури.
– ІТ сервісів.

Системи моніторингу ІТ інфраструктури призначені для контролів над працездатністю наступних компонентів: мережеве й серверне встаткування, бізнес ПЗ. Під контролем програми моніторингу повинні перебуває групи об'єктів, інформація про які необхідна адміністраторам.

Впровадження комплексної системи моніторингу ІТ допомагає підприємству:

– знизити час простою компонентів ІТ структури;
– збільшити доступність програм для бізнесу;
– здійснювати проактивний аналіз неполадок;
– підвищити рівень продуктивності використання інформаційних ресурсів.

Системи моніторингу ІТ сервісів орієнтовані в першу чергу на показники ступеня доступності, а також якості надання сервісів на основі оцінки користувачів. У процесі створення системи відбувається формування каталогу ІТ сервісів. Визначаються показники доступності й рівня якості кожного сервісу і його залежність від інших компонентів інформаційної структури компанії. Система проводить моніторинг ІТ компонентів і формує показники роботи сервісів. Моніторинг ІТ систем корисний системним адміністраторам, ІТ керівникам і менеджерам ІТ сервісів.

Система моніторингу ІТ сервісів допомагає компанії:

– зробити більше високим рівень доступності сервісів ІТ;
– знизити витрати на їхню підтримку;
– збільшити ефективність роботи ІТ персоналу і якості обслуговування.

Комплексні системи моніторингу працездатності ІТ інфраструктури

Впровадження автоматизованої системи моніторингу ІТ і контролі роботи інформаційної інфраструктури здатно підвищити рівень якості її функціонування за допомогою швидкого виявлення й ліквідації збоїв і неполадок, а також запобігання їхнього виникнення в майбутньому, у першу чергу, для найбільш критичних для бізнесу компанії сервісів.

Спеціалізовані фірми пропонують повний цикл послуг зі створення й експлуатації систем моніторингу ІТ, що дозволяють ефективно вирішувати наступні питання:

– вчасно фіксувати виникнення проблем у роботі компонентів ІТ структури;
– виявляти місце й характер неполадки;

– визначати вплив виниклої проблеми на можливість надань IT сервісів (це необхідно для вірного розміщення пріоритетів у роботах з ліквідації збоїв;
– проактивно стежити за змінами у функціонуванні інфраструктури;
– запобігати ймовірні збої.

Профільовані в даній сфері компанії займаються проектуванням, впровадженням в експлуатацію й підтримкою систем IT моніторингу. Проведення експертизи перед початком проекту впровадження допоможе правильно вибрати й інтегрувати один з одним необхідні продукти для ведення моніторингу елементів інфраструктури, що, у свою чергу, дозволить у підходящий термін і найбільше повно виконати завдання клієнтської компанії по підвищенню рівня надійності і якості роботи IT.

Підходи до створення комплексної системи моніторингу

У процесі побудови системи моніторингу застосовують 2 підходи:
– підхід від інфраструктури (тобто «знизу нагору»);
– підхід від IT сервісів (тобто «зверху долілиць»).

Як показує практика, найбільший ефект досягається при використанні комбінації даних двох підходів.

Побудова систем моніторингу від інфраструктури

Цей підхід передбачає організацію спостереження за основними апаратними й програмними компонентами з налаштуванням окремих консолей для виконання завдань різних адміністраторів на основі їхньої спеціалізації. Головною метою є допомога IT фахівцям в оперативному виявленні й ліквідації проблем, що з'являються при функціонуванні IT структури.

Організація системи моніторингу від IT сервісів

Застосування даного підходу полягає у формуванні каталогу послуг і відповідає методології сервісного підходу до керування IT (ITSM). Передбачається, що для кожного сервісу (послуги) повинна бути розроблена своя сервісно-ресурсна модель, що відбиває взаємодію між сервісом і іншими компонентами інфраструктури, потрібними для його роботи. З використанням сервісно-ресурсної моделі проводиться процедура налаштування програми моніторингу з метою контролю функціонування IT сервісу й всіх пов'язаних з ним компонентів інфраструктури. Цей підхід сприяє тому, що системні консолі стають корисними не тільки відповідальним за підтримку певних сервісів IT фахівців, але й диспетчерській службі, а також керівництву IT відділу.

Технічна сторона моніторингу

Для збору даних про стан інформаційних ресурсів і сервісів застосовують спеціалізоване програмне забезпечення. Важливим завданням стає правильний вибір і інтеграція продуктів, що найкраще підходять для самого повного і якісного виконання вимог клієнтської організації до моніторингу IT систем і ресурсів.

Що входить у комплексну систему моніторингу

Моніторинг мереж:
– моніторинг IP мереж – побудова й відображення топології мереж; збір, наступна обробка й відображення повідомлень про проблеми;
– моніторинг продуктивності мережевих інтерфейсів і пристроїв – збір статистичних даних по завантаженню й числу помилок; формування звітності й прогнозів;
– керування конфігураціями мережевого встаткування – автоматизація керування ними.

Моніторинг серверів і робочих станцій:
– моніторинг продуктивності серверів – одержання даних про різні параметри продуктивності, створення графічних звітів;
– моніторинг апаратних збоїв – одержання даних про збої в апаратному забезпеченні серверів;
– моніторинг збоїв в операційній системі – одержання даних про роботу ОС за допомогою певних параметрів.

Моніторинг додатків і сервісів:

– активний моніторинг програм і мережевих сервісів – одержання даних про рівень їхньої доступності й продуктивності за допомогою активних моніторів;

– моніторинг збоїв у програмах – збір і відображення відомостей про роботу різних додатків (з використанням певних параметрів;

– моніторинг продуктивності додатків – спостереження за часом виконання різних транзакцій і за ресурсами додатків;

– моніторинг сервісів – створення сервісно-ресурсної моделі, відбиття даних у формі ієрархічно зв'язаної структури.

Надання даних:

– портал системи керування ресурсами – вивід даних у єдиної веб-консолі;

– формування звітності – створення різноманітних звітів про функціонування IT інфраструктури.

Моніторинг бізнес-процесів:

– моніторинг стану бізнес-процесів – одержання й надання даних про протікання даних процесів.

Впровадження систем моніторингу IT

Проект впровадження системи починається із процесу базової інсталяції продуктів і закінчується остаточним їхнім налаштуванням під потреби конкретного замовника. Більшість програм поставляються вже в комплекті з готовим налаштуванням моніторингу певних типів ресурсів. Це допомагає значно скоротити строки впровадження. Звичайно, для того, щоб проект був реалізований в оптимальний час і без помилок, навіть початкова установка програми повинна виконуватися силами фахівців, що володіють досвідом інсталяції, налаштування й використання програмного продукту.

Інтеграція з іншими інформаційними системами (CMDB, HelpDesk і ін.) є важливим етапом при впровадженні системи IT моніторингу, що не може працювати ізольовано від інших. У більшості випадків стає необхідно забезпечити її взаємодію зі службою підтримки для реєстрації в автоматичному режимі інцидентів, а також із системою інвентаризації ресурсів IT.

Технічну підтримку, як правило, здійснюють інтегратори системи в рамках IT аутсорсингу. Для клієнтської компанії це зручно тим, що вона може вирішувати всі питання, пов'язані з моніторингом його інфраструктури, в одній крапці, що особливо важливо при використанні багатокомпонентної системи, що містить програми від різних виробників.

Супровід системи моніторингу також часто входить у пакет послуг, надаваних інтегратором. Навіть якщо система була здана в експлуатацію з повною документацією, після проведення впровадження в більшості випадків потрібне певний час, щоб системні адміністратори, що працюють у клієнтській компанії, змогли навчитися нею управляти. Для цього їм буде потрібно перейняти досвід у представників фірми, що займалася конфігуруванням системи. Найбільш доцільним буде скористатися допомогою фахівців інтегратора для тонкого налаштування впровадженої системи. До того ж послуга супроводу системи моніторингу, надавана аутсорсинговою компанією, дозволить скоротити число системних адміністраторів на підприємстві.

Розробка структурної схеми

Сервіс централізованого моніторингу й контролю

Сервіс централізованого моніторингу й контролю (СЦМК) – це сервіс, що складається не тільки з технічного, але й з експертного контуру, тобто він підкріплюється регулярно поповнюваною базою знань із експертного центра й потужною експертизою виділеної багатопрофільної команди. Фахівці останньої безупинно аналізують потік даних, надаваних засобами моніторингу, і можуть завчасно попередити про проблеми, запропонувавши способи їхнього рішення. Так що ж принципово міняється в цій схемі?

Корпоративний замовник одержує готовий бізнес-процес моніторингу й контролю стану IT. Цей процес досить просто й швидко (підключення й автоматичне налаштування

займають усього кілька годин) адаптується відповідно до потреб конкретної організації. Інкорпорована усередину процесу технологія обкачана на сотнях корпоративних клієнтів. Більше того, у процесі задіється такий обсяг компетенцій і експертизи, яким навіть велика компанія майже напевно не розташовує (наймати й утримувати в штаті фахівців такого рівня занадто дорого, оскільки в одній організації не реалізується стільки релевантних для їхнього рівня проектів).

Початок збору й нагромадження потрібних даних не відкладається на невизначений строк. Замовникові не прийде розглядати й погоджувати окремий бюджет на закупівлю ліцензій, довго впроваджувати продукт, збирати й навчати фахівців, тому що при створенні СЦМК ставка робиться на використання власних наробітків і компонентів, що функціонують на базі вільного ПЗ. Все налаштування вже автоматизоване, за неї відповідають виділені ІТ-менеджери й фахівці.

Перші результати можна одержати вже через кілька днів або тижнів (багато чого залежить від масштабу компанії, цілей і завдань бізнесу, а також від поточного стану інфраструктури). Більші витрати й неочевидні результати просто виключені, причому незалежно від того, чи підключається СЦМК час від часу (наприклад, перед сезонними піками продажів або для підтримки складного й дорогого впровадження) або постійно (для ощадливого регулярного ІТ-аудита інфраструктури або частини інфраструктури, наприклад регіональної).

Процес моніторингу й контролю ІТ увесь час актуалізується. Сервіс автоматично й безпомилково виявляє нові об'єкти моніторингу. Він дозволяє вирішити проблеми, які тільки що виявилися (разом із впровадженням нових ІТ-продуктів або погрозами ІБ), або закрити ті, які вирішені й більше ніколи не виявляться в інфраструктурі клієнта.

Замовник одержує можливість більш об'єктивно реєструвати не тільки ІТ-інциденти (миттєвий і правильний результат), але й – у міру нагромадження даних – будь-яку інформацію про вузькі місця в серверному ландшафті (відкладений, стратегічний результат). Крім того, він одержить всю інформацію про самих проблемний ІТ-сервіси, на яких потрібно звернути увагу в першу чергу. Всі відомості збираються й поєднуються досвідченими фахівцями й експертами, для яких ця діяльність є основною. Пропозиції, формовані на основі отриманої інформації, дозволяють більш ефективно використовувати наявні засоби й точніше планувати ІТ-бюджет.

Разом зі СЦМК замовник одержує готову базу кращих практик. Незважаючи на специфіку, властиву кожної компанії, більшість наявних ІТ-сервісів побудовано на основі добре вивчених і багато в чому стандартизованих рішень, особливо якщо це типові пропозиції вендорів або аутсорсерів, що дозволяє консолідувати досвід, отриманий при роботі з різними організаціями. У результаті рішення навіть складної, унікальної, з погляду клієнта, проблеми виявиться, швидше за все, уже глибоко пророблениим. Інакше кажучи, замовник перестає бути «площадкою для експериментів», він починає користуватися плодами досвіду тих, хто підключив для нього СЦМК – неважливо, на постійній основі або тимчасово.

СЦМК орієнтується на недопущення проблем, а не на усунення вже виниклих збоїв. Особливо, якщо мова йде про збої й простої, викликаних неякісними або застарілими архітектурними рішеннями. Такий підхід дозволяє мінімізувати втрати завдяки ранньому виявленню й виправленню потенційних недоліків і проблем різного ступеня критичності ще до того моменту, коли вони могли б нанести втрату бізнесу.

СЦМК може бути не революційним, а додатковим рішенням, що підтримує й контролює роботу внутрішньої ІТ-служби. Наприклад, такий підхід вигідний фармацевтичним або торгово-роздрібним компаніям, тобто тим галузям, де фінансова відповідальність бізнесу вкрай висока й діють глобальні обмеження, що роблять неможливої або хворобливої зміну моделі ІТ-підтримки. Для таких підприємств надзвичайно важливий подвійний контроль якості роботи ІТ, відсутність конфлікту інтересів, грамотна технічна й

організаційна експертиза, широкий діапазон знань (за рахунок можливостей сильного експертного центра).

СЦМК може стати тимчасовою страховкою для бізнесу. Якщо, наприклад, не влаштовує робота внутрішньої IT-служби або постачальника зовнішніх IT-послуг, дуже корисної може виявитися можливість обпертися на плечі команди експертів, що вже знає все про інфраструктуру компанії й у будь-який момент здатна прийти на допомогу.

Таким чином, вбудовування СЦМК у фундамент організаційно-технічної системи підтримки IT-інфраструктури організації не тільки дозволяє за порівняно невеликі гроші вирішити зазначені вище проблеми, але й дає додаткові переваги: якісний, добре спланований і грамотно реалізований процес по пошуку, правильному визначенню, класифікації, реєстрації й рішенню IT-проблем; необхідні технічні й експертні інструменти, що гарантують результат, причому без створення найчастіше неефективних внутрішніх механізмів моніторингу й контролю IT.

СЦМК-діяльність підтримується різними типами інструментальних засобів й процедур по їхньому використанню. Залежно від ситуації, ці інструменти можуть включати комбінацію різних можливостей – автоматизовані засоби можуть вирішувати окремі завдання СЦМК, інтегровані засоби можуть обслуговувати потреби багатьох учасників процесу програмної інженерії (наприклад, СЦМК, розробку, перевірку й атестацію й т.п.). Значимість інструментальної підтримки конфігураційного керування (як і інших аспектів діяльності в області програмної інженерії) росте з кожним днем разом зі складністю впровадження, ростом розміру проектів і складності проектного оточення. Можливості інструментальних засобів розвиваються для забезпечення підтримки:

– СЦМК-бібліотек (проектно-проектно-орієнтованих баз знань).
– Запитів на зміни (software change request – SCR) і процедур затвердження (approval).
– Керування кодом (і зв'язаних робітників продуктів) і змінами.
– Звітності за статусом конфігурацій і збору відповідних метричних показників.
– Аудитові конфігурацій.
– Керуванню й відстеженню стану й повноти програмної документації.
– Виконанню завдань по складанню програмних продуктів і їхніх модулів.
– Керуванню, контролю й поставці випусків (релізів) програмних продуктів.

Інструменти, використовувані для забезпечення конфігураційного керування, можуть також надавати метрики, необхідні для вдосконалювання процесів. SWEBOK звертає увагу на наступні ключові індикатори: роботи й прогрес по їхньому виконанню (Work and Progress) і індикатори якості – потік змін (Change Traffic), стабільність конфігурацій (Stability), роздробленість (Breakage), модульність (Modularity), переробка (Rework), адаптируємість (Adaptibility), середній час між збоями (MTBF – Mean Time Between Failures), зрілість/повнота інформації (Maturity). Звітність по цих індикаторах може бути організована різним образом, наприклад, по елементах конфігурацій або за типом запитів на зміни.

На рисунку 1 зображена структурна схема системи.

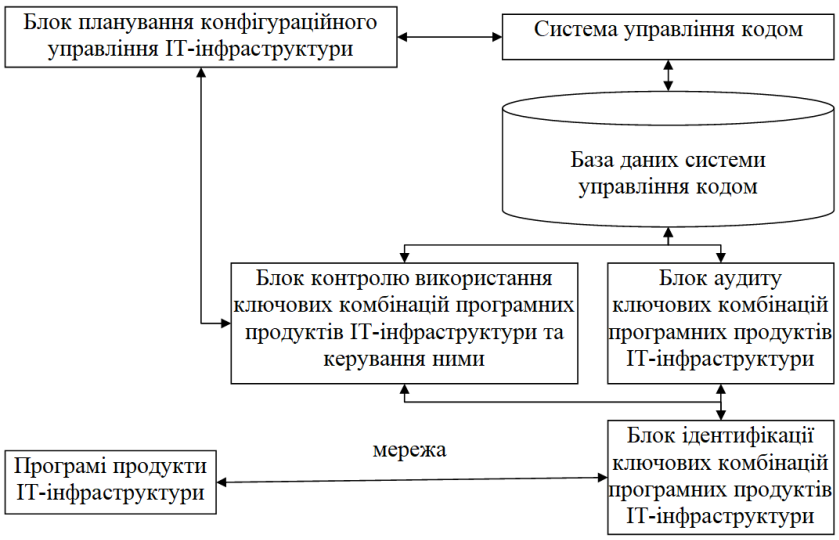


Рисунок 1 – Структурна схема системи

Зі структурної схеми видно, що система керування кодом підтримує програмні бібліотеки контролюючи доступ до елементів бібліотек, координує дії безлічі користувачів і допомагає в проведенні робочих процедур. Інші інструменти підтримують процес складання й випуску програмного забезпечення й документації на основі програмних елементів, що втримуються в бібліотеках. Інструменти для керування запитами на зміни програмного забезпечення використовуються для контрольованих системою конфігураційного керування програмних елементів. Інші інструменти можуть забезпечувати керування базою даних і необхідними менеджменту звітними засобами, а також діяльністю по розробці й забезпеченню якості. Як уже згадувалося вище, у рамках СЦМК-системи може бути об'єднаний цілий ряд інструментів різних типів. При цьому сама система конфігураційного керування може бути тісно зв'язана й підтримувати інші види робіт, що стосуються не тільки СЦМК.

У процесі планування інженери вибирають ті СЦМК-засоби, які застосовні для рішення поставлених перед ними завдань.

У процес планування розглядаються аспекти, які можуть “спливти” у процесі впровадження обираної системи конфігураційного керування. Зокрема, обговорюються й питання можливих “культурних” змін, якщо це необхідно Додаткова інформація, що зачіпає СЦМК-інструментарій, представлена в області знань SWEBOK “Software Engineering Tools and Methods”.

Висновок. У статті розглянуто та проаналізовано програмне забезпечення, створене в результаті виконання роботи, призначено для сервісу моніторингу та контролю стану ІТ. В межах України в недостатній мірі представлені вітчизняні розробки в цій області. У роботі наведені теоретичне узагальнення й рішення наукового завдання дослідження методів моніторингу та контролю стану ІТ. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем моніторингу та контролю стану ІТ; Досліджена система моніторингу та контролю стану ІТ; На основі отриманих результатів досліджень створена програмна реалізація сервісу моніторингу та контролю стану ІТ. Розроблені під час виконання роботи алгоритми дозволяють успішно вирішувати завдання моніторингу та контролю стану ІТ. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки. Розроблене програмне забезпечення має простий, дружній та зручний інтерфейс користувача, що забезпечує легкість у освоєнні роботи програмного продукту, зручність у використанні, і не потребує особливих спеціальних знань. При створені програмного забезпечення було використано об’єктно-орієнтований підхід, що відповідає

сучасним тенденціям у галузі розробки комерційних програмних систем. Програма реалізована на мові високого рівня Delphi 10.2 Tokyo. Дана мова програмування дозволяє найбільш ефективно обробляти дані. Це дозволило мінімізувати строк розробки програмного забезпечення, і, як слід, зменшити витрати на його розробку. Запропоноване програмне забезпечення ділиться на загальне програмне забезпечення, що поставляється із засобами обчислювальної техніки й спеціальне програмне забезпечення, що спеціально розроблене для даної конкретної системи й включає програми, що реалізують її функції. Даються необхідні рекомендації з установки розробленого програмного забезпечення. Для підвищення рівня безпеки запропоновано застосовувати алгоритм Діффі-Хеллмана.

Список літератури

1. Коваленко А.С. Разработка структуры базы данных интегрированной информационной системы / А.С. Коваленко, А.В. Коваленко // Информационные технологии и защита информации в информационно-коммуникационных системах: монографія / Под редакцией профессора В.С. Пономаренко. – Х.: Вид-во ТОВ «Щедра садиба плюс», 2015. – С. 54-64.
2. Кожанова А.С. Обґрунтування необхідності створення систем технічної діагностики інтегрованих інформаційних систем / О.А. Смірнов, А.С. Кожанова, О.В. Коваленко // Системи обробки інформації. – Х.: ХУПС, 2013. – Вип. 6(113). – С. 255-257.
3. Коваленко А.С. Задачи распознавания ситуаций в ERP системах / А.В. Коваленко ., А.А. Смірнов, А.С. Коваленко // Системи обробки інформації. – Х.: ХУПС, 2014. – Вип. 4(120). – С. 161-164.
4. Коваленко А.С. Підсистема технічної діагностики для автоматизації процесів керування в інтегрованих інформаційних системах / А.С. Коваленко , О.А.Смірнов, О.В. Коваленко // Системи озброєння і військова техніка.– Х.: ХУПС, 2014. – № 1(37). – С. 126-129.
5. Коваленко А.С. Анализ эффективности использования экспертной системы технической диагностики с традиционной структурой / А.С. Коваленко, А.А. Смирнов, А.В. Коваленко // Системи озброєння і військова техніка. – Х.: ХУПС, 2014. – № 2(38). – С. 106-108.
6. Коваленко А.С. Разработка структуры экспертной системы технической диагностики интегрированной информационной системы / А.С. Коваленко, А.А. Смирнов, А.В. Коваленко // Наука і техніка Повітряних Сил Збройних Сил України. – Харків: ХУПС, 2014. – № 2(15). – С.154-157.
7. Коваленко А.С. Разработка структуры экспертной системы технической диагностики интегрированной информационной системы / А.С. Коваленко, А.А. Смирнов, А.В. Коваленко // Наука і техніка Повітряних Сил Збройних Сил України. – Харків: ХУПС, 2014. – № 2(15). – С.154-157.
8. Коваленко А.С. Структура системи технічної діагностики інтегрованих інформаційних систем / А.С. Коваленко, О.А. Смірнов, О.В. Коваленко // Збірник наукових праць Кіровоградського національного технічного університету / техніка в сільськогосподарському виробництві, галузеве машинобудування, автоматизація. – Кіровоград: Вид-во КНТУ, 2014. – Вип. 27. – С. 245-251.
9. Коваленко А.С. Дослідження будови інтегрованої інформаційної системи та її елементів / А.С. Коваленко, О.А. Смірнов, О.В. Коваленко // Системи озброєння і військова техніка. – Х.: ХУПС, 2014. – № 4(40). – С. 85-88.
10. Коваленко А.С. Розробка структури бази даних для обліку технічного стану елементів інтегрованої інформаційної системи з урахуванням вимог споживачів інформації / А.С. Коваленко, О.А. Смірнов, О.В. Коваленко // Системи обробки інформації. – Х.: ХУПС, 2015. – Вип. 1(126). – С. 75-79.

УДК 004

Д. Рисований, магістр гр. КІ-18М-1,4
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ ОЦІНКИ ПРОДУКТИВНОСТІ СИСТЕМ ЗБЕРІГАННЯ ДАНИХ

У статті розроблено програмне забезпечення, яке призначено для системи платформи віртуалізації з підтримкою розподіленого сховища. Метою розробки є дослідження та програмна реалізація платформи віртуалізації з підтримкою розподіленого сховища. Об'єктом дослідження є процес віртуалізації з підтримкою розподіленого сховища. Предметом дослідження є методи віртуалізації з підтримкою розподіленого сховища. Методи дослідження базуються на методах серверної віртуалізації, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація платформи віртуалізації з підтримкою розподіленого сховища. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

комп'ютерна інженерія, серверна віртуалізація, розподілені сховища.

Постановка проблеми. Технології віртуалізації стали дуже популярні – на їхній базі будуються й приватні IT-інфраструктури, і величезні публічні хмари. Віртуалізується все: обчислення, зберігання даних, мережні функції, десктопи, окремі додатки.

Суть серверної віртуалізації – забезпечувати одночасний запуск на сервері декількох гостьових операційних систем, щоб зробити з одного фізичного сервера декілька віртуальних. При цьому кожна з гостьових систем працює зі своїм набором ресурсів, розподілом яких займається платформа віртуалізації, установлена на фізичному «хості».

Віртуалізація дозволяє скоротити кількість фізичних серверів: замість декількох старих можна встановити один могутніший і запустити потрібне число гостьових ОС у віртуальному середовищі, де вони будуть логічно ізольований друг від друга. Крім того таке середовище забезпечує гнучке адміністрування інфраструктури й підвищену відказостійкість: у випадку відмови одного із серверів кластера віртуальні машини автоматично «переїжджають» на інший сервер. Наявні технології дозволяють зробити це без зупинки сервісу, тобто непомітно для користувачів. Найчастіше за допомогою серверної віртуалізації корпоративні клієнти хочуть знизити енергоспоживання, спростити адміністрування серверів і виключити простої серверного встаткування. Таким чином, використання віртуалізації дозволяє істотно скоротити витрати на побудову центрів обробки даних (ЦОДів), закупівлю серверного й мережного встаткування, апаратних і програмних рішень. До слова, на приватну корпоративного сегмента доводиться більше 80% усього ринку віртуалізації.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи оцінки продуктивності систем зберігання даних.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація платформи віртуалізації з підтримкою розподіленого сховища.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем віртуалізації з підтримкою розподіленого сховища.
– Дослідження платформи віртуалізації з підтримкою розподіленого сховища.
– Програмна реалізація платформи віртуалізації з підтримкою розподіленого сховища.

Об'єктом дослідження є процес віртуалізації з підтримкою розподіленого сховища.

Предметом дослідження є методи віртуалізації з підтримкою розподіленого сховища.

Методи дослідження базуються на методах серверної віртуалізації, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Віртуалізація серверів – технологія, що дозволяє запустити кілька віртуальних серверів у рамках одного фізичного сервера. Віртуальні машини або сервери являють собою додатки, запущені на хостівій операційній системі, які емулюють фізичні пристрої сервера. На кожній віртуальній машині може бути встановлена операційна система, на яку можуть бути встановлені додатки й служби.

Серверна віртуалізація застосовується для консолідації серверів, розробки й тестування програмних продуктів, освітніх систем. Рішення серверної віртуалізації початкового рівня використовуються звичайно для відділів розробки/тестування; середнього рівня – для web-порталу, кластерів пошти й баз даних, додаткових серверів до «реальних» у кластері; верхнього рівня – для повноцінних центрів обробки даних, web-порталів, кластерів.

Розрахунок економічної ефективності використання рішення приводиться на основі попереднього аналізу існуючої інфраструктури й містить у собі вартість експлуатації IT-інфраструктури як з використанням технології віртуалізації, так і в «класичному» виді.

Економія до 85% досягається за рахунок:

– скорочення витрат на серверну кімнату – зниження темпів росту серверного парку дозволяє ефективніше використовувати серверні приміщення;

– скорочення витрат на електроенергію, споживану серверами й системою охолодження;

– скорочення витрат на ліцензії ОС Windows – можливість використання процесорних ліцензій для декількох віртуальних систем на одному сервері.

Віртуалізація ще два-три роки тому стала загальноприйнятої (commodity) технологією в сфері корпоративних IT.

Але незважаючи на свою повсякденність, питання поточного стану технологій віртуалізації, а головне – перспектив їхнього розвитку є досить і досить актуальними для IT-ринку (причому як для замовників, так і для IT-постачальників). Їхній розвиток триває не настільки бурхливо, як у минулі роки, але досить значимо для більшості IT-споживачів. Отут можна провести аналогію з рікою: її бурхливими джерелами й плавним плином у середній і нижній частинах, новиних подій унизу начебто б небагато, але саме вони найбільш важливі для жителів.

Віртуалізація є ключовий технологій для всіх різновидів IT-хмар, зовнішніх і внутрішніх, глобальних і локальних, публічних і приватних. Хмари зараз вступили в ту фазу свого розвитку, коли на перший план виходять питання підвищення їхньої внутрішньої ефективності (продуктивності, гнучкості, надійності), що, у свою чергу, у вирішальному ступені залежить від використовуваних технологій віртуалізації. Розвиток хмарних послуг іде в істотній мері за рахунок розширення мережі локальних провайдерів, бізнес яких будується саме на основі платформ віртуалізації. Замовники також уже пройшли фазу первинного впровадження технологій віртуалізації, перед ними встають питання модернізації існуючої інфраструктури, можливо навіть зі зміною вендора. Багато компаній переходять від використання технологій єдиного постачальника до мультивендорних схем, відповідно встають питання керування гетерогенними віртуалізованими середовищами.

Замовникам потрібно бути в курсі того, що відбувається на ринку віртуалізації й розуміти тенденції його розвитку – саме із цієї тези починається черговий щорічний звіт Gartner «Магічний квадрант для віртуалізації серверної x 86-інфраструктури» (Magic Quadrant for x86 Server Virtualization Infrastructure, 2017), у якому аналітики компанії дають свої відповіді на ці питання.

Структура й динаміка ринку

Саме поняття «інфраструктура серверної віртуалізації» уже давно досить стабілізувалося, у нього Gartner включає наступні основні компоненти: гіпервізори для

створення віртуальних машин (ВМ), віртуалізаційні технології використання ОС додатками в поділюваному режимі (так звані контейнери), базові набори засобів адміністрування віртуальних середовищ, а також базові набори убудованих засобів керування віртуальними середовищами (зокрема, підтримка живої міграції й основні функції автоматизації адміністрування). Але в цей список не входять високорівневі рішення для керування середовищами, у тому числі інструменти, що виконують такі функції, як автоматизація операцій, моніторинг віртуальних середовищ, виміри продуктивності додатків, планування й керування навантаженнями серверів та ін.

Але якщо із составом засобів віртуалізації все ясно, то із традиційними характеристиками IT-сегментів – обсягами продажів у грошовому вираженні – ясності як не було, так і немає. Протягом всіх шести років проведення досліджень даного ринку Gartner не давала кількісних оцінок (як абсолютних, так і по темпах росту). Зрозуміло, у цьому важко дорікнути аналітиків, оскільки даний пробіл лише відбиває специфіку віртуалізаційного напрямку: його дуже складно виділити із загальної IT-середовища й порахувати. Технології віртуалізації сильно інтегровані в інфраструктурні IT-продукти, до того ж отут досить великий приватна безкоштовних пропозицій. Коротше кажучи, віртуалізація – це саме той випадок, коли для розуміння щирої ситуації і її динаміки потрібно використовувати натуральні характеристики.

По даним Gartner, сьогодні близько 75% робочого навантаження для серверної x 86-інфраструктури виконується на віртуалізованих комп'ютерах (рік назад говорилося про 70%, а два роки тому – 66%), і, швидше за все, це не межа для росту цієї приватні. Основна частина віртуалізованого середовища доводиться на віртуальні машини (технологія гіпервізорів), але останнім часом спостерігається помітне підвищення інтересу замовників і провайдерів до використання контейнерів – багато в чому завдяки росту рівня зрілості хмарних обчислень (боротьба за підвищення ефективності, стандартизація сервісів, ріст числа й спектра SaaS-пропозицій і пр.).

Істотна частина віртуалізованої IT-інфраструктури доводиться на IaaS-провайдерів, близько 20% всіх ВМ надається користувачам через публічні IaaS-сервіси. У цьому сегмент за останній рік спостерігається вибухообразний ріст: у торішньому огляді про 6%, при тому що в 2011 р. ця приватна була 3%. В 2014 р., по оцінках Gartner, число нових ВМ у публічних хмарах уперше перевищило аналогічний показник для On-Premise-розвертування. Причому більшість створених ВМ використовуються для нових обчислювальних навантажень, а не для переносу в них On-Premise-обрахунків. У корпоративному сегменті, у якому переважає застосування успадкованих додатків, динаміка проникнення віртуалізації помітно нижче. У цілому можна констатувати, що основним драйвером у сфері віртуалізації є нові хмарні додатки й використання, що розширюється, методів гнучкої (agile) розробки ПЗ, при цьому прискореними темпами росте попит на полегшені технології віртуалізації, у тому числі – на контейнери.

Значимість ринку приватних хмар також росте. Спочатку замовники отут ішли по шляху створення On-Premise-інфраструктур, при цьому багато хто орієнтувалися на застосування віртуалізаційних технологій Open Source, у тому числі контейнерні. Зараз же більшість підприємств переходять або вже перейшли до роботи з безліччю різних архітектур (публічні й приватні хмари, On-Premise), що працюють на базі різних технологій віртуалізації. Приватна застосування моновіртуалізації на великому корпоративному ринку прагне до нуля. Вартість продовжує залишатися важливим фактором при прийнятті рішень про впровадження віртуалізації, але все-таки на передній план зараз виходять питання інтероперабельності й застосування хмарних моделей.

Gartner відзначає, що віртуалізація серверної x 86-інфраструктури є фундаментом, на якому базуються два вкрай важливих для всього IT-ринку напрямку його розвитку (причому взаємозалежних і в істотній мері пересічних): модернізація внутрішньої IT-інфраструктури замовників і хмарні обчислення. У першому випадку за допомогою віртуалізації вирішуються питання підвищення ефективності використання ресурсів, зниження вартості

(як капітальних витрат, так і операційних), оптимізації споживання енергії, підвищення швидкості розгортання нових ресурсів, загального підвищення рівня автоматизації IT. Значна частина серверного навантаження використовується для обслуговування хостуємих віртуальних десктопів (hosted virtual desktop, HVD), але оскільки саме в цьому напрямку віртуалізації спостерігається найвищий рівень консолідації (число віртуальних машин на один сервер), відсоток фізичних серверів, зайнятих під HVD, не настільки великий. При модернізації IT-інфраструктури віртуалізація виступає як загальний горизонтальний тренд, що торкає практично всіх підприємств (незалежно від розмірів і галузей) і всі обчислювальні робочі навантаження. Хмарного ж обчислення – поки більше специфічний вид використання IT, вони сьогодні використовуються там, де потрібні підвищені вимоги до гнучкості й масштабування IT-систем. Однак сфера застосування хмар швидко розширюється, їхня актуальність для замовників постійно росте. На думку експертів, найближчим часом хмарні обчислення стануть головним напрямком модернізації IT-інфраструктури в цілому.

Конкурентна ситуація

Хоча більшість підприємств уже досить добре знайомо з можливостями серверної віртуалізації й з конкретним пропозиціями вендорів, все-таки проблема вибору постачальника технологій як і раніше актуальна, більше того навіть більше значима, чим раніше. Справа в тому, що донедавна віртуалізація для замовників була тактичним завданням (випробування інновацій, рішення приватних завдань). Зараз ця тема стала стратегічної, потрібно робити вибір, що коштує дорожче й має на увазі довгострокові перспективи. Мова може йти про зміну поточного вендора, а найчастіше – про розширення состава використовуваних продуктів від різних постачальників. У кожному разі сьогодні для ухвалення рішення підприємству потрібно оцінювати весь спектр основних пропозицій на ринку (а не тільки від обраного раніше вендора), а головне – розуміти специфіку різних IT-виробників і перспективи розвитку їхнього бізнесу.

У цілому конкурентна ситуація на ринку серверної віртуалізації стабілізувалася ще два роки тому, і скільки-небудь разючих змін отут не варто очікувати. Прогнози про те, що платформні мегавендори можуть відтіснити піонера ринку, не збулися, VMware продовжує впевнено йти спереду. Єдиним рівноцінним конкурентом їй виступає Microsoft, але очікування того, що софтверний гігант зможе швидко наздогнати лідера, також не виправдалися. Хоча експерти Gartner підкреслюють, що в ринку віртуалізації буде довге життя й скорочення дистанції (чого поки не спостерігається) між парою провідних постачальників у майбутньому цілком реально.

Спочатку здавалося, що в боротьбу за лідерство зможе вступити Citrix, але компанія досить швидко відмовилася від своїх амбіцій (втім, можливо, їх і не було, цілком імовірно, що сплеск активності компанії в цьому напрямку й наступний спад були реалізацією споконвічно задуманого плану), вона досить швидко відкотилася спочатку у квадрант провидців, а потім – нішевих гравців.

У свій час висловлювалися припущення про те, що в погоню за лідерами кинеться Oracle, але компанія зайняла досить традиційну для себе позицію підтримки тільки власного стека продуктів і вище статусу «провидців» не змогла піднятися. Як ми й прогнозували рік назад, компанія не змогла удержатися в цьому сегменті, поповнивши нішевий квадрант.

Ветеран ринку серверної віртуалізації (починала майже одночасно з VMware на початку нульових років) компанія Parallels у квадранті цього року представлена під новим ім'ям Odin. Відзначимо відразу, що ця не нова назва компанії й не назва нової компанії. Це нова торговельна марка, який тепер позначається проблематика серверної віртуалізації все тої ж Parallels (назва самої компанії тепер асоціюється з напрямком клієнтської віртуалізації в основному для комп'ютерів Apple Mac). Parallels/Odin заслуговує великої поваги хоча б тому, що, будучи єдиним спеціалізованим постачальником віртуалізації, упевнено конкурує із глобальними мегавендорами.

Друга важлива специфіка компанії полягає в тім, що донедавна вона була фактично єдиним постачальником контейнерних технологій віртуалізації. Якийсь час назад здавалося,

що контейнерний напрямок є сугубо нішевим або навіть тупиковим, але в останні два роки воно переживає справжнє відродження, інтерес на ринку до нього швидко підвищується. Правда, потрібно відзначити такий парадокс: практично всі публікації на тему контейнерної віртуалізації останнього року зв'язані майже винятково з недавнім стартапом Docker, і в багатьох фахівців на ринку виникло відчуття, що Parallels взагалі пішла із цього ринку (тим більше, що це ім'я зв'язується тепер тільки із клієнтськими системами). Однак звіт Gartner вносить ясність: Odin займає стійку позицію у квадранті в оточенні IT-грандів і продовжує бути лідером по напрямку контейнерної віртуалізації.

Якщо ж говорити про те, хто може порушити сформовану за останні роки стабільність на ринку серверної віртуалізації, те, напевно, єдиний, хто має такі шанси – це китайська Huawei. Її поява у квадранті минулого року виявилося несподіванкою навіть для знавців теми, але швидко стало зрозуміло, що це відбулося не випадково, що компанія має амбіційні плани, що далеко йдуть. Цього року Huawei майже не просунулася у своїй позиції на квадранті в порівнянні з минулим роком, але Gartner відзначає, що саме вона має серйозний потенціал (і велике бажання) рухатися вперед.

Ключовою особливістю Huawei є її національність. Це єдина неамериканська компанія середовище провідних гравців цього ринку, що багато в чому визначає сильні й слабкі її сторони. Позитив – це добре відома активна політика просування китайської компанії, що базується багато в чому на потужній підтримці з боку уряду країни із другий по обсязі економікою у світі. Мінус – це саме сильний зв'язок економіки й політики в Китаї, і, отже, залежність бізнесу Huawei від геополітичної кон'юнктури. Подальші успіхи Huawei у світі (не тільки в області віртуалізації) в істотній мері залежать від того, наскільки сильно вона зможе просунутися на ринку США, чому поки багато в чому заважають всі ті ж геополітичні аспекти.

Як і в попередні роки, у нинішньому магічному квадранті представлені тільки комерційні пропозиції вендорів, у ньому відсутні різного роду проекти з використанням засобів Open Source, такі як Xen, KVM, OpenVZ і LXC. При цьому автори звіту, відзначаючи що сьогодні близько 25% використовуваних технологій серверної віртуалізації доводяться саме на відкриті технології, підкреслюють, що основна сфера їхнього застосування – пилотні впровадження або реалізація якихось унікальних проектів (Amazon, Google). При цьому роль відкритих проектів віртуалізації в розвитку ринку досить велика хоча б тому, що саме вони лежать в основі продуктів комерційних вендорів – Citrix (Xen), Oracle VM (Xen), Red Hat (KVM), Odin (OpenVZ). У дослідженні Gartner відзначаються досить успішні спроби проекту OpenStack вийти на корпоративний ринок, але експерти поки явно не поспішають із прогнозами про те, що він зможе конкурувати на рівні із провідними комерційними гравцями.

Розробка структурної схеми

Можливість упакувати додаток разом із залежними бібліотеками у віртуальний образ, легко розгорнути його (і при необхідності еластично масштабувати) у хмарному віртуальному середовищі привертає увагу багатьох компаній. Нерідко в платформи серверної віртуалізації вбудовуються засоби віртуалізації зберігання даних і мережних функцій, що дозволяє реалізувати так званий програмно обумовлений ЦОД. Мир підійшов до віртуалізації «усього» – Software-Defined Everything.

Як працюють сучасні контейнери й віртуальні машини.

У серверної віртуалізації обчислень можна виділити два класи: гіпервізори з повноцінними віртуальними машинами й контейнери. Останні відрізняються в першу чергу щільністю розміщення віртуальних середовищ на сервері (кількість контейнерів тут може бути у два із зайвим разу більше, ніж віртуальних машин на гіпервізорі) і підвищеною ефективністю (контейнери швидко завантажуються й забезпечують швидкий відгук системи на клієнтські запити). Однак не всяке прикладне навантаження можна «втиснути» у контейнер, і тоді доводиться використовувати «важкі» повноцінні віртуальні машини.

Гіпервізори – це віртуалізація на рівні встаткування. Між хостовою і гостьовими системами є прошарок, емулюючий апаратне забезпечення. У кожного гостьового середовища є власне ядро й заздалегідь певний набір ресурсів. Завантаження множинних копій ядра знижує щільність розміщення віртуальних машин на сервері. Час завантаження віртуальної машини становить кілька десятків секунд, що утрудняє оперативне виконання клієнтських запитів, коли потрібно швидко виділити додаткові ресурси.

При контейнерної віртуалізації між хостовою і гостьовими системами (контейнерами) цей прошарок відсутня: всі «гості» використовують те саме ядро «хазяїна» і деякі інші компоненти ОС. У результаті Web-сервіси, упаковані в контейнери, можуть обслужити в кілька разів більше клієнтських запитів без необхідності підключати додаткове встаткування. Ці сервіси відмінно справляються з динамічним внесенням виправлень у конфігурацію системи, забезпечуючи відповідність мінливому навантаженню при масовому наданні Web-послуг. Побудовані на основі контейнерної віртуалізації, вони демонструють більше високу (до 50%) продуктивність, а це значить, що на тому самому «залозі» можна реалізувати істотно більше послуг.

Раніше гіпервізорні й контейнерні системи були реалізовані в рішеннях різних виробників. Однак за останні кілька років з'явилися комбіновані платформи на основі гіпервізорів і контейнерів, завдяки чому користувачі можуть гнучко міняти співвідношення між ними у своєму ЦОДі й здійснювати керування за допомогою єдиного інструмента.

Спочатку рішення віртуалізації застосовувалися для того, щоб упорядкувати й консолідувати фізичні сервери, заощадити на капітальних і операційних витратах (устаткуванні й електриці), об'єднати й полегшити адміністрування. Компанії впроваджували VDI-інфраструктуру (розгортали користувальницькі десктопи усередині віртуальних машин), запускали базові сервіси по забезпеченню відказостійкості й сховища, користувалися різнорідними сторонніми й саморобними сценаріями для рішення специфічних завдань.

Поступово приватна автоматизації збільшувалася – нові віртуальні машини й сервіси стали створюватися автоматично за запитом користувача. Адміністратори впроваджують удосконалені засоби керування віртуальним середовищем: моніторинг, звітність, інтеграцію з існуючим ПЗ. Процеси конфігурації й відновлення віртуальних машин уніфіковані й автоматизовані. З'явилися розширені сервіси мобільності, відказостійкості, керування ресурсами й сховищами. Витрати на створення, підтримку й масштабування віртуальних середовищ із заданими параметрами можна розрахувати й спрогнозувати.

Конвергентні системи (об'єднання дискового простору, обчислювальних і мережних ресурсів у пул, заздалегідь зконфігурований для роботи в ЦОДі) – наступний крок уперед у порівнянні із традиційною інфраструктурою. Однак найсучаснішими й перспективними рішеннями є гіперконвергентні системи, у яких компоненти віртуалізації й програмно обумовленого сховища працюють спільно на тих самих серверах, дозволяючи ефективно використовувати як обчислювальні ресурси, так і розподілені по різних машинах диски. На відміну від монолітних (виділених) систем зберігання даних, гіперконвергентні системи масштабувати набагато простіше: досить додати диски у звичайні сервери. Що ж стосується витрат, те й тут вигода очевидна: при початковому впровадженні фінансових засобів потрібно значно менше.

Багато років лідерами віртуалізації на українському ринку були закриті рішення західних виробників. Крім того, широко використовувалися відкриті (open-source) технології. Хоча в останньому випадку мнима безкоштовність при експлуатації в «бойових» умовах великих підприємств оберталася більшими вкладеннями й зусиллями для адаптації цих відкритих рішень до промислових вимог.

У даній роботі підтримується в одному продукті обидва види серверної віртуалізації (віртуальні машини й контейнери) і віртуальне сховище.

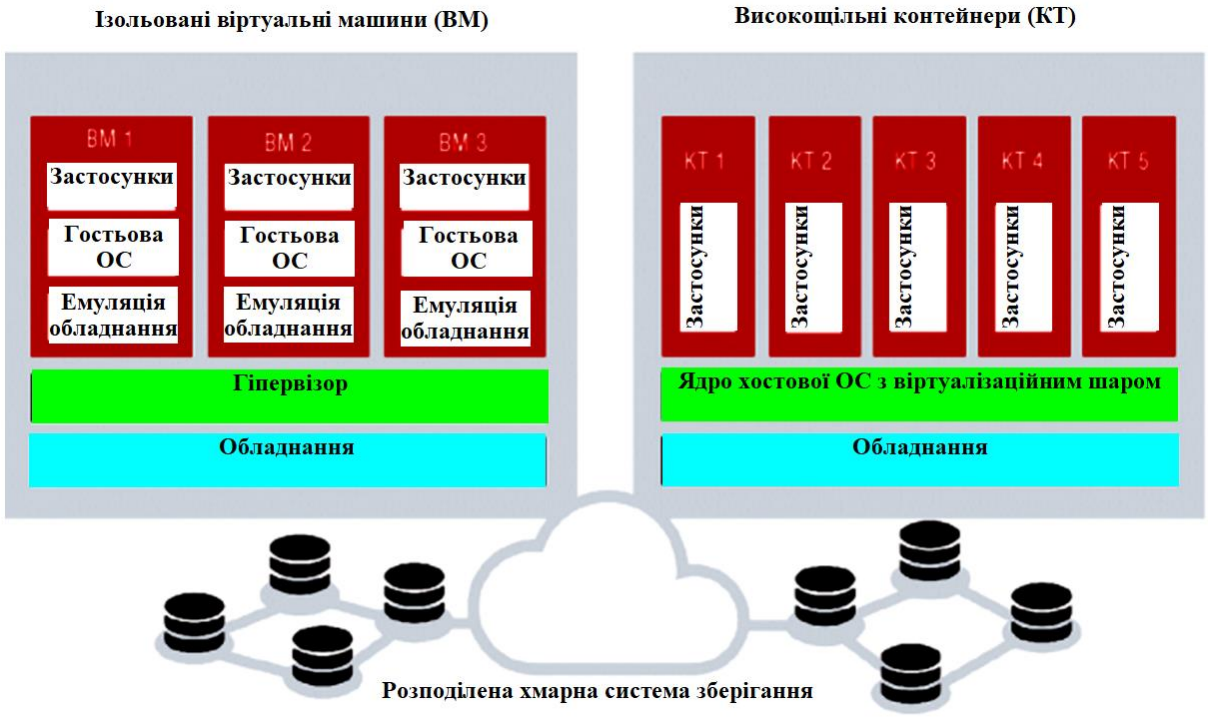


Рисунок 1 – Структурна схема системи

Продукт установлюється на голе «залізо» і не вимагає витрат на окрему операційну систему, дозволяючи використовувати звичайні сервери в трьох режимах:

Гіперконвергенція. Установлено компоненти й віртуалізації, і сховища. Сервер надає свої локальні диски загальному сховищу. Такі сервери поєднуються в локальні кластери з можливістю доступу до хмари. Спеціальний клієнт звертається до сховища по внутрішніх протоколах, крім необхідності створювати й класичні iSCSI-таргети.

Тільки віртуалізація. Бездисковий сервер надає свої обчислювальні потужності, використовуючи хмару як середовище перебування віртуальних машин. Така схема може придатися, коли обсяг сховища ще достатній, але потрібно додати обчислювальні потужності.

Тільки сховище. Локальні жорсткі диски використовуються для збільшення загального обсягу хмарного сховища. Ця схема затребувана, коли необхідно збільшити обсяг сховища за рахунок дешевих малопотужних серверів, заповнених фізичними дисками.

Висновок. У статті розглянуто та проаналізовано програмне забезпечення, яке призначено для платформи віртуалізації з підтримкою розподіленого сховища. В межах України в недостатній мірі представлені вітчизняні розробки в цій області. У роботі наведені теоретичне узагальнення й рішення наукового завдання дослідження методів віртуалізації з підтримкою розподіленого сховища. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем віртуалізації з підтримкою розподіленого сховища; Досліджена система віртуалізації з підтримкою розподіленого сховища; На основі отриманих результатів досліджень створена програмна реалізація платформи віртуалізації з підтримкою розподіленого сховища. Розроблені під час виконання роботи алгоритми дозволяють успішно вирішувати завдання віртуалізації з підтримкою розподіленого сховища. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки. Розроблене програмне забезпечення має простий, дружній та зручний інтерфейс користувача, що забезпечує легкість у освоєнні роботи програмного продукту, зручність у використанні, і не потребує особливих спеціальних знань. При створені програмного забезпечення було використано об’єктно-орієнтований підхід, що відповідає сучасним

тенденціям у галузі розробки комерційних програмних систем. Програма реалізована на мові високого рівня Delphi 10. Дана мова програмування дозволяє найбільш ефективно обробляти дані. Це дозволило мінімізувати строк розробки програмного забезпечення, і, як слід, зменшити витрати на його розробку. Запропоноване програмне забезпечення ділиться на загальне програмне забезпечення, що поставляється із засобами обчислювальної техніки й спеціальне програмне забезпечення, що спеціально розроблене для даної конкретної системи й включає програми, що реалізують її функції. Даються необхідні рекомендації з установки розробленого програмного забезпечення. Для підвищення рівня безпеки запропоновано застосовувати алгоритм Madryga.

Список літератури

1. Tanenbaum A.S. Computer Networks. Third edition, Prentice-Hall, New Jersey, 1996.
2. Jacobson V. Congestion Avoidance and Control. // ACM SIGCOMM'88. 1988.
3. Holzmann G. Design and Validation of Computer Protocols. Prentice Hall, New Jersey, 1991.
4. Postel J. Transmission Control Protocol. // RFC793 (STD7). 1981.
5. Braden R. T. Requirements for Internet Hosts – Communication Layers. // RFC1122. 1989.
6. Jacobson V., Braden R., Borman D. TCP Extensions for High Performance. // RFC1323. 1992.
7. Karn P., Partridge C. Estimating Round-trip Times in Reliable Transport Protocols. // ACM SIGCOMM'87. 1987.
8. 8. Nagle J. Congestion Control in IP/TCP Networks. // ARPANET Working Group Requests for Comment (RFC-896), DDN Network Information Center, SRI International, Menlo Park, CA. 1984.
9. Бертсекас Д., Галлагер Р. Сети передачи данных. Пер. с англ. М., Мир. 1989.
10. George F., Young G. SNA Flow Control: Architecture and Implementation. // IBM System Journal, vol. 21, no. 2. – 1982. – pp. 179-210.

УДК 004

Р. Самойленко, магістр гр. КІ-18М-1,4
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ ГЕОПАРАМЕТРИЧНОГО МОНІТОРИНГУ ВІДДАЛЕНИХ ОБ`ЄКТІВ КОРИСТУВАЧА

У статті розроблено програмне забезпечення, яке призначено для системи геопараметричного моніторингу віддалених об`єктів користувача. Метою розробки є дослідження та програмна реалізація системи геопараметричного моніторингу віддалених об`єктів користувача. Об'єктом дослідження є процес геопараметричного моніторингу віддалених об`єктів користувача. Предметом дослідження є методи геопараметричного моніторингу віддалених об`єктів користувача. Методи дослідження базуються на методах геопозиціонува́ння, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи геопараметричного моніторингу віддалених об`єктів користувача. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.
комп'ютерна інженерія, геопараметричний моніторинг, віддалені об`єкти користувача

Постановка проблеми. Одним із сучасних досягнень науково-технічного прогресу є розроблена система GPS, за допомогою якої будь-яка людина може визначити свої координати, а пілот посадити літак у зоні з нульовою видимістю.

Можливості системи глобального позиціонування з роками розширюються. Користувач може визначати свої координати з точністю практично до метра. Можливості системи GPS будуть розширюватися за рахунок модернізації, що припускає: введення додаткових каналів сигналу на супутнику, збільшення потужності сигналу й удосконалення

системи його корекції, використання спрямованих антен, а також інтеграцію з телевізійними й телефонними стільниковими мережами. За допомогою GPS літаки можуть приземлятися в повній темряві. Найближчим часом GPS допоможе контролювати рух автомобільного транспорту, забезпечуючи безпеку дорожнього руху, удосконалена система зможе бути застосована в електроенергетиці, у телекомунікаціях, при видобутку корисних копалин, картографії й навіть у сільському господарстві.

Якщо провести огляд сучасних систем GPS, то ми побачимо, що провідні світові держави мають свої супутникові системи, які забезпечують роботу приймача GPS. У США це система Navstar, у Росії – Glonass, у Європейському Союзі – Galileo. В зв'язку з тим, що Україна поки не розвертає свою систему супутників для реалізації системи GPS, то актуальним буде розробка вітчизняного програмного забезпечення даної системи.

У такий спосіб актуальним є завдання розробки системного програмного забезпечення яке буде використовувати GPS для пошуку поточного положення об'єктів.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи геопараметричного моніторингу віддалених об`єктів користувача.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи геопараметричного моніторингу віддалених об`єктів користувача.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем геопараметричного моніторингу віддалених об`єктів користувача.

– Дослідження системи геопараметричного моніторингу віддалених об`єктів користувача.

– Програмна реалізація системи геопараметричного моніторингу віддалених об`єктів користувача.

Об'єктом дослідження є процес геопараметричного моніторингу віддалених об`єктів користувача.

Предметом дослідження є методи геопараметричного моніторингу віддалених об`єктів користувача.

Методи дослідження базуються на методах геопозиціонува́ння, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Швидкість передачі даних в першу чергу залежіть від часу «старту» необхідному навігаційному приймачу на визначення позиції після включення. Це залежить від наявної в пам'яті початкової інформації. Виділяються наступні режими:

– «Холодний» старт («автопошук») – час, позиція, альманах і ефемериди невідомі;

– «Теплий» старт – позиція й ефемериди невідомі, час і альманах відомі;

– «Гарячий» старт («перезахват») – альманах, ефемериди відомі, час і позиція відомі з деякою помилкою.

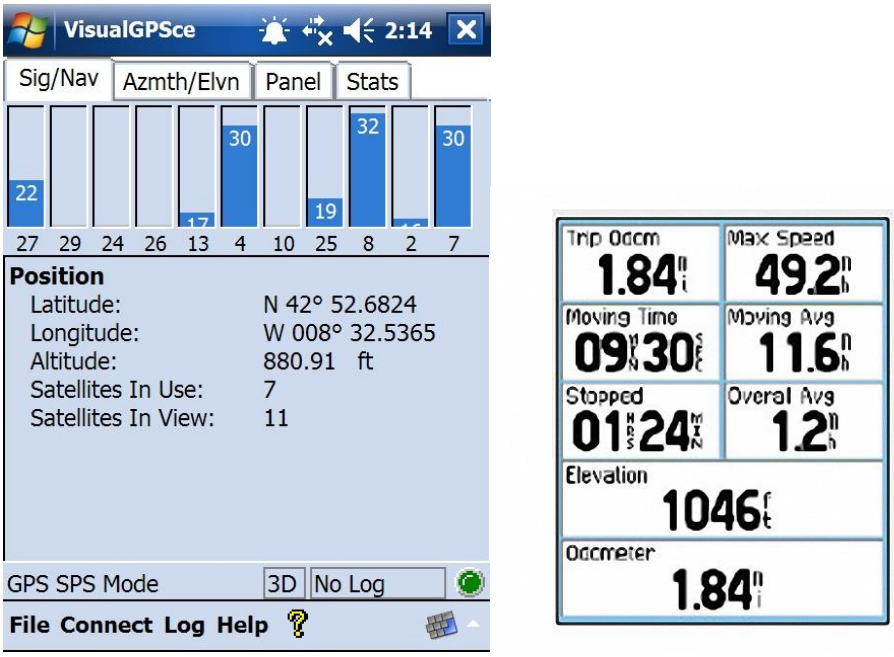


Рисунок 1 – Робота GPS у пристроях: кількість підключених супутників; поточне положення

Навігаційні повідомлення передані із супутників містять два типи даних – ефемериди й альманах супутників. В альманасі передаються параметри орбіти, за допомогою яких можна обчислити зразкове місцерозташування супутників з достатньо великим ступенем погрішності. Альманах, що зберігається в пам'яті приймача, постійно обновляється, тому що кожний супутник передає дані альманаху для всіх супутників угруповання. Час «життя» альманаху становить 2-3 місяці. Далі, величина накопиченої помилки в розрахунках буде неприпустимою.

Дані ефемерид містять параметри, що дозволяють більш точно обчислити поточне місце розташування супутників. На відміну від альманаху, кожний із супутників передає, тільки свої власні ефемериди. Час «життя» ефемерид не перевищує 4-6 годин.

Інформація даних ефемерид і альманаху, передана із супутників, постійно коректується. Це відбувається один раз у добу. Мережа наземних станцій, одержує інформацію із супутників, за аналогією зі звичайними користувачами, аналізує виміри, порівнює їх з опорними, розраховує коригувальні виправлення й передає їх на головну станцію, з якої здійснюється передача даних на супутники.

«Холодний» старт приймача може бути зв'язаний не тільки з його тривалою бездіяльністю, але переміщенням на велику відстань у виключеному стані. Якщо перший випадок пов'язаний із застарілим альманахом і помилкою у визначенні поточного точного часу, то в другому випадку приймач, не знаючи про своє переміщення, буде намагатися знайти супутники, яких повинні бути видимі на «старому» місці. Користувач може «допомогти» приймачу й зменшити час «холодного» старту, указавши на базовій карті зразкове «нове» місце розташування. Під час «холодного» старту приймач сканує весь діапазон можливих значень частот і часових затримок навігаційних сигналів. При цьому, у багатоканальних приймачах, кілька каналів можуть використовуватися для пошуку одного супутника, щоб прискорити час його захвата. Після того, як сигнал хоча б від одного супутника буде отриманий і розібраний, приймач буде мати повну інформацію про альманах всього угруповання й, по суті, перейде до «теплого» старту.

При «теплому» старті, приймач, включений після 6-и годин бездіяльності, почне «пошук» сигналів супутників, використовуючи значення поточного часу й дані, що зберігаються в пам'яті, альманаху. Буде здійснюватися пошук тільки тих супутників, які, по теоретичних розрахунках перебувають у видимій півкулі й повинні бути доступні приймачу. Відповідно, відомий досить вузький діапазон частот і часових затримок, що потрібно

просканувати у процесі пошуку сигналів. Ця інформація істотно прискорює час захвата супутників, у порівнянні з «холодним» стартом, коли пошук ведеться на широкому діапазоні всіх можливих значень затримок і частот.

Варто відзначити, що в момент включення, багатоканального приймача починає пошук сигналів з декількох супутників одночасно. Інформація передана із супутників прив'язана до єдиної шкали часу, містить однакову структуру й досягає антени приймача, приблизно в один й той же час. Тому дані ефемерид, одночасно захоплених супутників, надійдуть у приймач майже що одночасно. Якщо кількість таких супутників більше або рівняється трьом, то це дозволяє приймачу відразу ж розрахувати позицію. У випадку, коли сигнали блокуються перешкодами, то може знадобитися досить тривалий час на визначення позиції.

Наявність повністю отриманих ефемерид не гарантує використання цього супутника у підрахунку позиції. Інформація передана в ефемеридах може бути неправильною, помилковою, або пов'язаною з несправністю в роботі супутника. Це може бути зв'язано не тільки з несправністю супутника, але й діагностичними роботами проведеними на його борті, процесом уведення його в експлуатацію або тестуванням нових режимів.

«Гарячий» старт пов'язаний з короткочасним вимиканням приймача (до 6-и годин) не вимагає тривалого часу на визначення позиції. Це пояснюється тим, що отримані раніше ефемериди містять «свіжі» дані, використовувані для визначення точних координат супутників і можуть використовувати в обчисленні позиції. У випадку включення приладу після граничного часу, ефемериди розглядаються застарілими й починає діяти принцип «теплого» старту. Якщо на момент включення приймача видимими залишилися менш 3-х супутників з «свіжими» ефемеридами, то для визначення позиції буде потрібно якийсь час на збір даних ефемерид нового супутника.

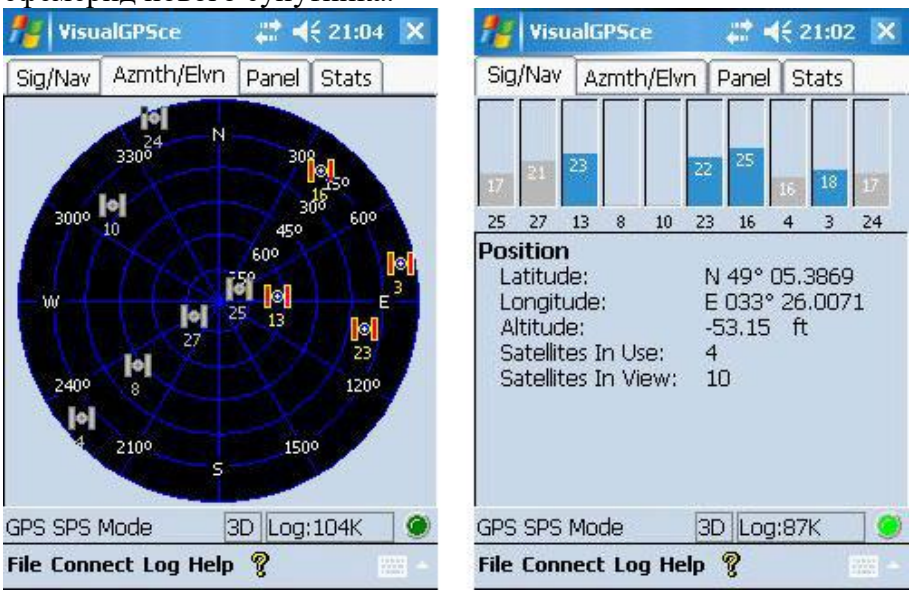


Рисунок 2 – Поточне положення супутників

Дані ефемерид передаються в складі трьох пакетів. Кожний з пакетів містить однаковий часовий ідентифікатор (IOD – issue of data) по якому можна об'єднати загальну інформацію. Інформація ефемерид передана із супутників кожні 30 секунд, змінюється раз в 2 години, і містить однаковий на цей час IOD. Якщо один з пакетів був пропущений, або отриманий з помилками, то можна виділити аналогічний пакет з наступного повідомлення, перевірити його ідентифікатор і не чекаючи наступних пакетів, використовувати його з раніше отриманими. Це дозволяє приймачу прискорити час «старту».

Існує мінімальний можливий час, необхідний приймачу на «старт», і це визначається структурою переданого сигналу із супутників. Виробники навігаційної апаратури, використовуючи стандартні методи навігації, можуть наблизитися до цього часу, але

зменшити його не зможуть. Одним з методів, призначених для рішення цієї проблеми, є Assisted-GPS (A-GPS). Його принцип полягає в обчислення точного місця розташування супутників без інформації ефемерид, на одержанні яких потрібен час. Обчислення здійснюється на використанні точних моделей орбіт супутників, доступних через спеціальні Інтернет – сервіси.

З іншого боку, максимальний час «старту» може значно перевищувати заявлене в технічній специфікації на навігатор час. Це пояснюється навколишніми умовами, у яких відбувається «захват» супутників і «старт» приймача. Якщо приймач перебуває в умовах сильних фізичних перешкод, то навігаційний сигнал піддається зовнішньому впливу, містить помилки й неправильно декодується. Більше, того геометричний фактор цих супутників, що є одним із критеріїв точно визначення позиції, сильно погіршується. Всі ці умови можуть значно збільшити час «старту» приймача.

Показник CEP – окружність можливої помилки (Circular Error of Probability) один з можливих шляхів оцінити точність вироблених GPS вимірів у даній точці тепер. Завдяки великій кількості факторів зовнішнього середовища впливаючих на виміри – в одній точці показання приладу будуть різними в різні моменти часу. До таких факторів відносяться вплив іоносфери, вплив нижніх шарів атмосфери, багатопроменевість, наявність перешкод на шляху сигналу. Показник CEP використовує опорну точку, або задаваєму користувачем, або що обчислюється як середнє геометричне між всіма вимірами, для того, щоб побудувати серію кіл що показують відповідно 50, 90, 95, 99% можливої помилки.

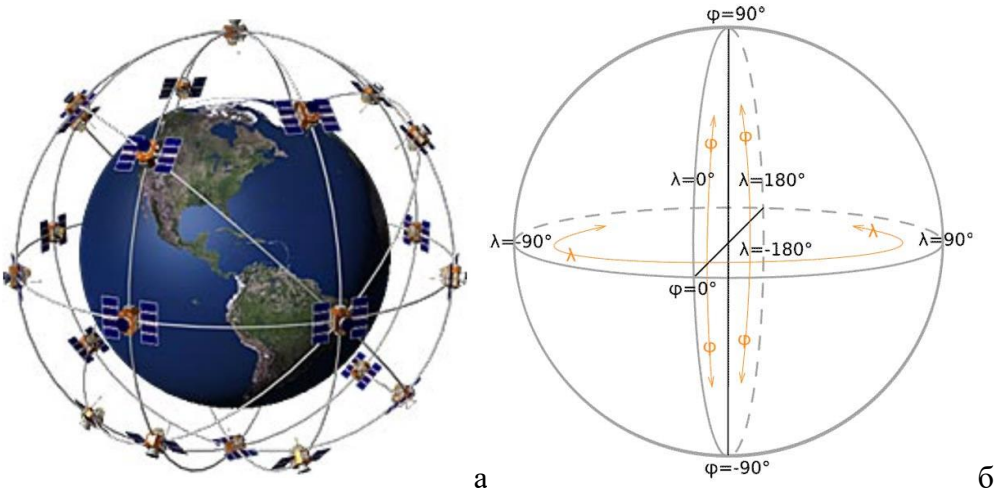
Для того, щоб визначити CEP повинна бути взята серія вимірів, зроблена в одній точці. Наприклад, включений і нерухливий GPS з інтервалом в 2-5 секунд реєструє точки треку, які потім завантажуються, конвертуються в shape-файл і аналізуються.

Очевидна регулярність розташування точок пов'язана з роздільною здатністю цифрових значень видаваних GPS. Наприклад точність із якої GPS Garmin 12 видає координати – 0.000005 десяткових градусів по довготі, і 0.000005 по широті.

Для обчислення CEP дані повинні бути спроектовані. Для обчислення виміряються відстані між середньою точкою й кожним виміром, а потім вираховується на якій відстані перебуває потрібний відсоток точок.

Результати обчислення CEP 4 різних окружностей: Average = 6.999e+006 5.82936e+006, SD = 7.00012e+006 5.83025e+006, Circular Error Probabilities (CEP), 50% = 3.42281, 90% = 7.36774, 95% = 9.52791, 98% = 14.2946.

Приклад показує, що 50% точок перебувають на відстані 3.4 метра від середнього значення, 98% точок на відстані 14.2 метра від середнього. З діаграми також видний розкид помилки.



а б

Рисунок 3 – Обчислення положення: а – орбіти супутників; б – система координат розрахунку

На рисунку 3 а, показання 3-х 40-хвилинних сесій прийому координат, по 1022 виміри через 2 сек у сесії (усього 3066 вимірів).

На рисунку 3.3 б, обчислені значення CEP (50, 90, 95, 98), щодо середнього значення (чорна точка в центрі), графік являє собою візуальне подання обчислених значень CEP (різним кольором показані різні серії вимірів, усього 3 серії).

На даний момент існує, як мінімум, три найбільш затребувані способи спільного використання GPS і КПК.

По-перше, до наладоника можна докупити опціональний модуль. Останній може помітно розрізнятися по способу сполучення, але в основному найбільш популярні зараз карткова модифікація й Bluetooth-варіант. Перший не дуже зручний через те, що займає один або єдиний слот розширення, зате відносно дешевий, ну а другий цілком ергономічний – не прийдеться піклуватися про точне позиціонування, от тільки ціна його, як правило, досить висока.

Другим способом є збагатити наладоник GPS-функціями при їхній відсутності в штаті, це є з'єднання звичайного навігатора й КПК за допомогою спеціального кабелю. Подібний варіант гарний своєю роздільністю й повноцінністю GPS-частини: при відсутності потреби в КПК можна відправлятися в дорогу лише з навігатором, не обтяжуючи себе додатковою ношею.

Рисунок 4 – Навігаційні прилади GPS

Ну й по-третє, існує можливість сполучити обоє пристрої в одному корпусі, одержавши КПК із інтегрованим модулем GPS. Пристрій значно мобільніший багатьох персональних GPS-навігаторів. При цьому кишенькові комп'ютери мають відмінний кольоровий екран, про яке спеціалізовані приймачі можуть тільки мріяти. Дисплеям наладоників властива чутливість до натискань, більш по мірках навігаторів розміри, порівняно високий дозвіл, багата палітра кольорів і т.д. Загалом, звичайні приймачі програють по всіх статтях, будучи оснащені несенсорним, часто монохромним екраном зі скромними характеристиками й досить високою інертністю.

Зовнішністю КПК, як правило, наділені більш привабливою, ніж навігатори. Правда, у подорожі це навряд чи придасться, а от відсутність у корпусів наладоників водонепроникності, а також їхні слабкі характеристики до фізичних навантажень досить недоречні.

Рисунок 5 – Фізично захищений GPS прилад

Функціональність GPS-приймача – одна з основних якостей подібних пристроїв. Тому спеціалізовані пристрої настільки популярні: вони націлені виробником на навігацію, а тому мають весь базис необхідних функцій.

GPS-здатності КПК звичайно не забезпечені програмним комплектом. Як правило, користувачеві доводиться самому завантажувати потрібне.

Якщо розглядати апаратну половинку КПК із GPS і персонального навігатора, то базових розходжень тут мало – звичайно приймачі так само, як і КПК мають 12-ти канальність і підтримку WAAS, а також інші основні характеристиками. Зате опціональності в наладоників відсутні.

– Ще одна перевага КПК з інтегрованим навігаційним модулем перед звичайними GPS-приймачами – наявність слота розширення, а точніше, підтримка SDIO, тобто здатність працювати з периферією. Подібний дріб'язок додасть наладонику функціональності, оскільки дозволить взяти в подорож, скажемо, камеру, Bluetooth-адаптер або GSM-модуль, а також багато чого іншого – на сьогоднішній день спектр доступного устаткування досить великий, і кожний зможе вибрати щось цікаве й корисне конкретно для себе. GPS-навігатори, як правило, позбавлені подібної можливості, а роздільні набори GPS і КПК не занадто зручні, оскільки далеко не всі наладоники оснащені двома слотами розширення.

Розробка структурної схеми

Структурна схема роботи системи зображена на рисунку 3.6. На ній показано структуру взаємодії адміністратора сервера стеження за користувачами пристроїв. Під час руху чи роботи пристрою в цілому програма на пристрої намагається знайти супутники та при їх знайдені проводить таємну передачу поточних координат приладу через межу Інтернет на сервер.

Після отримання цих даних, які називаються «Мітка геокодування», адміністратор через безкоштовні карти Яндекс та Google знаходить поточну позицію приладу і при необхідності може його відшукати якщо пристрій буде зв’язаний з Інтернет мережею постійно.

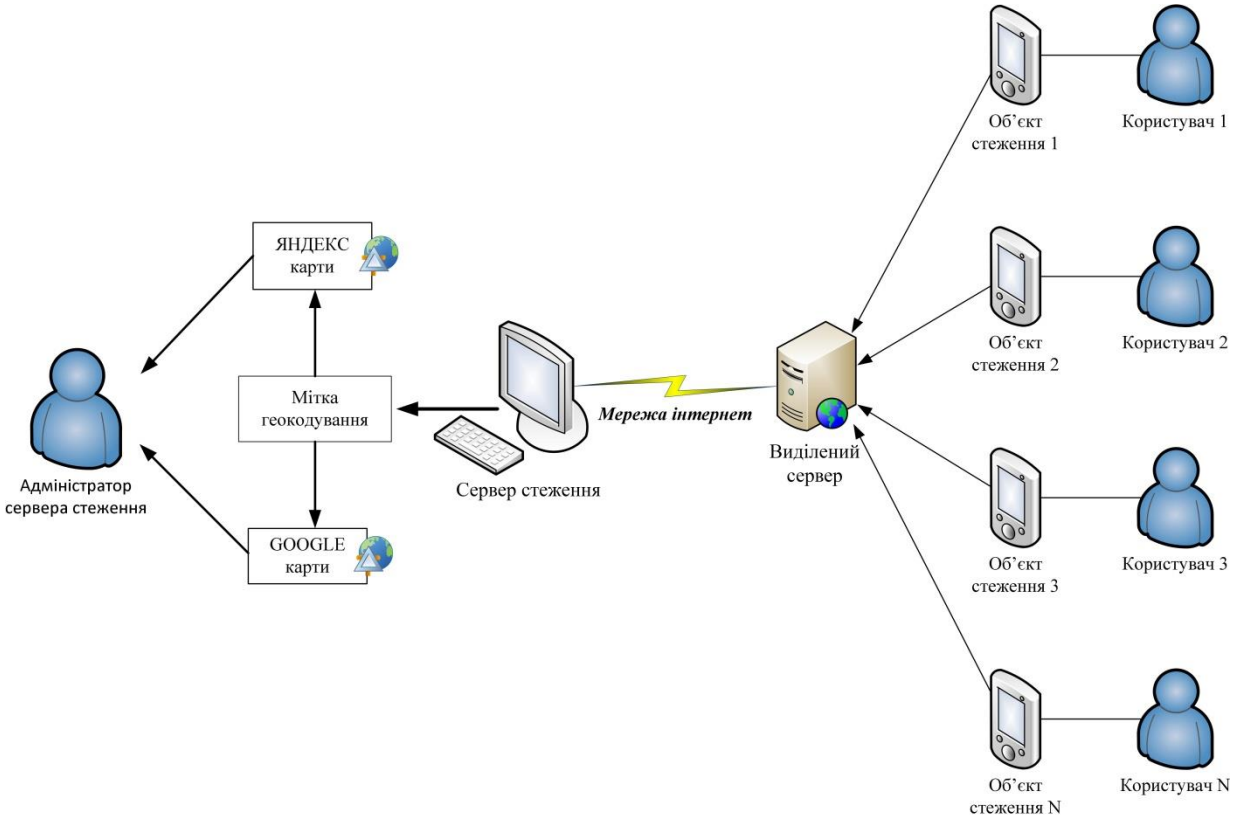


Рисунок 6 – Структурна схема роботи системи

Мітка геокодування позначає місце на карті за допомогою значка. За замовчуванням використовується стандартний значок, однак його завжди можна замінити на будь-який інший.

Мітки інтерактивні й реагують на події миші. За замовчуванням при клацанні кнопкою миші по мітці, відкривається вспливаюче вікно.

Утримуючи кнопку миші, мітку можна пересувати по карті (цю можливість необхідно включити).

Щоб додати мітку на карту необхідно передати в конструктор класу Ymaps.Placemark координати точки її прив'язки й список параметрів, а потім за допомогою методу карти addoverlay() додати мітку на карту.

На рисунку 7 зображена структурна схема пошуку пристроїв.

```
// Створює мітку в центрі Кіровограда
var placemark = new Ymaps.Placemark(new
Ymaps.Geopoint(37.609218,55.753559));
// Всстановлює точку
placemark.name = "Кіровоград";
placemark.description = "Центр України";
// Додає мітку на карту
map.addoverlay(placemark);
```

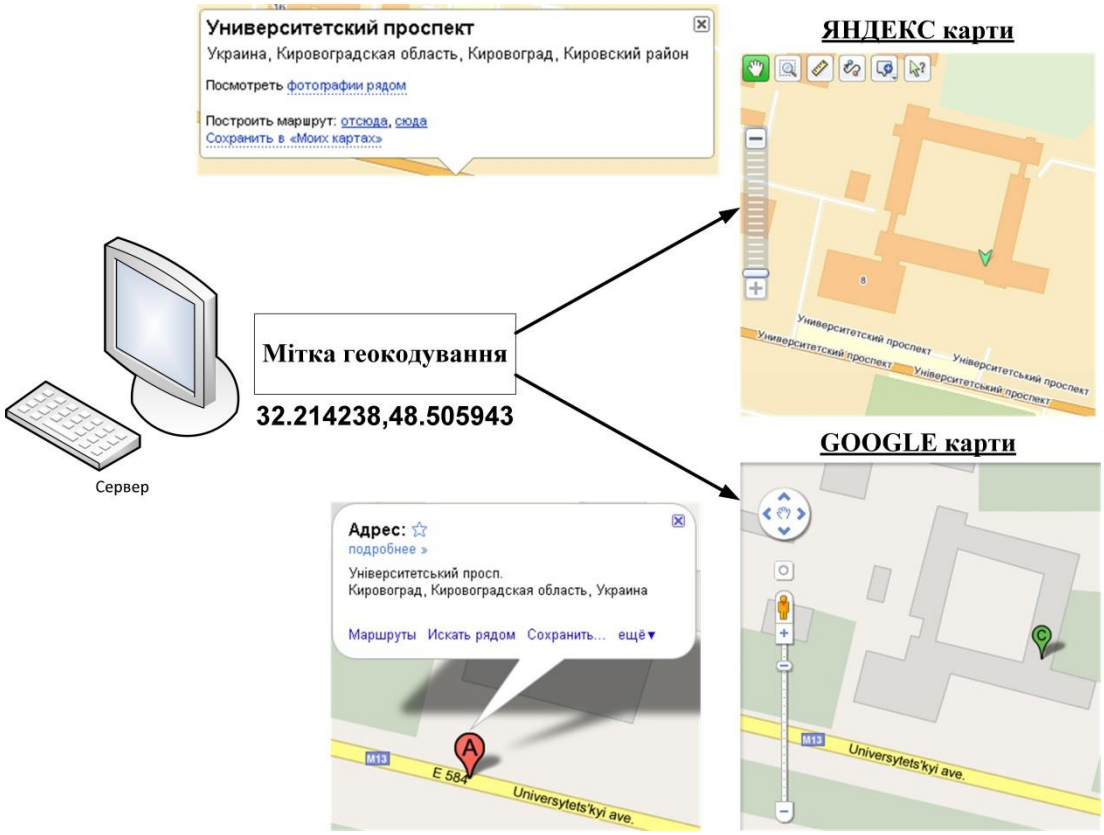


Рисунок 7 – Структурна схема пошуку пристрою

Висновок. У статті розглянуто та проаналізовано програмне забезпечення, яке призначено для системи геопараметричного моніторингу віддалених об`єктів користувача. В межах України в недостатній мірі представлені вітчизняні розробки в цій області. У роботі наведені теоретичне узагальнення й рішення наукового завдання дослідження методів геопараметричного моніторингу віддалених об`єктів користувача. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем геопараметричного моніторингу віддалених об`єктів користувача; Досліджена система геопараметричного моніторингу віддалених об`єктів користувача; На основі отриманих результатів досліджень створена програмна реалізація системи геопараметричного моніторингу віддалених об`єктів користувача. Розроблені під час виконання роботи алгоритми дозволяють успішно вирішувати завдання геопараметричного моніторингу віддалених об`єктів користувача. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки. Розроблене програмне забезпечення має простий, дружній та зручний інтерфейс користувача, що забезпечує легкість у освоєнні роботи програмного продукту, зручність у використанні, і не потребує особливих спеціальних знань. При створені програмного забезпечення було використано об’єктно-орієнтований підхід, що відповідає сучасним тенденціям у галузі розробки комерційних програмних систем. Програма реалізована на мові високого рівня Delphi 2010. Дана мова програмування дозволяє найбільш ефективно обробляти дані. Це дозволило мінімізувати строк розробки програмного забезпечення, і, як слід, зменшити витрати на його розробку. Запропоноване програмне забезпечення ділиться на загальне програмне забезпечення, що поставляється із засобами обчислювальної техніки й спеціальне програмне забезпечення, що спеціально розроблене для даної конкретної системи й включає програми, що реалізують її функції. Даються необхідні рекомендації з установки розробленого програмного забезпечення. Для підвищення рівня безпеки запропоновано застосовувати алгоритм RSA.

Список літератури

1. Дреев А.Н. Использование неравномерного распределения единичных битов для дополнительного сжатия SPIHT кода / А.Н. Дреев, А.А. Смирнов // Информационные системы в управлении, образовании, промышленности: монография. Под редакцией профессора В.С. Пономаренко. – Х.: Вид-во ТОВ «Щедра садиба плюс», 2014. – С. 498.
2. Дрєєв О.М. Дослідження впливу шляху розгортки на ступінь ентропійного стиснення цифрового зображення / О.М. Дрєєв, О.В. Слюсар // Збірник наукових праць Кіровоградського національного технічного університету. Техніка в сільськогосподарському виробництві, галузеве машинобудування, автоматизація. Випуск 21. – Кіровоград: КНТУ. – 2008 – С. 115-118.
3. Дрєєв О.М. Метод розвантаження телекомунікаційного сервера за рахунок кешування зображень / О.М. Дрєєв // Збірник наукових праць Кіровоградського національного технічного університету. Техніка в сільськогосподарському виробництві, галузеве машинобудування, автоматизація. Випуск 25. Ч. І. – Кіровоград: КНТУ. – 2012 – С. 419-424.
4. Дрєєв О.М. Метод прогнозування завантаженості серверу телекомунікаційної мережі / О.М. Дрєєв, О.А. Смірнов, Є.В. Мелешко, О.В. Коваленко // Системи обробки інформації. Випуск 3(101) Том 2. – Х.: ХУПС. – 2012. – С. 181-188.
5. Дрєєв О.М. Оцінка якості стиснення зображень на основі дискретного перетворення Хартлі / О.В. Коваленко, О.П. Доренський, О.М. Дрєєв // Системи озброєння і військова техніка. Науковий журнал 2(34) – Х.: ХУПС – 2013. С. 99-102.
6. Дрєєв О.М. Дослідження впливу ступеня стиснення зображень на оперативність їх доставки у телекомунікаційній системі / О.А. Смірнов, О.М. Дрєєв, О.П. Доренський // Збірник наукових праць "Системи обробки інформації". – Випуск 8(115). – Х.: ХУПС – 2013. – С. 234-239.
7. Дреев А.Н. Сравнение битовых плотностей при использовании различных методов кодирования информации / А.Н. Дреев, А.А. Смирнов // Системи обробки інформації, 2014, випуск 2 (118), том 2 – Харків: ХУПС – 2014. С 64-66.
8. Дрєєв О.М. Моделювання впливу інтенсивності трафіку на оперативність доставляння інформації / О.М. Дрєєв // Науково-виробничій журнал "Зв'язок". – Київ: ДУТ, 2014. – № 2 (108) С. 24-29.
9. Дреев А.Н. Повышение вероятности доставки сообщений в телекоммуникационных системах и сетях для обеспечения информационной безопасности / А.Н. Дреев, А.А. Смирнов //«Безпека інформації» Том 21, №1 2015 р. – Київ: НАУ – 2015. – С. 22-28.
10. Дрєєв О.М. Узагальнення вейвлету Хаара / О.М. Дрєєв, Г.М. Дрєєва // Збірник тез доповідей Комбінаторні конфігурації та їх застосування, 15-16 жовтня 2010 р. – Кіровоград – С. 58.

УДК 004

А. Сахарова, магістр гр. КІ-18М-1,4
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ МОНІТОРИНГУ РОБОТИ ТАЙМ-КЛУБУ

У статті розроблено програмне забезпечення, яке призначено для системи моніторингу роботи тайм-клубу. Метою розробки є дослідження та програмна реалізація системи моніторингу роботи тайм-клубу. Об'єктом дослідження є процес моніторингу роботи тайм-клубу. Предметом дослідження є методи моніторингу роботи тайм-клубу. Методи дослідження базуються на методах оптимізації, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи моніторингу роботи тайм-клубу. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.
комп'ютерна інженерія, моніторинг, тайм-клуб

Постановка проблеми. У зв'язку з розширенням та розповсюдженістю ЕОМ не вимагає зусиль розрахувати статистику зростання потреби у покращенні технологій та удосконаленню передачі даних. Певний ряд додатків, які мають необхідність у системах

зв'язку, можуть спростити та пришвидшити розуміння основних проблем, що пов'язані з мережами зв'язку та виявити методи їх усунення.

На даний час наявна велика кількість додатків, що вимагають ізольованого доступу до баз даних. Досить поширеними прикладами слугують інформаційні і фінансові служби, доступні користувачам персональних ЕОМ, що поширилися у різних сферах діяльності.

Варто відмітити також є багато додатків, що вимагають дистанційного відновлення баз даних, яке в свою чергу може сполучитися з доступом до даних. Приклад: апаратури автоматичного підрахунку голосів, системи керування інвентаризацією, система резервування авіаквитків і т.д.

В багатьох застосунках подібного типу є широкий географічно розподілених пунктів, у яких потрібні вхідні дані. Також є одним широко відомим додатком слугує електронна пошта, для людей, що надають переваги у користуванні мережею. Такий додаток дає змогу використовувати пошту, читати, заносити у файл, розповсюджувати між інших користувачів, доповнюючи її коментарями або читати знаходячись у різних точках мережі. Звичайно, така служба має багато переваг у порівнянні з традиційною поштою з погляду ефективності у передачі та доставки і гнучкості у її функціонуванні.

Для промисловості засобам зв'язку та передачі даних приділяється куди більше уваги, так як ця система дає змогу виконувати передачу даних на великі відстані. Як сфера економічної діяльності індустрія глобальних мереж (далі ГМ) розвивається і посідає досить вагоме місце.

Для загального числа користувачі, локальні мережі (далі ЛМ) є достатньо новою областю засобів передачі даних. Тоді як у промисловості виробництва ЛМ розвивалася з разючою швидкістю за останній час. Внесення змін та впровадження локальних мереж пояснюється в основному підвищенням ефективності та покращенням продуктивності персоналу, що підтверджує ефективність рішень.

Дана мета встановлюється фірмами-постачальниками ЛМ та керівництвом установ і розроблювачами ЛМ, як необхідний крок у покращенні промислових комплексів. Застосування та експлуатація ЛМ дозволяє спростити доступ до пристроїв та кінцевого обладнання даних (далі ООД), встановленим на підприємстві. Пристрої даного типу не тільки ЕОМ (персональні, міні– і великі ЕОМ), але й інші різновиди, що застосовуються в установах, приклад: принтери, графобудівники, сканери, та інше. Все зростаюче число електронних пристроїв збереження, обробки, передачі файлів і баз даних.

Локальна мережа представляють собою канал та ряд протоколів обміну даними для здійснення зв'язку з робочими станціями і ЕОМ. На сьогодні велика кількість організацій, прагнуть слідувати загальноприйнятим протоколам, в результаті міжнародних зусиль, що спрямовані на прийняття стандартів, які рекомендуються для промислових галузей.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи моніторингу роботи тайм-клубу.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи моніторингу роботи тайм-клубу.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

- Огляд існуючих систем моніторингу роботи тайм-клубу.
- Дослідження системи моніторингу роботи тайм-клубу.
- Програмна реалізація системи моніторингу роботи тайм-клубу.

Об'єктом дослідження є процес моніторингу роботи тайм-клубу.

Предметом дослідження є методи моніторингу роботи тайм-клубу.

Методи дослідження базуються на методах оптимізації, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу.

Створення тайм-клубу на базі ОС Linux

При розробці тайм-клубу одним з головних завдань був вибір ОС, яка буде використовуватись, цей аспект впливає практично на весь процес організації процесу розробки – обладнання та програми, які будуть використовуватись, організацію мережі. Саме тому необхідно розглянути дві основні платформи, Linux та Windows. Організація тайм-клубу можлива в обох випадках. Тому розглянемо, які з переваг дає використання Linux.

Структуру Linux найлегше представити у вигляді двох шарів.

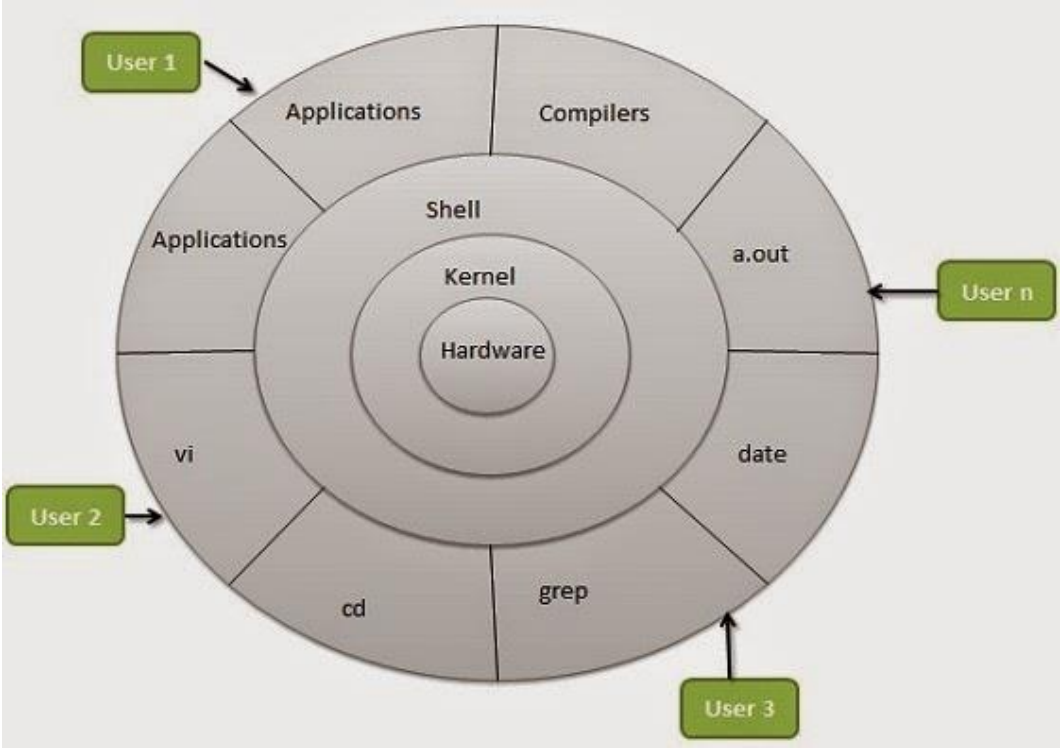


Рисунок 1 – Архітектура Linux

Перший є ядро, воно безпосередньо взаємодіє з залізом та забезпечує роботу всього іншого ПЗ на комп'ютери з різним апаратним забезпеченням. В свою чергу ядро надає програмам визначений набір системних API, за допомогою яких виконується створення процесів, керування ними, їх взаємодія та синхронізація, також файлове введення/виведення.

Другий є саме програмне забезпечення, прикладне або системне: командний інтерпретатор, графічна оболонка і т.д.

Розглянемо більш детально ядро системи. Воно дозволяє всім іншим програмам спілкуватися з периферійними пристроями, надає та регулює доступ до файлів, керує пам’яттю та процесами.

Ядро – це зв'язковий, до якого звертаються за допомогою системних викликів, зв'язок цей не однобічний: ядро може і повертати в разі потреби деякі дані. Основною перевагою ядра жорстка стандартизація системних API. Завдяки цьому багато в чому досягається переносність коду між різними версіями Linux і абсолютно різним апаратним забезпеченням.

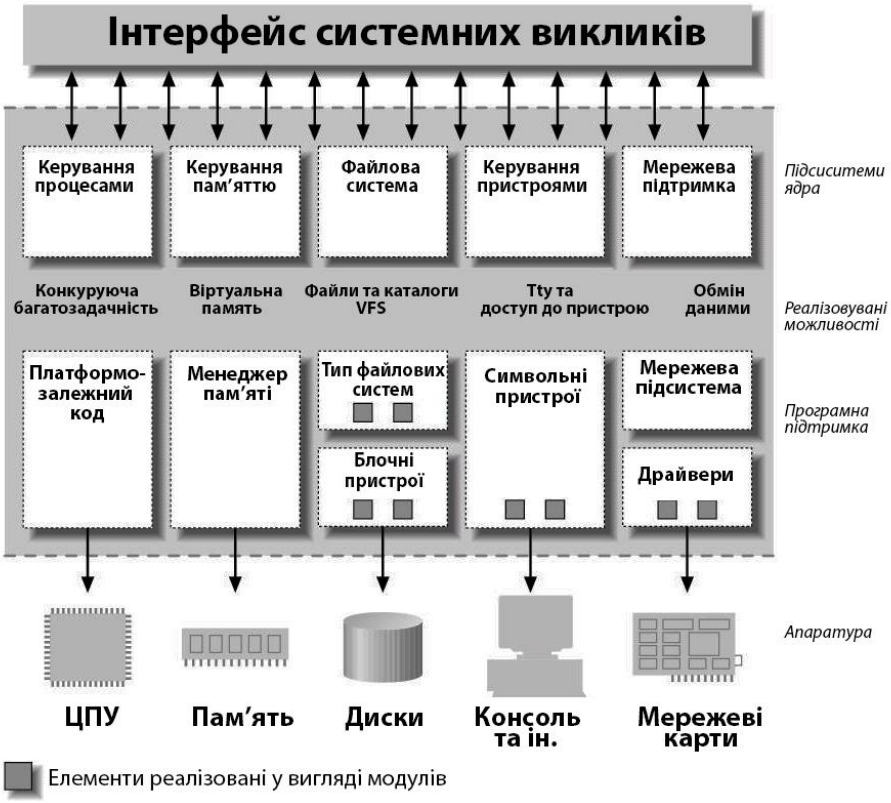


Рисунок 2 – Будова ядра Linux

Звертання до ядра системи можна розділити на дві групи: програма викликає підсистему керування файлами або підсистему керування процесами. Перша відповідає за усе, що зв'язано з файлами: керування, розміщення, доступ.

Процеси – це у загальному випадку, будь-які запущені програми, тому підсистема керування процесами служить для їх життєздатності, синхронізації та керування. Також важливо і те, що файлова підсистема і підсистема керування процесів можуть спілкуватися один з одним, а саме: будь-який процес може викликати системні API для роботи з файлами. Перевага Linux полягає в тому, що ці API універсальні (та й у Windows спостерігається те саме). Найголовніші серед них: open, close, read, write, stat, chown, chmod (зміст майже усіх викликів інтуїтивно зрозумілий з назви, окрім останніх трьох, що служать для керування атрибутами файлів, прав доступу та інформації про власника) та ін. Системні виклики у програмі мовою С є звичайною функцією, інформацію з кожного з них можна запросто знайти в man. Підсистема керування файлами – майже єдина з усіх працює з драйверами, які є модулями ядра. Чим характеризується деяка вибірковість, так це тим що є ще і мережна підсистема, яка працює, наприклад: із драйвером мережної карти; з драйверами різних сучасних мережних пристроїв. Робота обміну даними з драйверами може проходити двома способами: за допомогою буфера чи потоку. Суть першого методу, це інформація, яка виділяється в кеш, у який заноситься необхідний блок даних. Потів інформація з кеша передається до драйвера.

Драйвер – це єдиний елемент ядра, здатний виконувати керування периферійними пристроями. Однак підсистема керування файлами може взаємодіяти з драйвером і через потік, що в свою чергу потік, являє собою по символьну передачу даних драйверові. Слід звернути увагу, що спосіб взаємодії з драйвером визначається не користувачем й не додатком, він є характеристикою того пристрою, яким керує драйвер. Зрозуміло, що потокова взаємодія дозволяє більш ефективно та швидко передавати дані, ніж спілкування через буфер. Так як на заповнення буфера витрачається час, тому й зростає час відгуку.

Тут більш глибоко розглянемо підсистему керування процесами. Вона відповідає за синхронізацію та взаємодію процесів, планування виконання процесів, розподіл пам'яті. Для

даних цих цілей у підсистему керування процесами включені три модулі. Прикладом взаємодії підсистем керування файлами і процесами можна навести завантаження файлу на виконання. В такому випадку підсистемі керування процесів потрібно звернутися до колеги, для того щоб прийняти файли, що виконуються. Тепер розглянемо виклики, які слугують для роботи з процесами: exec (виконує процес), fork (створює новий процесу), wait (один зі способів синхронізації), exit (завершує виконання процесу), brk (керує пам'яттю, виділеної процесові), signal (оброблювачі виключень) і ін. Наступні два модулі є важливими в розумінні всієї підсистеми керування процесами. Перший модуль, розподілює пам'ять, дозволяє уникнути недостачі оперативної пам'яті, хоча механізм свопінгу та файлів підкачування (технічно правильно, тобто називається віртуальною пам'яттю), в тіні зостається лише інший факт: операційна система в особі описуваної підсистеми, може або скидати всі дані, що відносяться до конкретного процесу, на диск, або скидати сторінки пам'яті, так зване сторінкове заміщення. Отже, модуль розподілу пам'яті виконують дуже важливу функцію – визначають якому процесові скільки виділити пам'яті.

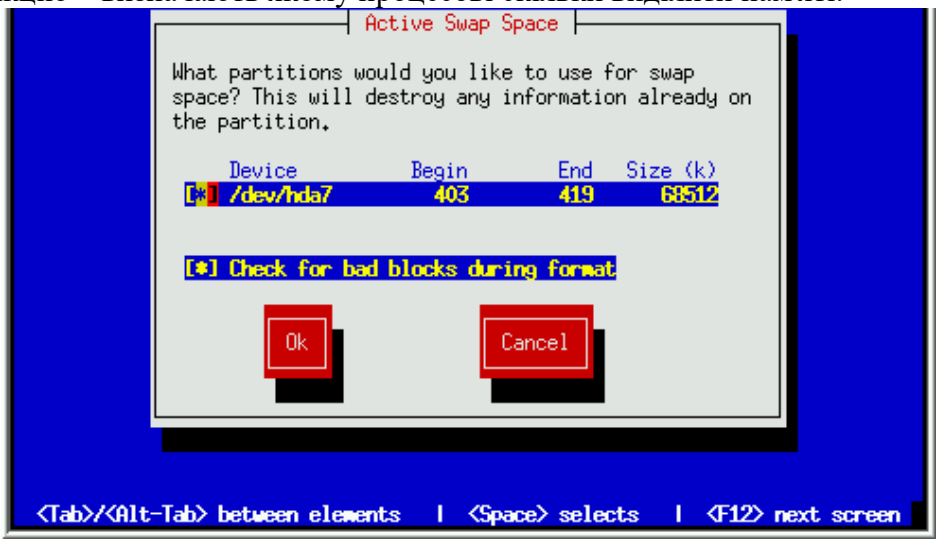


Рисунок 3 – Механізм свопингу

Підчас запуску, програма завантажується з якогось накопичувача в оперативну пам'ять. У випадку якщо програма не міститься в ОЗП, то частини її, що у даний момент не виконуються, будуть зберігатися у вторинному запам'ятовуючому пристрої, зазвичай у вінчестері, й така пам'ять називається – віртуальною. Звичайно, перед виконанням необхідна частина програми повинна бути переміщена в оперативну пам'ять. Ці функції виконує ядро операційної системи, диспетчер віртуальної пам'яті, що знаходиться в мікроядрі. Тому для програми і для користувача ці дії прозорі. Тому на запити до віртуальної пам'яті витрачається набагато більше часу, ніж до ОЗП.

Другий модуль – це планувальник. Основна задача, якого не менш важлива. Так як Linux – мультизадачна ОС, тому може одночасно виконувати безліч процесів. Нам відомо, що у фіксований момент часу на одному процесорі може виконуватися лише одна команда.

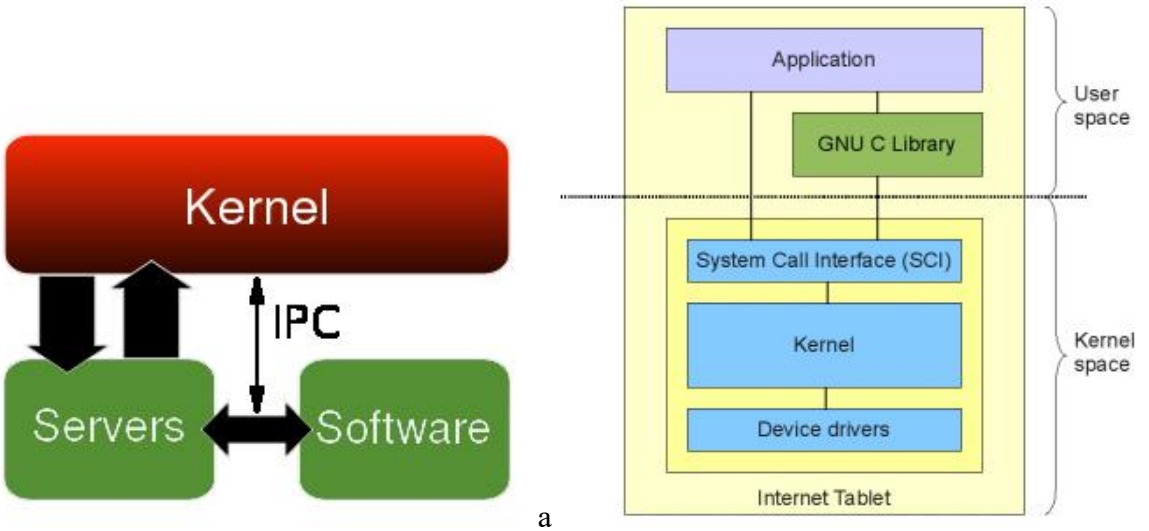


Рисунок 4 – Рівень апаратного контролю: а – взаємозв'язок; б – організація дій

Це пов'язано з тим, що потрібний віртуальний рефері, який буде визначати, якому з процесові виконуватися зараз, а якому – через секунду і так далі. На практиці, планувальник переключає контекст, а саме перед тим, як зупинити виконання певного процесу, він запам'ятовує стан регістрів, пам'яті і інше, а вже потім запускає інший процес у його власному адресному просторі.

Слід звернути увагу на один нюанс: кожен запущений процес "думає", що він єдиний. Для такого й існує механізм пріоритетів. Таким чином чим вище пріоритет, тим швидше почне виповнюватися процес.

Процеси можуть виконувати обмін даними між собою. В такому випадку їх синхронної взаємодії, синхронізацію здійснює модуль взаємодії такий як, функція wait.

Останній рівень – це апаратний контроль, на цьому рівні відбувається обробка переривань та зв'язок ядра з залізом. Варто зазначити лише пару моментів.

По-перше ці переривання можуть "переривати" роботу процесора й вимагати уваги до себе, при чому після цього процесор без проблем повертається до виконання залишених процесів.

По-друге, обробку переривань здійснюють спеціальні функції ядра. Windows 8/10 побудовані на архітектурі мікроядра (microkernel architecture), тоді як ОС Windows 95/98 використовують монолітне (monolithic) ядро. Мікроядра являються порівняно невеликими і модульними. Завдяки цьому нові пристрої зазвичай додаються, як модулі, які можна завантажувати/вивантажувати на етапі виконання без перекомпіляції ядра.

В архітектурі мікроядра побудовані також FreeBSD і Mac OS X. Монолітні ядра використовуються ще й у Linux, вони оптимізовані для більш високої продуктивності з мінімальними контекстними переключеннями. Така архітектура спрощує підтримку коду ядра для розроблювачів, однак потребує перекомпіляції ядра при додаванні нових пристроїв.

Слід звернути увагу, що описані тут розходження є "класичними", тоді як на практиці монолітні ядра можуть підтримувати модульність, що найчастіше і відбувається, а мікроядра можуть вимагати перекомпіляції.

Створення тайм-клуб на базі ОС Windows

Перша й основна перевага використання ОС Windows для організації тайм-клубу це простота для користувача, так як загальна більшість користувачів використовує саме цю операційну систему та ряд програмних продуктів, що надаються до неї. Однак на програмному рівні ядро системи є критичною частиною коду, тому будь-які помилки, що відбуваються в ядрі, приводять до фатального краху системи – "синього екрану".

Проте користувальницькі підсистеми не сильно критично впливають на роботу системи в цілому. Через те що вони ізольовані одне від одного та від ядра засобами керування пам'яттю й власне процесором.

Загалом – це помилки типу "Порушення загального захисту". Тому як тільки код ядра починає звертатися в заборонені для нього області пам'яті, такі як спроба прочитати або записати дані, виконати невірну інструкцію, перехід на заборонену область, негайно спрацьовує система захисту пам'яті процесора, і керування передається системному оброблювачеві виключень. В свою чергу оброблювач виключень не може відновити коректне поводження коду. Це й приводить до виконання журналювання, дампа пам’яті на синій екран із указівкою типу помилки і вмісту пам'яті в області, де спрацював захист.

Помилки, що виникають у застосунках, виконуються на рівні користувача, а саме на менш привілейованому рівні, ніж ядро. Через це система в стані контролювати процес і при виникненні помилки або збою керування передається оброблювачеві помилок, що називається "Doctor Watson". Цей оброблювач примусово завершить додаток та ядро системи й інших підсистем залишаються в цілісності та збережені.

Ядро Linux має два види виключень, що звичайно називають "oops" і "panic". Зазвичай в кожній операційній системі паніка відбувається в тих випадках, коли ядро виявляє серйозну несправність. У такому випадку система яким-небудь чином зашкодила сама собі, вона потребує негайно зупинитися, доки вона не виконає невідворотних критичних змін, типу знищення файлової системи.

Скрізь, де тільки можливо, Linux намагається виявляти проблему та виправити її без зупинки всієї системи. Наприклад, більшість ситуацій типу "oops" приводять до завершення процесу, що нормально запустився, але потім зациклив систему.

Також виникають ситуації, коли все настільки критично, що повна паніка є найкращим виходом. Вважається, що користувачі стабільних версій ядра не повинні зустрічати ні "паник", ні "oops". Але в реальному світі вони іноді відбуваються.

Нещодавно було виявлено "TF-баг", який є гарним прикладом паніки. Процесор намагається передати керування процесові, якого не існує, що в свою чергу призводить до краху всієї системи. В цьому випадку, у системи немає іншої альтернативи, ніж перезавантажитися.

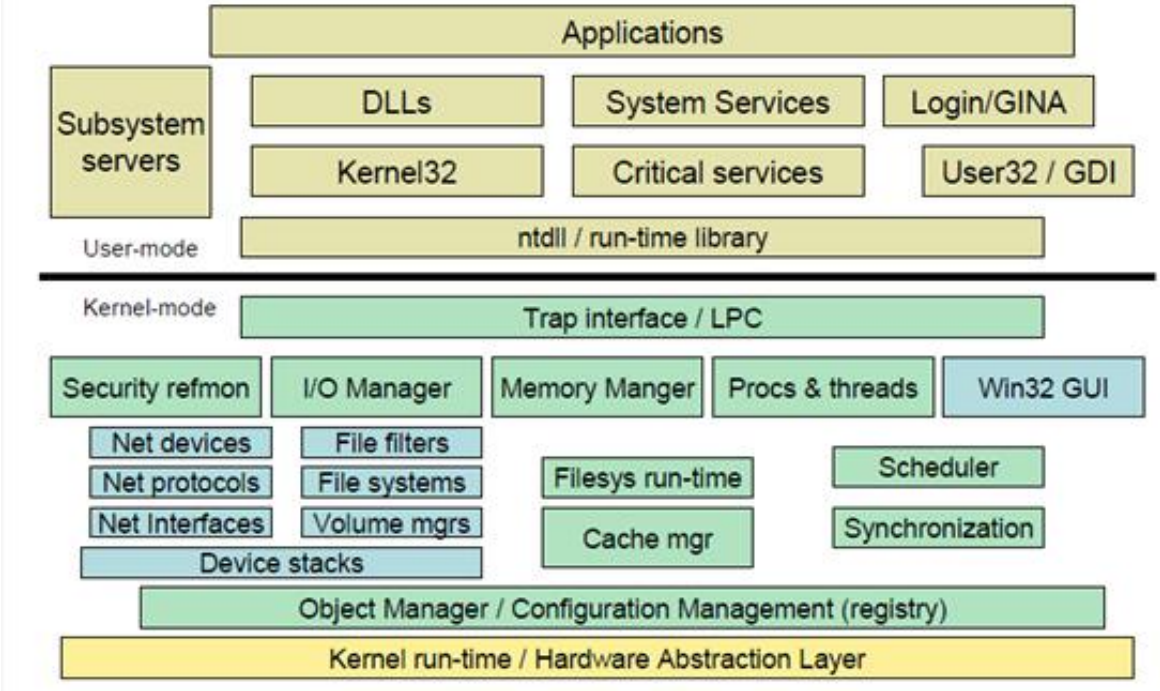


Рисунок 5 – Архітектура ОС Windows

Ядро Windows 8/10, складається з декількох системних компонентів, кожний з яких відповідає за визначений набір задач (основні компоненти ядра).

Мікроядро (Microkernel) – це компактний код, так зване, серце системи. В рамках мікроядра працюють ключові служби такі як: диспетчер пам'яті, диспетчер задач і інші. Ядро, що поставляється з Red Hat Linux і деякими іншими дистрибутивами, має баг у файловій системі ext3. Дана помилка приводить до "oops", завершуючи час від часу деякі процеси, також цей баг призводить до зменшення швидкості роботи всієї системи. Однак ця помилка вже виправлена, в патчі є відновленні від Red Hat, цей випадок ознайомлює багатьох користувачів з помилками типу "oops".

Рівень абстрагування (Hardware Abstraction Layer, HAL), цілком абстрагує код системи від конкретного апаратного обладнання. Тому використання HAL дозволяє забезпечити стійкість та переміщуваність 99% коду системи між різним обладнанням.

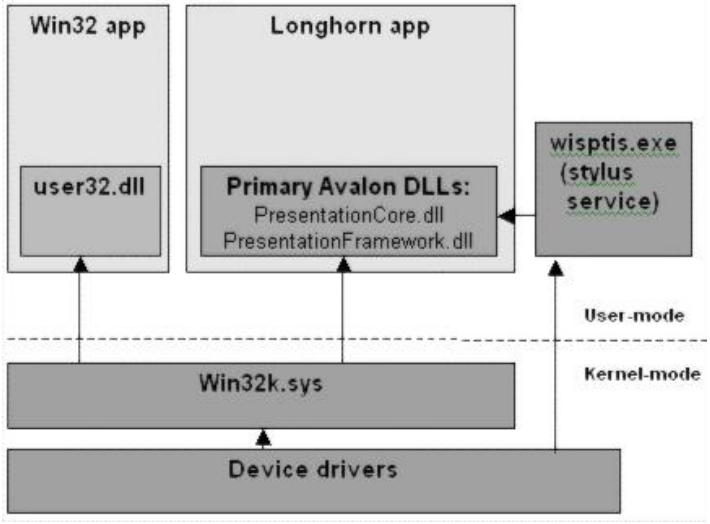


Рисунок 6 – Модуль графічного інтерфейсу

Windows XP містить вбудований механізм контролю драйверів: правильно написаний і ретельно протестований драйвер поставляється з цифровим підписом (Driver Signing). Правильне настроювання системи полягає в забороні установки драйверів без коректного підпису. Диспетчер введення/виведення (Input/Output Manager), повністю контролює потоки обміну між системою й пристроями. Драйвери пристроїв працюють у контексті I/O Manager. У випадку якщо драйвер написаний з помилками і може привести до збою, то викликається фатальний крах ядра і всієї системи. В 70% випадків фатальних збоїв ("синій екран") являється результат некоректного поводження драйверів пристроїв.

Модуль керування об'єктами (Object Manager), виконує керування віртуальною пам'яттю (Virtual Memory Manager), керування безпекою (Security Reference Monitor), керування процесами (Process Manager), керування локальними викликами (Local Procedure Calls Facilities) – важливі компоненти ядра системи. Особливе за значенням місце посідає в ядрі системи саме модуль графічного інтерфейсу – Win32k.sys. Загалом це частина підсистеми Win32, що відповідає за виведення та малювання й керування графічним інтерфейсом. Даний модуль розташований у ядрі спеціально для того, аби істотно підвищити продуктивність графічних операцій введення/виведення. Проте розміщення настільки критичної частини в ядрі накладає надзвичайно жорсткі вимоги до коректності його виконання. Тобто помилка в коді Win32k.sys призведе до краху системи. Тому розробники Windows приділяють величезну увагу цьому модулю, й саме він найбільше ретельно тестується. Певний час експлуатації систем Windows показує, що код Win32k.sys працює абсолютно коректно і не містить фатальних помилок, але некоректний драйвер відеосистеми може усе зіпсувати.

Операційні системи Linux і Windows досить сильно відрізняються в реалізації різних сервисів і служб. В Linux графічна система існує окремо від ядра і функціонує як звичайний

додаток. В операційних системах Windows графічна система інтегрована в ядро. У випадку використання операційної системи на робочій станції, особливо при запуску графікоємних додатків, можливо, краще, коли графічна система входить у ядро – у цьому випадку вона може швидше працювати. А при роботі на сервері краще відділення графічної системи від ядра ОС, тому що вона завантажує пам'ять і процесор. У випадку Linux графічну систему можна просто відключити, до того ж, якщо системний адміністратор її все-таки хоче використовувати, у Linux є кілька графічних оболонок на вибір, деякі з них (наприклад, Window Maker) досить слабко завантажують машину. Ця ж особливість Linux-образних операційних систем дозволяє запускати ці ОС на машинах з досить скромними обсягами ОЗП і т.п. У випадку Windows же графічна система занадто тісно інтегрована в ОС, тому вона повинна запускатися навіть на тих серверах, на яких вона зовсім не потрібна. Тоді як в Windows також реалізовані додаткові функції для підвищення стабільності роботи ОС. Система захисту файлів Windows автоматично запобігає випадковим змінам системних файлів операційної системи, внесені користувачем або додатками, ефективно захищаючи всю систему в цілому. Тобто, коли якась програма внесла зміни або просто замінила системні файли Windows, вважаючи, що в програми більш нові, Windows відслідковує зміни і повідомляє про це користувача, говорячи, що для стабільності системи бажано відновити вихідні файли. Так само існує підтримка декількох версій DLL, що підвищує сумісність додатків і підвищує стабільність.

Відмітимо що, методику поділу прав доступу в Windows 2000 і Linux.

У першому – поділ прав доступу заснований на ACL (access control lists), а саме приміром, можна настроїти систему таким чином, що адміністратор не матиме можливості керувати файлами користувачів. В Linux завжди є супер користувач – root, який має доступ абсолютно до усього.

Тому теоретично модель безпеки в Windows краще: щоб цілком заволодіти добре набудованою системою Windows, хакеру прийдеться ламати більше, у Linux же досить зламати доступ до root. Також у Linux використовуються більш старі технології, однак деякі дистрибутиви Linux зараз починають підтримувати ACL, серед них – ASPLinux.

Але теорія трохи змазується практикою з тієї сторони, що в Windows не так швидко, як у Linux, усуваються "діри", що вже відноситься до плюсів відкритої моделі розробки.

Таким чином виявляється, що в Windows по статистиці більше дір, через які зловмисник може пробратися в систему.

В Linux підтримуються кілька файлових систем, найбільш найсучасніші – це Ext2, Ext3, XFS. ОС Windows зав'язана по великому рахунку на одну файлову систему – NTFS або FAT 32. Файлові системи Ext2, Ext3, XFS по оцінках працюють швидше.

Принципова ж відмінність у тім, що в Linux узагалі немає поняття диска, фізичного або логічного. Уся робота з пристроями збереження даних організується через спеціальні файли пристроїв, що відображають фізичний носій або його частини (розділи) у файлову систему.

Суттєва відмінність – це наявність у Windows технології Active, щось подібне в Linux реалізується за допомогою CORBA і Bonobo. Ця технологія, з одного боку, надає користувачеві безліч зручностей, з іншого боку – вона ж допускала у свій час такі речі, як автоматичний запуск Outlook'ом вірусу, що потрапляв через пошту.

Одна зі значних відмінностей цих технологій у тім, що елементи Active можуть впроваджуватися в текст HTML, що має як ряд переваг, так і недоліків. Також можна перелічити ще ряд відмінностей Linux-подібних операційних систем від Windows, наприклад, убудовану підтримку вилученого доступу в Linux і відсутність її у Windows за замовчуванням, вона реалізується в серверних версіях Windows, а також за допомогою додаткових засобів, наприклад, Citrix. Як Linux так і в Windows сильно розрізняються мережні підсистеми (IP-stack), по ряду оцінок мережна підсистема Linux ефективніше.

Звичайно можна навести ще великий та багатий набір ПЗ, що може поставлятися разом з Linux, тим часом, Windows також розвивається в цьому напрямку. Додаткові

відмінності в архітектурі в основному зводяться до відмінностей роботи монолітних та модульних ядер, які також найчастіше не є перевагами або недоліками, а просто відмінностями, що не відображають змін у характеристиках роботи.

Опис структури стека TCP/IP

Transmission Control Protocol/Internet Protocol (TCP/IP) це промисловий стандарт стека протоколів, розроблений для глобальних мереж. Структура протоколів TCP/IP приведена на рисунку 3.7.

Протоколи TCP/IP поділяються на 4 рівні.

Найнижчий (рівень IV) відповідає на фізичному і канальному рівням моделі OSI. Цей рівень у протоколах TCP/IP не регламентується, проте підтримує всі популярні стандарти фізичного і канального рівня: для локальних мереж, а саме: Token Ring, Ethernet, Fast Ethernet, FDDI, 100VG-AnyLAN, для глобальних мереж, протоколи з'єднань "точка-крапка" SLIP і PPP, протоколи територіальних мереж з комутацією пакетів X.25, frame relay.

Була також розроблена спеціальна специфікація, яка визначає використання технології ATM, як транспорт канального рівня. Зрозуміло з появою нової технології локальних або глобальних мереж, вона швидко включається в стек TCP/IP за рахунок розробки відповідного RFC, що визначає метод інкапсуляції пакетів IP у її кадри.

Наступним рівнем є (рівень III) – рівень міжмережевої взаємодії, що займається передачею пакетів з використанням різних транспортних технологій локальних мереж, територіальних мереж, ліній спеціального зв'язку і т.п. Як основний протокол мережного рівня (у термінах моделі OSI) у стеці використовується протокол IP, що завжди проектувався, як протокол передачі пакетів у складених мережах, що в свою чергу складаються з великої кількості локальних мереж, об'єднаних як локальними, так і глобальними зв'язками.

Тому протокол IP добре працює в мережах зі складною топологією, раціонально використовуючи наявність у них підсистем та економічно витрачаючи пропускну здатність низько швидкісних ліній зв'язку. Протокол IP є дейтограмним протоколом, це означає, що він не гарантує доставку пакетів до вузла призначення, але намагається це зробити.

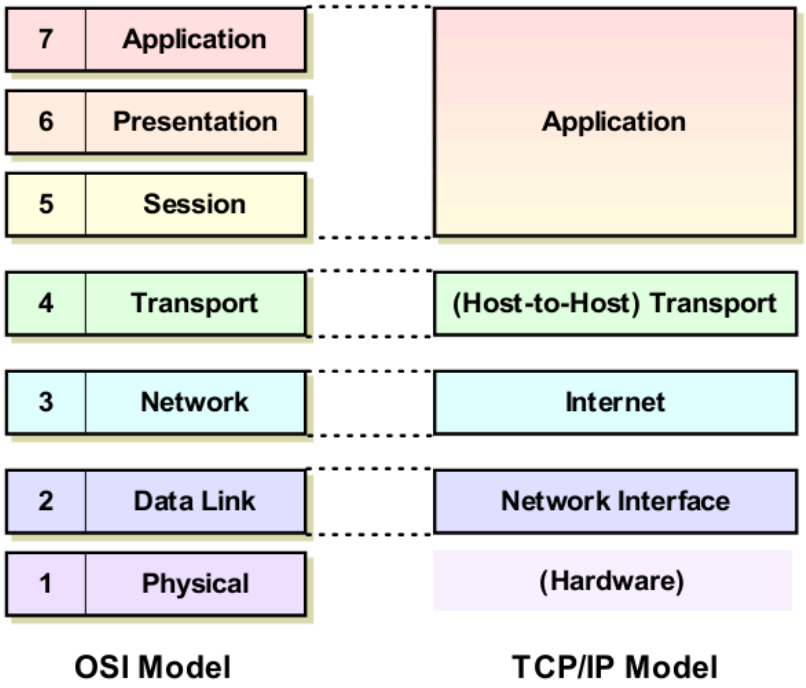


Рисунок 7 – Стек TCP/IP

Міжмережевий рівень взаємодії, до нього відносяться всі протоколи, зв'язані зі складанням й модифікацією таблиць маршрутизації, такі як протоколи збору маршрутної інформації RIP (Routing Internet Protocol) і OSPF (Open Shortest Path First).

Також протокол міжмережних керуючих повідомлень ICMP (Internet Control Message Protocol). Останній протокол призначений для обміну інформацією про помилки між маршрутизаторами мережі і вузлом – джерелом пакета.

За допомогою спеціальних пакетів ICMP повідомляється про неможливість доставки пакета, про перевищення часу життя або тривалості зборки пакета з фрагментів, про аномальні величини параметрів, про зміну маршруту пересилання і типу обслуговування, про стан системи і т.п.

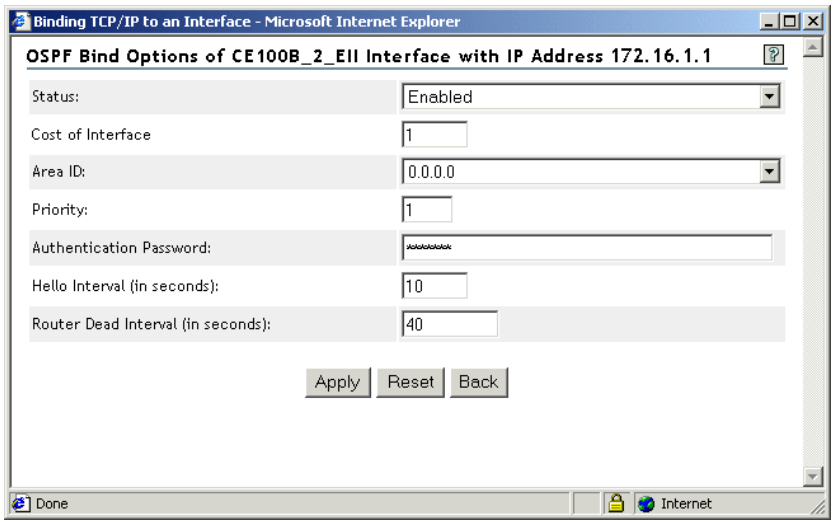


Рисунок 8 – Динамічна маршрутизація OSPF

Наступний рівень (рівень II) це так званий основний, на цьому рівні функціонують протокол керування передачею TCP (Transmission Control Protocol) і протокол дейтограм користувача UDP (User Datagram Protocol).

Протокол TCP забезпечує надійну передачу повідомлень між вилученими прикладними процесами за рахунок утворення віртуальних з'єднань. Протокол UDP забезпечує передачу прикладних пакетів дейтограмним способом, як і IP, і виконує тільки функції сполучної ланки між мережним протоколом і численними прикладними процесами.

Найвищий рівень (рівень I) називається прикладним. За тривалий час використання в мережах різних країн і організацій стек TCP/IP накопичив велику кількість протоколів і сервісів прикладного рівня. До їх ряду відносяться такі широко використовувані протоколи: протокол емуляції термінала telnet; протокол копіювання файлів FTP; поштовий протокол SMTP; використовуваний в електронній пошті мережі Internet; гіпертекстові сервіси доступу до вилученої інформації; такі як WWW і багато інших. Зупинимося трохи докладніше на деякі з них. У стеці TCP/IP протокол FTP пропонує найбільш широкий набір послуг для роботи з файлами, однак він є і самим складним для програмування.

Протокол пересилання файлів FTP (File Transfer Protocol) реалізує вилучений доступ до файлу. Для того, щоб забезпечити надійну передачу, FTP використовує як транспорт протокол із установленням з'єднань – TCP. Крім пересилання файлів протокол FTP пропонує й інші послуги. Так, користувачеві надається можливість інтерактивної роботи з вилученою машиною, наприклад, він може роздрукувати вміст її каталогів. Нарешті, FTP виконує аутентифікацію користувачів. Перш, ніж одержати доступ до файлу, відповідно до протоколу користувачі повинні повідомити своє ім'я і пароль. Для доступу до публічних каталогів FTP-архівів Internet парольна аутентифікація не потрібна, і її обходять за рахунок використання для такого доступу визначеного імені користувача Anonymous. Додатки, яким не потрібні всі можливості FTP, можуть використовувати інший, більш економічний протокол – найпростіший протокол пересилання файлів TFTP (Trivial File Transfer Protocol).

Даний протокол реалізує тільки передачу файлів, причому як транспорт використовується більш простий, ніж TCP, протокол без встановлення з'єднання – UDP.

Перша задача зв'язана з передачею інформації. Протоколи передачі керуючої інформації визначають процедуру взаємодії SNMP-агента, що працює в керованому обладнанні, і SNMP-монітора, що працює на комп'ютері адміністратора, що часто називають також консоллю керування. Протоколи передачі визначають формати повідомлень, якими обмінюються агенти і монітор.

Протокол SNMP (Simple Network Management Protocol) використовується для організації мережного керування. Споконвічно протокол SNMP був розроблений для віддаленого контролю і керування маршрутизаторами Internet, що традиційно часто називають також шлюзами. З ростом популярності протокол SNMP стали застосовувати і для керування будь-яким комунікаційним обладнанням – концентраторами, мостами, мережними адаптерами і т.д. і т.п. Проблема керування в протоколі SNMP розділяється на дві задачі.

Протокол telnet забезпечує передачу потоку байтів між процесами, а також між процесом і терміналом. Найбільше часто цей протокол використовується для емуляції термінала віддаленого комп'ютера. При використанні сервісу telnet користувач фактично керує віддаленим комп'ютером так само, як і локальний користувач, тому такий вид доступу вимагає гарного захисту. Тому сервери telnet завжди використовують як мінімум аутентифікацію по паролю, а іноді і більш могутні засоби захисту, наприклад, систему Kerberos.

Друга задача зв'язана з контрольованими перемінними, що характеризують стан керованого пристрою. Стандарти регламентують, які дані повинні зберігатися і накопичуватися в пристроях, імена цих даних і синтаксис цих імен. У стандарті SNMP визначена специфікація інформаційної бази дані керування мережею. Ця специфікація, відома як база даних MIB (Management Information Base), визначає ті елементи даних, що керований пристрій повинний зберігати, і припустимі операції над ними.

Протокол PPTP (Point-to-Point-Tunneling Protocol) розроблений компанією Microsoft разом з компаніями Ascend Communications, 3Com/Primary Access, ECI-Telematics і US Robotics. Цей протокол був представлений у робочу групу "PPP Extentions" IETF як претендент на стандартний протокол створення захищеного каналу при доступі віддалених користувачів через публічні мережі (у першу чергу Internet) до корпоративних мереж. Цей протокол одержав статус проекту стандарту Internet, однак, як стандарт так і не був затверджений. Зараз робоча група IETF розглядає можливість прийняття як стандарт протокол L2TP (Layer 2 Tunneling Protocol), що повинний об'єднати кращі сторони протоколу PPTP із протоколом аналогічного призначення L2F (Layer 2 Forwarding), запропонованого компанією Cisco.

Протокол PPTP дозволяє створювати захищені канали для обміну даними по різних мережних протоколах – IP, IPX або NetBEUI. Дані цих протоколів інкапсулюються за допомогою протоколу PPTP у пакети протоколу IP, за допомогою якого переносяться в закодованому виді через будь-яку мережу TCP/IP. Інкапсулюється вихідний кадр PPP, тому протокол PPTP можна віднести до класу протоколів інкапсуляції канального рівня в мережний.

Багатопротокольність – основна перевага інкапсулюючих протоколів канального рівня, до яких відноситься протокол PPTP. Протокол SSL орієнтується на один протокол мережного рівня – IP. До того ж розміщення протоколу захищеного каналу безпосередньо під прикладним рівнем вимагає перепису додатків, якщо вони хочуть скористатися можливостями захисту. Захист даних на канальному рівні робить засоби захисту прозорими як для протоколів прикладного рівня, так і для протоколів мережного рівня. Існують також і варіанти вбудовування засобів створення захищеного каналу на мережному рівні. Мається кілька протоколів цього типу, що використовують кодування й інкапсуляцію протоколу мережного рівня в мережний. Для захисту даних у IP-мережах розроблена захищена версія протоколу IP, що найчастіше називають IPSec. Ця версія підтримує аутентифікацію на

мережному рівні, а також може виконувати кодування користувальницьких даних. IPSec – це набір стандартів, частина з яких існує у виді проектів, а частина ще знаходиться в стадії розробки.

Протокол IPSec не визначає жорстко, які методи кодування повинні використовуватися для аутентифікації і створення захищеного каналу, проте для перших реалізацій визначений варіант IPSec, що використовує дайджест-функцію MD5 для аутентифікації й алгоритм шифрування DES для утворення захищеного каналу. Недоліком протоколу IPSec є те, що він працює тільки в IP-мережах і не визначає способу захищеного транспортування пакетів інших протоколів. Цей недолік усувають такі протоколи, як PPTP або L2F.

Розробка структурної схеми

Спочатку розгляду структурної схеми необхідно розуміти, що тайм-клуб це громадський заклад, що надає послуги доступу до Інтернету за гроші, (за погодинну платню). Слово «клуб» в назві походить від того, що деякі з таких закладів також працюють як звичайні клуби, де клієнтам надають можливість спілкуватися з колом людей на спільну тематику при цьому маючи доступ до деяких додаткових послуг (бар) тощо.

В Україні до поширених різновидів тайм-клубів належать також «комп'ютерні клуби», які передусім надають доступ до комп'ютерів для ігор і можуть зовсім не мати Інтернету.

Розглянемо структурну схему розробленого магістерського ПЗ яка зображена на рисунку 9. Як можна побачити з рисунку структура розробленого ПЗ дуже проста.

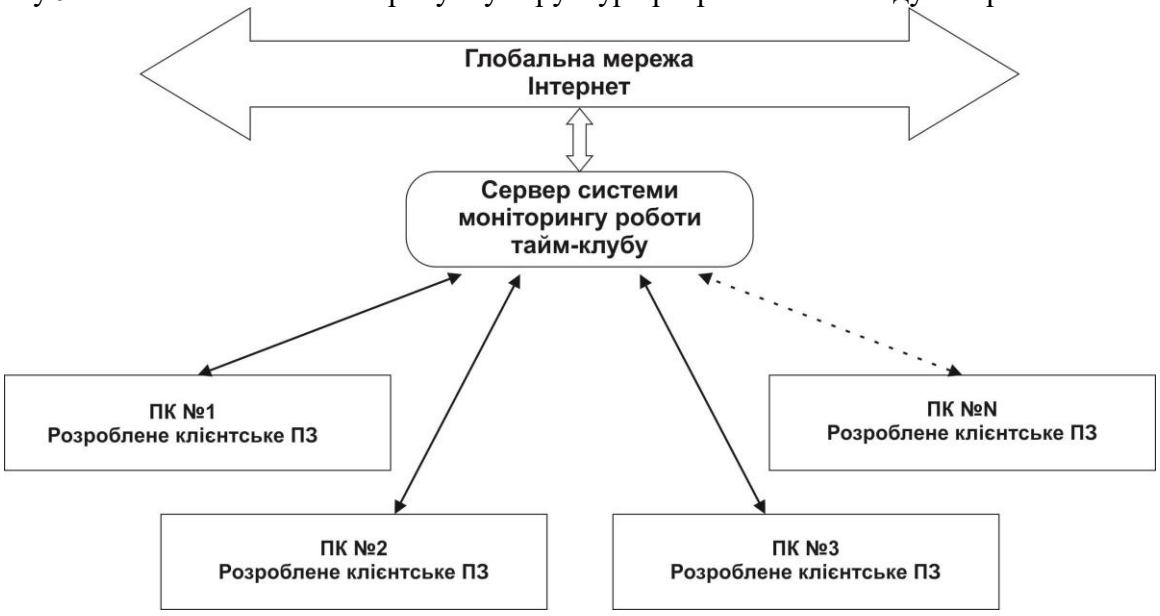


Рисунок 9 – Структурна схема роботи системи

Адміністратор на сервері отримує через роутер канал глобальної мережі Інтернет. На сервері встановлено серверну частину розробленого ПЗ яка через локальну мережу зв’язується з клієнтською частиною розробленого ПЗ (ПК 1– ПК N). Відвідувач тайм-клубу оплачує по тарифу час за ПК, після цього адміністратор вказує номер машини користувачу та розблоковує ПК. Після цього відбувається відлік часу відповідно до внесених коштів користувачем.

Висновок. У статті розглянуто та проаналізовано програмне забезпечення, яке призначено для операційної системи моніторингу роботи тайм-клубу. В межах України в недостатній мірі представлені вітчизняні розробки в цій області. У роботі наведені теоретичне узагальнення й рішення наукового завдання дослідження методів моніторингу роботи тайм-клубу. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем моніторингу роботи тайм-клубу; Досліджена система моніторингу роботи тайм-клубу; На основі отриманих результатів досліджень створена

програмна реалізація системи моніторингу роботи тайм-клубу. Розроблені під час виконання роботи алгоритми дозволяють успішно вирішувати завдання моніторингу роботи тайм-клубу. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки. Розроблене програмне забезпечення має простий, дружній та зручний інтерфейс користувача, що забезпечує легкість у освоєнні роботи програмного продукту, зручність у використанні, і не потребує особливих спеціальних знань. При створені програмного забезпечення було використано об'єктно-орієнтований підхід, що відповідає сучасним тенденціям у галузі розробки комерційних програмних систем. Програма реалізована на мові високого рівня Delphi XE8. Дана мова програмування дозволяє найбільш ефективно обробляти дані. Це дозволило мінімізувати строк розробки програмного забезпечення, і, як слід, зменшити витрати на його розробку. Запропоноване програмне забезпечення ділиться на загальне програмне забезпечення, що поставляється із засобами обчислювальної техніки й спеціальне програмне забезпечення, що спеціально розроблене для даної конкретної системи й включає програми, що реалізують її функції.

Список літератури

1. Смірнов О.А. Дослідження впливу ступеня стиснення зображень на оперативність їх доставки у телекомунікаційній системі / О.А. Смірнов, О.М. Дрєєв, О.П. Доренський // Системи обробки інформації. – 2013. – Вип. 8(115). – С. 234-239.
2. Смірнов О.А. Аналіз процесів стиснення та відновлення зображень на основі цифрових методів // О.А. Смірнов, О.П. Доренський, О.М. Дрєєв // Наука і техніка Повітряних сил Збройних Сил України. – 2013. – № 3(12). – С.122-127.
3. Доренський О.П. Формалізація процесу зміни станів програмних об'єктів складних систем на основі формального апарату скінченних автоматів Мура / О.П. Доренський, О.А. Смірнов // Зв'язок : Науково-виробничий журнал. – 2014. – № 3 (109) – С. 27-31.
4. Доренський О.П. Синтез структури інтегрованої моделі об'єктно-орієнтованого програмного забезпечення / О.П. Доренський // Системи обробки інформації. – 2014. – Т. 2, Вип. 2(118). – С. 68-72.
5. Dorensky O. Method of the Models' Synthesis for Software Automated System Objects' States in Digital Images Processing / Oleksandr Dorensky // Збірник наукових праць Кіровоградського національного технічного університету: Техніка в сільськогосподарському виробництві, галузеве машинобудування, автоматизація. – 2014. – Вип. 27. – С. 283-292.
6. Доренський О.П. Метод синтезу тестових структур взаємодії програмних об'єктів під час проектування програмного забезпечення на основі об'єктно-орієнтовної технології / О.П. Доренський // Системи управління, навігації та зв'язку. – Полтава: ПолтНТУ, 2014. – Вип. 3 (31). – С. 107–114.
7. Доренський О.П. Метод синтезу тестових моделей поведінки програмних об'єктів інформаційно-телекомунікаційної системи спеціального призначення / О.П. Доренський // Збірник наукових праць Харківського університету Повітряних Сил. – 2014. – Вип. 3(40). – С. 109-112.
8. Dorensky O. Development of the theoretical bases of logical domain modeling of a complex software system / Oleksandr Dorensky, Alexey Smirnov // International Journal of Computational Engineering Research (IJCER). – India, Delhi, 2014. – Vol. 4, Issue 4. – P. 19-23.
9. Доренський О.П. Дослідження помилок програмного забезпечення // О.П. Доренський, О.М. Змеул // Актуальні задачі сучасних технологій : Міжнар. наук.-техн. конф., 19-20 груд, 2012 р. : збірн. тез доп. – Тернопіль, 2012. – С. 187-188.
10. Доренський О.П. Особливості процесу розробки програмного забезпечення компресії цифрових зображень / О.П. Доренський // Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку : наук.-практ. конф., 12-13 бер, 2014 р. : збірн. тез доп. – Х., 2014. – С. 10-12.

УДК 004

М. Свириденко, магістр гр. КН-18МЗ-1,4
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ МОНІТОРИНГУ ЦОД З СЕРЕДОЮ ПЕРЕДАЧІ ДАНИХ РЕАЛІЗОВАНОЮ ЗА СТАНДАРТОМ IEEE 802.3BQ

У статті розроблено програмне забезпечення, яке призначено для системи моніторингу ЦОД з середою передачі даних реалізованою за стандартом IEEE 802.3bq. Метою розробки є дослідження та програмна реалізація системи моніторингу ЦОД з середою передачі даних реалізованою за стандартом IEEE 802.3bq. Об'єктом дослідження є процес моніторингу ЦОД з середою передачі даних реалізованою за стандартом IEEE 802.3bq. Предметом дослідження є методи моніторингу ЦОД з середою передачі даних реалізованою за стандартом IEEE 802.3bq. Методи дослідження базуються на методах моніторингу ЦОД, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи моніторингу ЦОД з середою передачі даних реалізованою за стандартом IEEE 802.3bq. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.
комп'ютерні науки, система моніторингу, ЦОД, IEEE 802.3bq

Постановка проблеми. На сучасному етапі розвитку центрів обробки даних (ЦОД) впровадження 25-гігабітних мережних інтерфейсів Ethernet відповідає насущним практичним потребам. У випадку симетричних ліній зв'язку перехід на швидкості 25 і 40 Гбіт/с можливий, але може бути здійснений тільки на базі екранованої техніки структурованих кабельних систем (СКС).

Донедавна для швидкостей понад 10 Гбіт/с вибір середовища передачі в ЦОД обмежувався пропозицією багатомодової і одномодової техніки. Завдання вибору можливих середовищ передачі помітно ускладнилося після офіційної ратифікації стандарту IEEE 802.3bq в 2016 році. У цьому документі зафіксовані основні параметри фізичного рівня й правила взаємодії мережних інтерфейсів 25 і 40 Гбіт/с, що використовують як середовище передачі симетричний чотирьохпарний кабель.

Найбільш витратні через наявність великої кількості ліній нижні рівні інформаційної інфраструктури ЦОД (у першу чергу в межах внутрирядної проводки) можуть бути реалізовані на базі менш примхливої в інсталяції й не настільки дорогою електропровідної техніки. Обмеження по дальності не має в цій частині ЦОД вирішального значення, оскільки довжина створюваних ліній відносно невелика (середня довжина лінії зв'язку звичайно не перевищує 30 м). На верхніх магістральних рівнях застосовуються волоконно-оптичні рішення, що відповідає класичному підходу до використання техніки СКС.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи моніторингу ЦОД з середою передачі даних реалізованою за стандартом IEEE 802.3bq.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи моніторингу ЦОД з середою передачі даних реалізованою за стандартом IEEE 802.3bq.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем моніторингу ЦОД з середою передачі даних реалізованою за стандартом IEEE 802.3bq.

– Дослідження системи моніторингу ЦОД з середою передачі даних реалізованою за стандартом IEEE 802.3bq.

– Програмна реалізація системи моніторингу ЦОД з середою передачі даних реалізованою за стандартом IEEE 802.3bq.

Об'єктом дослідження є процес моніторингу ЦОД з середою передачі даних реалізованою за стандартом IEEE 802.3bq.

Предметом дослідження є методи моніторингу ЦОД з середою передачі даних реалізованою за стандартом IEEE 802.3bq.

Методи дослідження базуються на методах моніторингу ЦОД, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Комплексні об'єкти IEEE 802.3bq

Особливість стандарту IEEE 802.3bq – комплексний розгляд каналу зв'язку. Під цим розуміється, що у використовуваній моделі враховуються такі різнорідні структури, як:

– пасивна фізична частина лінії, описувана, наприклад, стандартом ISO/IEC 11801;

– активне встаткування на ділянці від розеточної частини рознімного з'єднувача до електричного виходу трансівера.

Зазначений підхід означає, що канал зв'язку формується з обліком чотирьох комплексних об'єктів:

– стаціонарна лінія ISO/IEC 11801;

– повний простий тракт ISO/IEC 11801;

– так званий лінк 40 GBase-T (в англомовній документації 40 GBase-T Link);

– фізичний тракт 40 GBase-T PHY (в англомовній документації 40 GBase-T PHY-Channel).

Перші два об'єкти докладно описані в стандартах СКС. Лінк 40 GBase-T фактично являє собою тракт СКС, доповнений двома прикінцевими розніманнями фізичного інтерфейсу трансіверів MDI. Фізичний тракт 40 GBase-T PHY – це повний шлях передачі сигналів між виходами двох друкованих плат PCB електронних схем трансіверів інтерфейсів, що з'єднуються.

До всіх цих об'єктів застосуємо принцип повної вкладеності.

При формуванні структури вкладених об'єктів IEEE 802.3bq приймаються в увагу наступні базові постулати:

– об'єкти ISO/IEC 11801 розглядаються узагальнено без детального опису конфігурації їхньої структури;

– між об'єктами IEEE 802.3bq і ISO/IEC 11801 забезпечується простий «безшовний» перехід;

– можливість використання консолидаційної точки й застосування схеми крос-коннекта не передбачається;

– акцент робиться на структурі й характеристиках двоконнекторної моделі тракту передачі;

– загальна «електрична» довжина фізичної частини каналу зв'язку становить не більше 30 м.

Окремо відзначимо, що «електрична» довжина тракту в певних межах відрізняється від фізичної. Це пояснюється передбаченої в стандарті можливістю застосування прикінцевих шнурів з різним діаметром провідників і, відповідно, різним внесеним загасанням при рівній довжині. Останнє має немаловажне значення з погляду забезпечення поточного адміністрування ЦОД.

Скорочення максимальної довжини тракту

У стандарті IEEE 802.3bq зафіксовано, що для мережних інтерфейсів 25 GBase-T і 40GBase T найбільша довжина тракту становить 30 м. Вибір такого значення обумовлений не можливостями техніки (ще десять років тому була експериментально продемонстрована

передача 100-гігабітного сигналу на відстань 100 м з необхідним рівнем якості), а міркуваннями простоти реалізації ліній і енергетичної ефективності інтерфейсу.

Останнє визначається тим, що через помітно більше високе загасання потужність споживання мідножильного інтерфейсу починає перевищувати потужність споживання його волоконно-оптичного аналога, якщо довжина лінії близько 50 м.

Крім того, порівняння даних показує, що 30-метрові тракти по своїх характеристиках добре узгоджуються з лінійним сигналом.

Елементна база 25- і 40-гігабітних кабельних трактів

Для побудови фізичного рівня можуть бути використані тільки тракти Категорії 8. На відміну від мережних інтерфейсів 10 GBase-T, можливість застосування техніки молодших категорій не передбачається. Тракти, відомі як 8.1 і 8.2, можуть бути реалізовані двома способами.

Техніка Категорії 8.1, що створена на базі 6_A, обґрунтовано вважається більш дешевою. Деякий її програш по забезпечуваних параметрах впливу повністю нівелюється можливостями апаратурної компенсації перешкоди в цифровому сигнальному процесорі.

Техніка Категорії 8.2 розроблена на базі Категорії 7_A. Її сильною стороною є поліпшені характеристики – у першу чергу шумові.

Апаратні засоби збільшення якості передачі інформації

Необхідність введення в стандарт IEEE 802.3bq додаткових об'єктів обумовлена тим, що тракт передачі розглядається як єдина структура, для формування якої залучаються включаємі послідовно активні й пасивні елементи. Комплексний облік їхньої взаємодії дозволяє поліпшити якісні показники каналу зв'язку за рахунок нарощування параметрів RL, NEXT, FEXT, PS-NEXT і PS-FEXT.

У момент з'єднання інтерфейсів виконується процедура тест-преамбули:

– установлюється необхідне для мережних структур взаємовідношені інтерфейсів, що з'єднуються, відповідно до правила «головний – підлеглий» (англ. master – slave);

– настроюються адаптивні схеми придушення перешкод різної природи (англ. cancellation).

Введення до складу функціональних модулів трансівера вузлів придушення перешкоди пояснюється тим, що канали зв'язку 25 GBase-T і 40 GBase-T функціонують у режимі переважного впливу двох видів перешкод: перехідного й зворотного відбиття. На відміну від теплового шуму приймача ці впливи, що заважають, передбачувані й потенційно можуть бути подавлені за допомогою корекції.

Крім того, для компенсації відповідного впливу уточнюються коефіцієнт передачі між взаємодіючими ланцюгами і їхні частотні характеристики. Після цього залишається сформувати коригувальний сигнал і відняти його з «суміші» вхідного інформаційного сигналу із шумом.

Для більш простого виконання корекції перехідної перешкоди доцільно, щоб сигнал перевищував шум. Фактично ця вимога задає верхню граничну частоту симетричного кабельного тракту, що визначається за величиною ACR.

Очищення сигналу від перешкод здійснюється послідовно, а реалізує її сигнальний процесор приймача мережного інтерфейсу, що використовує відпрацьовані ще в 90-х роках минулого століття процедури обробки вступника сигналу за схемою «на льоту».

Активне апаратне придушення перехідних і зворотних шумів необхідно, тому що дуже важко домогтися позитивних величин відносини сигналу до шуму в смузі частот високошвидкісних каналів винятково пасивними засобами, навіть якщо застосовується найсучасніша елементна база Категорії 8.

Ще одним наслідком високої обчислювальної потужності сигнального процесора стає відмова від амплітудно-імпульсної модуляції PAM лінійного сигналу, застосовуваної в перших поколіннях гігабітної і мультигігабітної техніки, на користь більше складної, але ефективної квадратурно-імпульсної модуляції QAM. Захищеність сигналу від перешкоди пропорційна відстані між кінцями векторів окремих комплексних сигналів.

Необхідність використання екранованої техніки

Механізм придушення перешкоди заснований на попередній обробці зашумленого вхідного повідомлення в цифровому сигнальному процесорі. Оскільки йому необхідна інформація про сигнали, що надходять на приймач по сусідніх каналах, процесор не здатний виділити зовнішню перехідну перешкоду, величина якої визначається параметрами ANEXT і AFEXT, а також їхніми сумарними варіантами.

Найкращим засобом придушення міжкабельної (у загальному випадку міжелементної) перешкоди до прийнятного рівня стає перехід на екрановані кабельні вироби. Варіанти введення екранування можуть бути різними:

– тільки загальна оболонка, що екранує, – конструкції класу F/UTP зі збереженням сепаратора (характерні для техніки Категорії 8.1);

– повністю екрановані конструкції виду F/FTP або SF/FTP (техніка Категорії 8.2).

Правильно підібрані екрани при наявності якісного заземлення забезпечують придушення перешкоди приблизно на 40 дб у всім робочому частотному діапазоні.

Переваги техніки категорії 8.2

Істотне поліпшення функціонування каналу зв'язку за рахунок глибокої попередньої обробки сигналу в процесорі неминуче приводить до збільшення навантаження на джерело живлення. Оскільки на високих швидкостях у цифровому сигнальному процесорі виконується значний обсяг обчислень, зростає споживання струму від джерела живлення й збільшується навантаження на систему охолодження апаратної зали.

Менша захищеність, властива техніці Категорії 8.1, змушує в помітно більшому ступені «розганяти» сигнальний процесор, що неминуче позначається на споживаній потужності.

Тракт передачі Категорії 8.2 реалізується на більше якісній елементній базі й тому потенційно має кращі параметри. Основні вигоди від її використання визначаються енергетичним виграшем і можливістю досягнення більшої дальності зв'язку.

Енергетична ефективність ліній Категорії 8.2 обумовлена підвищенням відносини сигналу до шуму, що помітно знижує навантаження на цифровий сигнальний процесор і, відповідно, на споживану їм потужність. З обліком того, що кількість окремих інтерфейсів у типовій монтажній шафі висотою 42 або 45U може перевищувати сотню, навіть економія споживаної потужності в декілька ватт на кожному інтерфейсі обертається зниженням енергоспоживання одного монтажного конструктиву на 1 кВт.

Розширенню потенційної області застосування 25-гігабітних мережних інтерфейсів у сполученні з кабельною технікою Категорії 8.2 сприяє тенденція, що намітилася, впровадження в ЦОД плоских структур з підвищеним рівнем зв’язності окремих вузлів. Скорочення очікуваного середнього часу затримки супроводжується при цьому збільшенням середньої довжини кабельного тракту. У таких ситуаціях може бути затребуване потенційне 1, 5-кратне збільшення дальності зв'язку зі збереженням якісних показників формованого каналу.

У той же час обсяги впровадження техніки Категорії 8.2 стримуються відсутністю зворотної сумісності з лініями молодших класів по форм-факторові рознімних з'єднувачів.

Додаткові заходи по поліпшенню якості функціонування інтерфейсів

Так звані напівекрановані конструкції з незаземленим розривним екраном забезпечують придушення міжкабельної перешкоди приблизно на 20 дБ у всьому робочому частотному діапазоні розглянутих мережних інтерфейсів. Вони досить популярні в кабельних системах Категорії 6_A (компанії Draka, Reichle & De-Massari, Leviton і ін.), де їхнє застосування виправдано з погляду придушення міжкабельної перешкоди.

Варіант застосування класичного незаземленого екрана для кожної пари з розворотом металізації убік проводів (компанія Teldor) залишився незатребуваним через підвищені ризики утворення струмових петель, навіть якщо виконуються вимоги стандартів ЦОД до електромагнітної обстановки в апаратній залі.

Проектними прийомами нарощування A-ACR є відмова від регулярних джгутів на користь біфілярного укладання кабелів у канал і скорочення довжини комутаційних шнурів.

Техніка Категорії 8.2 дозволяє одержати виграш приблизно в 20 дБ по захищеності від перешкод. Отриманий запас може бути витрачений на рішення різних завдань – наприклад, на збільшення дальності передачі 25-гігабітних сигналів до 50 м. Потенційну можливість такого рішення демонструє графік мал. 2, з якого треба, що сигнал на виході 50-метрового тракту забезпечує перевищення над перешкодою у всій робочій смузі ще до його обробки в цифровому сигнальному процесорі.

Основним недоліком техніки Категорії 8.2 уважається неможливість застосування як з'єднувач рознімання модульного типу. Проблема частково вирішена завдяки розробці з'єднувача ARJ-45, що вважається більш перспективним у порівнянні з GG45 і Tera.

Впровадження 25-гігабітних мережних інтерфейсів Ethernet відповідає потребам сучасного етапу розвитку ЦОД. У випадку симетричних ліній зв'язку перехід на швидкості 25 і 40 Гбіт/с технічно можливий, але може бути здійснений тільки на базі екранованої техніки СКС.

Разом з тим характеристики навіть найбільш сучасної техніки Категорії 8 недостатні для забезпечення необхідної якості передачі, внаслідок чого потрібне обов'язкове застосування методів апаратного придушення перехідної перешкоди в мережному інтерфейсі.

Довжина ліній зі швидкістю передачі 25 Гбіт/с може бути збільшена приблизно в 1,5 рази й доведена до 50 м, що помітно розширює проектну й експлуатаційну гнучкість інформаційної інфраструктури ЦОД.

Розробка структурної схеми

Програмне забезпечення системи моніторингу ЦОД з середою передачі даних реалізованою за стандартом IEEE 802.3bq надає багатий набір можливостей, що спрощують і автоматизують моніторинг критично важливого інженерно-технічного встаткування. Воно дозволяє контролювати стан всіх пристроїв, запитувати інформацію з журналів подій і архівні дані, допомагаючи користувачам уживати відповідні дії. Це безкоштовне й простої в установці програмне рішення масштабується відповідно до росту бізнесу.

Переваги системи моніторингу ЦОД з середою передачі даних реалізованою за стандартом IEEE 802.3bq**:**

– Моніторинг у реальному часі. Через систему екранних меню системи моніторингу ЦОД з середою передачі даних реалізованою за стандартом IEEE 802.3bq користувачі можуть одержувати інформацію про поточний стан критично важливого інженерно-технічного встаткування ЦОД. Програма забезпечує перегляд всієї поточної інформації про пристрої ЦОД, а також їхніх журналів подій, у тому числі й для декількох об'єктів у різних країнах.

– Простота установки й запровадження в дію. Програма легко встановлюється на сервер або ПК. Вона була спеціально розроблена для швидкої інсталяції й запровадження в дію.

– Міграція на програмне забезпечення системи моніторингу ЦОД з середою передачі даних реалізованою за стандартом IEEE 802.3bq. Якщо необхідно не тільки моніторинг пристроїв, але й програмне рішення для керування всією інфраструктурою ЦОД (DCIM), то використання системи моніторингу ЦОД з середою передачі даних реалізованою за стандартом IEEE 802.3bq є найпростішим способом міграції на повнофункціональне програмне забезпечення DCIM.

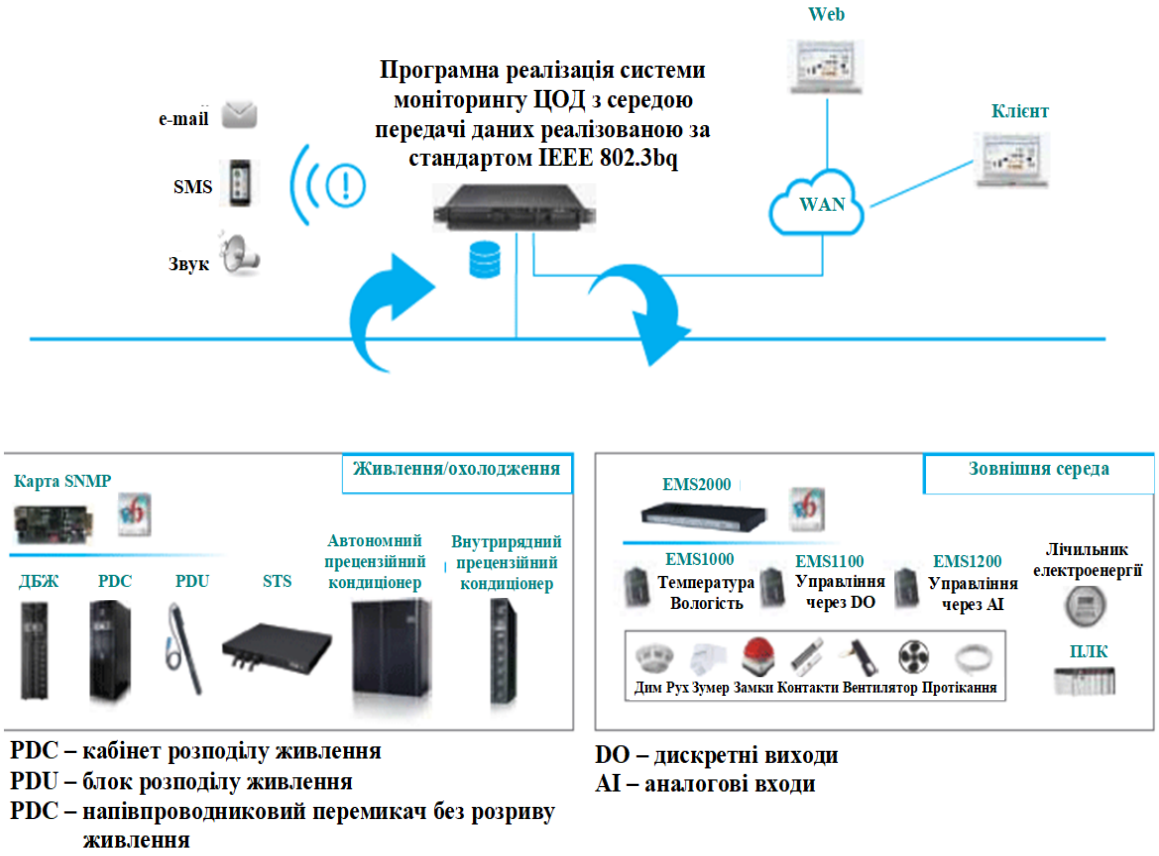


Рисунок 1 – Структурна схема системи

Висновок. У статті розглянуто та проаналізовано програмне забезпечення, яке призначено для системи моніторингу ЦОД з середою передачі даних реалізованою за стандартом IEEE 802.3bq. В межах України в недостатній мірі представлені вітчизняні розробки в цій області. У роботі наведені теоретичне узагальнення й рішення наукового завдання дослідження методів моніторингу ЦОД з середою передачі даних реалізованою за стандартом IEEE 802.3bq. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем моніторингу ЦОД з середою передачі даних реалізованою за стандартом IEEE 802.3bq; Досліджена система моніторингу ЦОД з середою передачі даних реалізованою за стандартом IEEE 802.3bq; На основі отриманих результатів досліджень створена програмна реалізація системи моніторингу ЦОД з середою передачі даних реалізованою за стандартом IEEE 802.3bq. Розроблені під час виконання роботи алгоритми дозволяють успішно вирішувати завдання моніторингу ЦОД з середою передачі даних реалізованою за стандартом IEEE 802.3bq. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки. Розроблене програмне забезпечення має простий, дружній та зручний інтерфейс користувача, що забезпечує легкість у освоєнні роботи програмного продукту, зручність у використанні, і не потребує особливих спеціальних знань. При створені програмного забезпечення було використано об’єктно-орієнтований підхід, що відповідає сучасним тенденціям у галузі розробки комерційних програмних систем. Програма реалізована на мові високого рівня Embarcadero Delphi 10.2. Дана мова програмування дозволяє найбільш ефективно обробляти дані. Це дозволило мінімізувати строк розробки програмного забезпечення, і, як слід, зменшити витрати на його розробку. Запропоноване програмне забезпечення ділиться на загальне програмне забезпечення, що поставляється із засобами обчислювальної техніки й спеціальне програмне забезпечення, що спеціально розроблене для даної конкретної системи й включає програми, що реалізують її функції. Для підвищення рівня безпеки запропоновано застосовувати алгоритм LOKI_91.

Список літератури

1. Семенов С.Г. Анализ методов прогнозирования в телекоммуникационных сетях автоматизированных систем управления / С.Г.Семенов // Збірник наукових праць «Системи управління, навігації та зв'язку», – К.:ЦНДІ навігації і управління, – 2008.-Вип. 2(6) .- С.134-137
2. Семенов С.Г. Математическая модель процесса доставки информационных пакетов в компьютерной сети системы критического применения / С.Г.Семенов, И.В.Ильина // Науково-технічний журнал «Радіоелектронні і комп'ютерні системи» Х.:ХАІ, – 2008.-Вип. 1(28) – С.162-165
3. Семенов С.Г. Оптимизация трафика на основе сбалансированной загрузки информационно-телекоммуникационной сети // Системи обробки інформації. – Х.: ХВУ, 2004. – № 8(36). – С.206-210
4. Семенов С.Г. Математическая модель мультисервисного канала связи на основе экспоненциальной GERT-сети / С.Г. Семенов, Є.В. Мелешко, Я.В. Ілюшко // Системи озброєння і військова техніка. – Х.:ХУ ПС. – 2011. –Вип. 3(27). – С. 64-67.
5. Семенов С.Г. Математична модель системи криптографічного захисту електронних повідомлень на основі GERT-мережі / С.Г. Семенов, О.О. Сур // Системи управління, навігації та зв'язку. – К.:ЦНДІ навігації і управління. – 2012. – Том 1. Вип. 1(21). – С. 131-137
6. Семенов С.Г. Исследования вероятностно-временных характеристик мультисервисного канала связи с использованием математического аппарата GERT-сети / С.Г. Семенов, В.В. Босько, І.А. Березюк // Системи обробки інформації. – Х.: ХУ ПС. – 2012. – Том 1. Вип. 3(101). – С. 139-142.
7. Семенов С.Г. Моделирование защищенного канала связи с использованием экспоненциальной GERT-сети / С.Г. Семенов, А.А. Можаев // Информатика, математическое моделирование, экономика. – Смоленськ.: Смоленский филиал АНО ВПО ЦС РФ "Российский университет кооперации". – 2012. – Том.1. – С. 152-160.
8. Семенов С.Г. Методика математического моделирования защищенной ИТС на основе многослойной GERT-сети / С.Г. Семенов // Вісник Національного технічного університету «Харківський політехнічний інститут». – Х.:НТУ «ХПІ». – 2012. –№62 (968). – С 173-181.
9. Семенов С.Г. Защита данных в компьютеризированных управляющих системах / С.Г. Семенов, В.В. Давыдов, С.Ю. Гавриленко. – LAP Lambert Academic Publishing GmbH & Co. KG (Саарбрюккен, Германия), 2014. – 236 с.
10. Смирнов А.А. Анализ и сравнительное исследование перспективных направлений развития цифровых телекоммуникационных систем и сетей / А.А.Смирнов, В.В.Босько, Е.В.Мелешко // Системи обробки інформації. – Х.: ХУ ПС, 2008. – Вип.7(74). – С.120-123.
11. Смирнов А.А. Усовершенствование метода управления очередями в многопротокольных узлах телекоммуникационной сети / А.А.Смирнов, Е.В.Мелешко // Збірник тез та доповідей другої всеукраїнської науково-практичної конференції «Системний аналіз. Інформатика. Управління». Запоріжжя. Тези доповідей. Запоріжжя: КПУ, 2011.

УДК 004

Д. Сотнічанко, магістр гр. КІ-18М-1,4
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ SDS ДЛЯ ЗБЕРІГАННЯ ДАНИХ

У статті розроблено програмне забезпечення, яке призначено для системи SDS для зберігання даних. Метою розробки є дослідження та програмна реалізація системи SDS для зберігання даних. Об'єктом дослідження є процес SDS для зберігання даних. Предметом дослідження є методи SDS для зберігання даних. Методи дослідження базуються на методах побудови мереж та зберігання даних, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи SDS для зберігання даних. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення..
комп'ютерна інженерія, система SDS, зберігання даних

Постановка проблеми. Незважаючи на те що вартість зберігання одиниці інформації знижується рік у рік, потребу в ємності зберігання випереджає можливості IT-бюджетів, і

компаніям доводиться шукати більше ефективні рішення для зберігання даних. Економічно й функціонально привабливою альтернативою традиційним монолітним корпоративним масивам стають програмно обумовлені системи зберігання.

Що розуміється під програмно обумовленим зберіганням (Software Defined Storage, SDS)? Принцип програмної визначаємості припускає абстрагування програмного забезпечення від апаратного, на якому воно виконується. Це надає організаціям додаткову волю при виборі використовуваного устаткування. Таким чином, SDS привабливі можливістю зниження витрат за рахунок використання стандартної – а тому більше дешевої – техніки. Однак, як і у випадку, наприклад, хмарних сервісів, економія сама по собі мало що виходить, та й не завжди виправдується (скупий, як ми пам'ятаємо, платить двічі), якби не інші переваги.

У програмно обумовлених рішеннях тепер доступні ті ж функції, що й у корпоративних системах зберігання старшого класу – зокрема, дедуплікація на льоту й гарантована якість сервісу. Завдяки зниженню цін на флеш-накопичувачі, SDS здатні забезпечити ту ж продуктивність, що й класичні системи, не уступаючи їм у надійності. Це вже зрілі рішення: вони цілком придатні для підтримки будь-яких віртуалізованих навантажень, і підприємства усе ширше їх використовують.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи SDS для зберігання даних.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи SDS для зберігання даних.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем SDS для зберігання даних.
– Дослідження системи SDS для зберігання даних.
– Програмна реалізація системи SDS для зберігання даних.

Об'єктом дослідження є процес SDS для зберігання даних.

Предметом дослідження є методи SDS для зберігання даних.

Методи дослідження базуються на методах побудови мереж та зберігання даних, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. В умовах швидкого росту обсягів і розмаїтості створюваних типів даних, програмно-визначаємі системи зберігання дають компаніям можливість ефективно адаптуватися до різких темпів росту. Останнім часом саме поняття програмно-визначаємої СЗД активно просувається на ринку, і в результаті далеко не всі добре розуміють, що ж насправді позначає цей термін. Давайте докладніше розглянемо, що за ним криється.

Коли мова йде про програмно-визначаємих СЗД, важливо розуміти, що головне тут – зовсім не програмне забезпечення. Адже до складу традиційних масивів зберігання завжди входили складні стеки ПЗ, а для керування СЗД завжди використовувалися програмні компоненти (наприклад, для переносу файлів і виділення томів). До того ж добування програмного забезпечення із традиційного масиву й оформлення його у вигляді окремого продукту не робить систему зберігання програмно-визначаємою. Так у чому ж тоді справа?

В основі програмно-визначаємої системи зберігання лежить принцип інтелектуального застосування методів розподілених обчислень до проектування систем зберігання. Об'єднання можливостей розподілених обчислень зі стандартним устаткуванням і новими способами оптимізації системи зберігання підвищує ефективність використання простору, збільшує продуктивність, поліпшує керованість і масштабованість. У результаті ми отримуємо всі базові компоненти для економічного рішення проблеми різкого росту обсягів даних:

– гнучкі горизонтально масштабовані програмні СЗД, призначені для роботи на стандартному устаткуванні;

– локальний доступ до даних по декількох протоколах;
– убудовані механізми гео-реплікації;
– і все це реалізовано з використанням спрощених і істотно більше масштабованих засобів керування.

У результаті компанії можуть скоротити капітальні й операційні витрати за рахунок:
– підвищення гнучкості, оперативності й масштабованості керування системою зберігання;
– впровадження більше простій і сучасної моделі використання додатків.

У цьому й складається концепція програмно-визначаємої системи зберігання.

Гнучкість, масштабованість, простота й відсутність компромісів

Гнучка горизонтальна масштабованість має на увазі можливість інкрементно нарощувати ємність СЗД шляхом простого додавання стандартних вузлів. У міру росту потреб у ресурсах таку гнучку систему можна буде розширювати легко й передбачувано. При цьому традиційні масиви зберігання при досягненні межі однієї окремої системи вимагають додавання нових систем, кожна з яких адмініструється окремо від масиву. Це приводить до ускладнення керування, тому що доводиться, наприклад, переносити дані між системами або розробляти складну логіку виділення ресурсів, щоб вибрати систему для розміщення нових робочих навантажень. А принцип горизонтального масштабування, що припускає розширення однієї логічної системи, дозволяє простіше вирішити проблему різкого росту обсягів даних.

Гнучка горизонтальна масштабованість дозволяє зберігати немислимі раніше обсяги даних. Труднощі зберігання різноманітних типів інформації вирішуються за допомогою доступу з використанням декількох протоколів і забезпечення локального доступу до цих даних у різних додатках. СЗД із підтримкою декількох протоколів – це система, у якій забезпечений доступ до тих же базовим даним через інтерфейс одного або декількох протоколів. Використання декількох інтерфейсів протоколів добре підходить для зберігання й обробки неструктурованих даних (аудіопотоків, даних соціальних мереж, файлів журналів, даних телеметрії й т.п.), на які доводиться чимала частка. Такі платформи можуть легко підтримувати робочі процеси одержання даних за допомогою прикладних мережних протоколів (наприклад, REST), і одночасно забезпечують локальну аналітику цих даних в інфраструктурах Hadoop і Spark за допомогою протоколів доступу (наприклад, HDFS), оптимізованих для обробки потокових даних.

Гнучка горизонтальна масштабованість і використання декількох протоколів – ключові функції нових програмно-визначаємих СЗД. Але що робити з існуючими системами зберігання? Чи застосовна концепція програмно-визначаємої СЗД до всього середовища? Так, але небагато іншим способом. Останній елемент концепції дозволяє вирішувати проблеми за допомогою функцій керування й автоматизації, які, деякою мірою, дозволяють управляти традиційною інфраструктурою зберігання так, ніби вона була програмно-визначаємою.

Це досягається шляхом застосування до традиційних середовищ зберігання випробуваних принципів абстрагування, створення пулів ресурсів і автоматизації на основі політик. Такі компоненти керування, звичайно називані програмно-визначаємими контролерами СЗД, автоматизують багато складних процесів керування системами зберігання для традиційних інфраструктур – зокрема, виділення ресурсів, захист, міграцію й перепрофілювання даних. Завдяки цьому IT-служби можуть знизити операційні витрати, пов'язані з існуючими системами зберігання, одночасно підвищивши якість обслуговування й зменшивши час надання послуг.

Поставка програмно-визначаємої СЗД разом з устаткуванням

У принципі, програмно-визначаємі системи зберігання працюють незалежно від устаткування. Але це не виходить, що їх обов'язково потрібно здобувати у вигляді повністю програмного рішення. Хоча великі підприємства можуть придбати відповідне ПЗ й потім створити власні програмно-визначаємі системи зберігання, такий варіант може виявитися

неприйнятним для компаній меншого масштабу. Іноді, для обліку більше широких інтересів замовників, програмно-визначаєма СЗД може поставлятися разом зі стандартним устаткуванням у формфакторі пристрою. Такий варіант поєднує в собі переваги програмно-визначаємого стека зі способом придбання, характерним для традиційних масивів.

Тому якщо ви задастеся питанням, що краще: придбати програмно-визначаєма СЗД у вигляді програмного рішення або апаратного пристрою, то відповідь дуже проста: вибирайте той варіант, що більше вам підходить.

Рішення проблеми із ЦОД

Програмно-визначаєма СЗД являє собою один з елементів програмно-визначаємого центру обробки даних. Інші два елементи – це програмно-визначаємі обчислювальні ресурси (згадаєте віртуалізацію й контейнеризацію) і програмно-визначаєма мережа. Із цих трьох елементів СЗД була реалізована останньої. Проектування системи для надійного зберігання даних з можливістю горизонтального масштабування, доступу з використанням декількох протоколів, гео-розподілу, локальної аналітики, так ще й із простими засобами керування – це воістину непросте завдання. Саме тому постачальникам СЗД знадобилося стільки часу на створення систем, що відповідають очікуванням замовників.

Використовуючи програмно-визначаєму систему зберігання, компанії можуть створювати величезні гео-розподілені пули, для розширення яких потрібно дуже мало зусиль із боку IT-служби й користувачів. Це також дає безпрецедентні економічні переваги, тому що платформи на базі стандартного устаткування усе ширше використовуються як основа для систем зберігання наступного покоління, які приходять на зміну більше дорогим спеціалізованим масивам.

А починається все із правильного розуміння концепції програмно-визначаємої СЗД: це підхід до проектування систем зберігання, у якому використовуються принципи розподілених обчислень, і який дозволяє реалізувати гнучкі функції горизонтального масштабування, доступу з використанням декількох протоколів, гео-розподілу й локальної аналітики, а також спростити керування. Саме так ми зможемо вирішити критично важливе завдання зберігання зрослих обсягів самих різних типів даних.

Розробка структурної схеми

Пропонується програмно обумовлене сховище даних під маркою « SDS-сховище». Воно масштабується до 8 Пбайт шляхом об'єднання дискового простору серверів у розподілене відказостійке й масштабоване сховище даних. Архітектура « SDS-сховища» розрахована таким чином, що СЗД буде стабільно працювати при втраті будь-якого фізичного сервера або цілої групи серверів, а не тільки окремого диска. Висока доступність досягається за рахунок реалізації двох типів надмірності: за допомогою реплікації й надлишкового кодування. « SDS-сховище» підтримує багаторівневе зберігання даних, у тому числі можна використовувати SSD Tiering.

Реплікація забезпечує створення повних копій даних, але накладні витрати досить високі: дві репліки – 100-процентний ріст витрат, три – 200-процентний. Надлишкове кодування являє собою програмний аналог RAID6 (3+2; 5+2; 7+2; 17+3), у цьому випадку накладні витрати менше. Найвища продуктивність досягається при реплікації, а ефективне споживання ємності властиво для надлишкового кодування. Коли потрібна висока продуктивність (для баз даних і віртуалізації), рекомендують використовувати репліки. Якщо ж сховище призначене для «холодних» даних – резерву, архівної інформації, то краще віддати перевагу надлишковому кодуванню.

Замовник, готовий взяти на себе ризики самостійного розгортання програмного забезпечення, може скористатися ПЗ на базі відкритого вихідного коду, наприклад Ceph. Однак, «SDS-сховище» приблизно у два рази ефективніше Ceph, оскільки в ньому відсутній сервіс моніторингу (ця функціональність виконується сервісом MDS). У сценаріях випадкового запису «SDS-сховище» перевершує Ceph в 10 разів. Цього вдалося домогтися за рахунок оптимізації роботи з кешем і журналювання. Ceph здійснює запис відразу й у журнал, і на жорсткий диск системи SDS для зберігання даних, а « SDS-сховище» спочатку

формує всі дані в SSD-Журналі, а потім у фоновому режимі відправляє їх на жорсткий диск системи SDS для зберігання даних.

Програмно обумовлене зберігання зручно саме по собі, однак найбільшу цінність воно здобуває в рамках повністю програмно обумовленого центра обробки даних. Одним з важливих етапів для досягнення цієї мети є розгортання гіперконвергентної інфраструктури (Hyperconverged Infrastructure, HCI).

Найбільші вигоди реалізація програмно обумовленого зберігання забезпечує в рамках гіперконвергентної інфраструктури. Об'єднання обчислювальних потужностей і ємності зберігання на базі загальної платформи дозволяє, зокрема, більш ефективно управляти ресурсами як єдиним інтегрованим рішенням (замість декількох окремих підсистем).

Гіперконвергентне рішення сполучить у собі гіпервізорну й контейнерну віртуалізацію й програмно обумовлене сховище даних. Віртуалізація й сховище інтегровані прямо: гіпервізор «знає» про те, що працює зі сховищем, а сховище – про те, що забезпечує своїми ресурсами віртуалізацію. Платформа повністю готова до корпоративних завдань. Розгорнути й налаштувати кластер можна протягом година. Наше рішення легко масштабувати, причому в одному кластері без проблем може застосовуватися устаткування різних виробників.

Вузли гіперконвергентного кластера можуть, залежно від потреб, виконувати різні функції, при цьому підтримуються різні сполучення. Наприклад, високопродуктивний сервер можна використовувати тільки для віртуалізації, він буде звертатися до ресурсів сховища по протоколі TCP/IP. І навпаки, якщо потрібна більша ємність для зберігання даних, до малопотужних серверів з більшою кількістю дисків досить підключити полки JBOD. Це дозволяє підбирати й балансувати за вартістю використовуване апаратне забезпечення.

Стандартний корпоративний пакет включає необхідні засоби для забезпечення високої відказостійкості й доступності: міграція без простою (Zero-downtime migration), швидка міграція дисків (Storage Live Migration), висока доступність (High Availability). Відновлення хостов не вимагає перезавантаження, тому строки обслуговування скорочуються. Відказостійкість забезпечується на рівні сервера, стійки й залу. Убудований механізм резервування передбачає повне й інкрементальне резервне копіювання. У сполученні зі сховищем це дозволяє повністю забезпечити потреби в резервному копіюванні – купувати сторонні рішення вже не потрібно.

Для гіпервізорної віртуалізації використовується дороблений KVM, продуктивність якого вдалося підвищити на 30%. Для цього компанія внесла більше 200 виправлень у ядро гіпервізору. Вибір KVM був визначений тим, що за останні кілька років він став для багатьох синонімом гіпервізорной віртуалізації. На KVM перейшли такі гіганти, як Apple, Intel і PayPal.

Проте не рекомендуємо будувати рішення на базі відкритого гіперпервизора KVM, оскільки відкритий код однаково зажадає акуратного складання, доробки сервісів і конфігурації вихідних параметрів. До того ж, володіючи меншим, чим вендор, досвідом і інсталяційною базою, замовник ризикує зробити дорогу помилку при виборі архітектури. В остаточному підсумку витрати на доведення, виправлення недоліків і підтримку вкупі з іншими неявними витратами можуть із лишком перевищити вартість ліцензій.

У свою чергу, використання гіперконвергентних систем дозволяє знизити витрати за рахунок зменшення кількості устаткування (окремі СЗД не потрібні), більше економічного керування й т.д. Розгортання великого кластера на класичної SAN-інфраструктурі може зайняти дні, тижні, а іноді й місяці, тим часом гіперконвергентий кластер «піднімається» за годину й масштабується за мінути, причому лінійним і зрозумілим образом.

Крім убудованої віртуалізації, на базі KVM підтримуються гіпервізори VMware vSphere і Microsoft Hyper-V. При розробці багато уваги приділялося тому, щоб продукт був максимально простим в експлуатації. Підтримуються різні режими відказостійкості й немає обмежень ні по кількості вузлів у кластері, ні по територіальній далекості, що актуально для нашої країни. Відповідне програмне забезпечення встановлюється на будь-яке популярне

устаткування, при цьому для побудови відказостійкої конфігурації можуть використовуватися недорогі диски SATA.

Безумовно, гіперконвергентні системи не вирішать всіх завдань. У майбутньому будуть затребувані різні підходи, наприклад, дезагрегація – підхід, протилежний гіперконвергенції. Не всі можна віртуалізувати, є багато завдань, де потрібні фізичні обчислювальні потужності. «Одне відомо точно: майбутнє за програмно обумовленими ЦОДами. І до цього майбутнього треба бути готовим.

Настроювання продуктивності СЗД

Якщо компанія не хоче витратити гроші понапрасну, вона повинна заздалегідь знати, як буде поводитися система зберігання даних – наскільки успішно СЗД зможе справлятися із пропонованими до неї вимогами. Замовники, що бажають упевнитися в тому, що їхній бізнес-додатка стануть працювати швидше й надійніше, при заміні СЗД все частіше запитують послуги тестування. Клієнти звичайно звертаються за такими послугами на етапі ухвалення рішення про подальший розвиток своєї інфраструктури, адже, крім теоретичних знань, їм необхідно опиратися на практичні результати, отримані в діючому робочому середовищі.

Питання вибору устаткування рано або пізно виникає в будь-якої компанії, наприклад, у зв'язку з незадоволеністю поточною продуктивністю додатків. Роботу таких систем, як бази даних для масової транзакційної обробки даних, можна прискорити шляхом переходу із традиційних жорстких дисків на флеш-накопичувачі.

В інформаційних систем класу OLTP вузьким місцем, що обмежує їхня продуктивність, найчастіше виявляється швидкість запису в журнальні файли бази даних. Як показало тестування, у випадку використання системи Huawei S2600T відповідний показник удалося збільшити в 1,7 рази: максимальне значення швидкості запису для дисків SAS склало 281 Мбайт/с (в однопотоковому режимі), для дисків SSD – 468 Мбайт/с (у трьохпотоковому режимі). Таким чином, ця система молодшого класу підходить для підтримки баз даних OLTP.

Однак показник 450-500 Мбайт/с був досягнутий аж ніяк не сам собою – для цього треба було оптимізувати параметри програмного й апаратного забезпечення. Це ще раз підкреслює важливість настроювання продуктивності, у цьому випадку на рівні екземпляра бази даних: швидкість запису після настроювання збільшилася більш ніж у два рази. Отже, якщо система перестала справлятися з підтримкою додатків і користувачів, перше, що потрібно зробити (якщо це ще не було зроблено), – спробувати оптимізувати її роботу відповідно до типу навантаження, і тоді, можливо, не прийде шукати нове рішення. Потреба в настроюванні СЗД найчастіше виникає в процесі експлуатації, коли яка-небудь інформаційна система не дозволяє забезпечити задані показники продуктивності (наприклад, зросло число користувачів або функцій системи).

Для підвищення продуктивності роботи СЗД застосовуються такі засоби, як ПЗ Multipath (використання декількох інтерфейсів для доступу до конкретного СЗД). Як показало тестування, у випадку СЗД Huawei 5500 V3 швидкість записів випадкових блоків обсягом 8 Кбайт зросла на 30%, а читання – на 15%. Підключення ж пристроїв прямого доступу й «сирих» пристроїв не дає яких-небудь вигід. У всякому разі, файлова система ext3 при підключенні СЗД до ОС Linux забезпечує такий же рівень продуктивності. При цьому відмова від «сирих» пристроїв в ОС Linux спрощує супровід баз даних.

Додатки розрізняються вимогами до уведення-виводу, а системи зберігання – архітектурою, тому дати які-небудь загальні рекомендації щодо настроювання продуктивності СЗД важко. Для баз даних OLTP рекомендується відмовитися від пристроїв прямого доступу й використовувати файлову систему ОС Linux, а при підключенні великої кількості серверів до однієї СЗД – ПЗ Multipath.

Замовники проявляють усе більше невдоволення щодо обмежень і недоліків традиційних підходів до зберігання даних у частині масштабування, складності, вартості, обслуговування й т.д. Наприклад, як відзначається в преамбулі до щорічного огляду 10th

Quality Awards Survey for NAS Systems, опублікованому на сайті searchstorage, загальний рівень оцінок використовуваних систем зберігання найнижчий за всі десять років проведення опитувань, причому зниження задоволеності користувачів спостерігається другий рік підряд, що пояснюється зрослим рівнем очікувань і вимог.

Разом з тим більшість користувачів поки не готові відмовлятися від роками перевірених рішень. Це підтверджують і показники продажів: по оцінці аналітичного агентства Markets&Markets, в 2016 році обсяг усього ринку програмно обумовлених систем зберігання склав 4,72 млрд доларів, тоді як тільки в IV кварталі минулого року, по даним IDC, традиційних систем зберігання було продано на 10,4 млрд доларів. Проте зміна очікувань користувачів змушує вендорів розвивати свої традиційні рішення таким чином, щоб вони забезпечували можливості, схожі з надаваними програмно обумовленими системами.

Серед ключових тенденцій в області СЗД виділяємо – поряд із програмною визначаємістю й поширенням флеш-технологій – горизонтально масштабовані системи NAS. Традиційні вертикально масштабовані системи накладають обмеження на кількість серверів NAS, які можуть бути об'єднані в кластер. Це приводить до утворення не зв'язаних між собою «острівців» NAS і до обмежень на число файлів у файловій системі. Горизонтально масштабовані рішення для корпоративного сегмента пропонують всі провідні постачальники СЗД: Dell EMC, HPE, Hitachi, IBM і, звичайно, NetApp.

Однак підвищення вимог стосується не тільки корпоративних систем, але й рішень середнього класу. Наприклад, компанія ще в 2014 році представила центральну систему керування DSM 5.0, за допомогою якої її сервери NAS можуть бути об'єднані в кластер загальною ємністю 1 Пбайт. Малі підприємства ростуть, ростуть і їхньої вимоги, – тому й у нас з'являються більше серйозні системи, такі як флеш-сервер.

Восени минулого року представила потужний пристрій FlashStation FS3017 на базі флеш-накопичувачів. Оснащене двома багатоядерними процесорами Intel, воно забезпечує високу швидкість доступу й обробки тої інформації, що на ньому зберігається: 200 тис. IOPS при випадковому записі блоками 4K. Загальна вартість володіння системою оцінюється в 0,8 долара на 1 Гбайт. Убудований додаток для створення миттєвих знімків і реплік здатно тиражувати 65 тис. резервних копій на інші площадки, чим досягається практично миттєвий захист даних.

На багатьох підприємствах гостро коштує питання надійності зберігання даних. На базі рішень можна побудувати інфраструктуру за принципом Active-Passive. При виході з ладу одного сервера, другий протягом 30 з візьме на себе всю роботу й користувачі навряд чи помітять неполадки. Нова версія програмного забезпечення High Availability підтримує конфігурацію з виділеними серверами N+M: після відмови сервера запис здійснюється на резервний (один або трохи). При відновленні дані переносяться назад. Один резервний сервер може бути з'єднаний з декількома основними, і навпаки – один основний з декількома резервними.

Крім зберігання даних, системи NAS від можуть виконувати й інші функції – наприклад, NVR, тобто виконувати запис із камер відеоспостереження. Підтримується безліч сумісних камер, але навіть при відсутності в цьому списку тої або іншої моделі, камера буде підтримуватися, якщо вона працює по протоколі ONVIF. Крім цього, сервери можуть виконувати функції поштового сервера, Web-сервера, хмарного сховища, мультимедійного сервера, сервера печатки, сервера резервного копіювання й т.п. Функціональність NAS-серверів була по достоїнству оцінена користувачами. Відповідно до згадуваного опитування searchstorage, функціональність рішень одержала більше високу середню оцінку, ніж продукти NetApp, HPE, Dell EMC у категорії продукції середнього класу (midrange). І в цілому вони були оцінені вище аналогів своїх іменитих конкурентів.

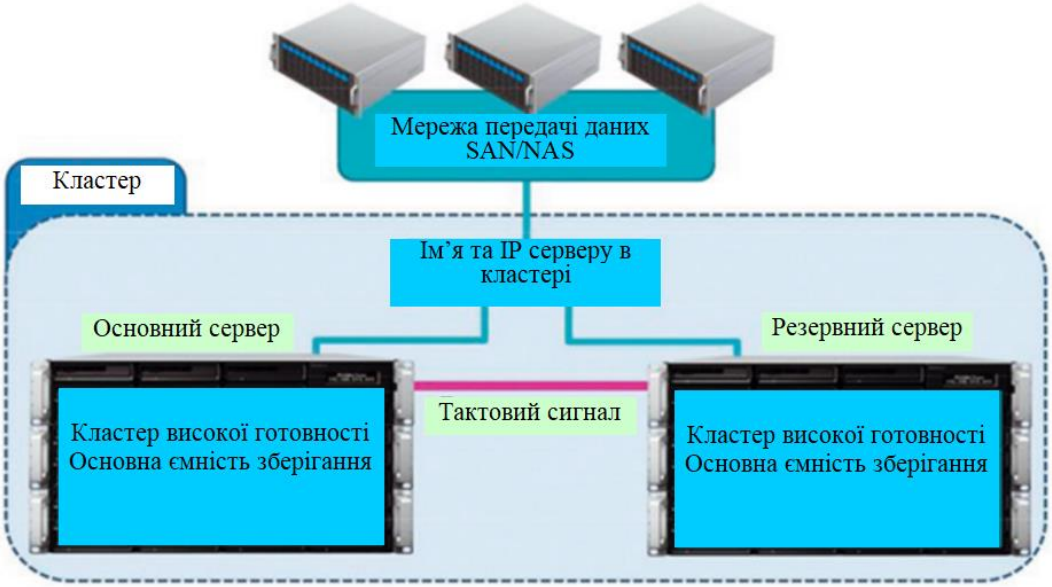


Рисунок 1 – Структурна схема системи

Програмно обумовлене зберігання називають найбільшим просуванням в області рішень для зберігання даних із часів появи мережних сховищ. Перехід від монолітних пропрієтарних сховищ до гнучким програмного представляється неминучим у світлі цифрової трансформації, що відбувається, і швидкого росту обсягу даних. SDS надає організаціям додаткову гнучкість при створенні нових ємностей зберігання й забезпечує значне зниження витрат (наприклад, для цієї мети можуть використовуватися стандартні успадковані сервери). Однак поки деякі замовники готові перенести критичні дані на програмно обумовлені сховища, та й вендори традиційних рішень не стоять на місці, розширюючи функціональність і підвищуючи гнучкість своїх рішень. Так що вся битва технологій в області СЗД ще спереду.

Висновок. У статті розглянуто та проаналізовано програмне забезпечення, яке призначено для операційної системи SDS для зберігання даних. В межах України в недостатній мірі представлені вітчизняні розробки в цій області. У роботі наведені теоретичне узагальнення й рішення наукового завдання дослідження методів SDS для зберігання даних. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем SDS для зберігання даних; Досліджена система SDS для зберігання даних; На основі отриманих результатів досліджень створена програмна реалізація системи SDS для зберігання даних. Розроблені під час виконання роботи алгоритми дозволяють успішно вирішувати завдання SDS для зберігання даних. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки. Розроблене програмне забезпечення має простий, дружній та зручний інтерфейс користувача, що забезпечує легкість у освоєнні роботи програмного продукту, зручність у використанні, і не потребує особливих спеціальних знань. При створені програмного забезпечення було використано об'єктно-орієнтований підхід, що відповідає сучасним тенденціям у галузі розробки комерційних програмних систем. Програма реалізована на мові високого рівня Visual C#. Дана мова програмування дозволяє найбільш ефективно обробляти дані. Це дозволило мінімізувати строк розробки програмного забезпечення, і, як слід, зменшити витрати на його розробку. Запропоноване програмне забезпечення ділиться на загальне програмне забезпечення, що поставляється із засобами обчислювальної техніки й спеціальне програмне забезпечення, що спеціально розроблене для даної конкретної системи й включає програми, що реалізують її функції. Даються необхідні рекомендації з установки розробленого програмного забезпечення. Для підвищення рівня безпеки запропоновано застосовувати алгоритм

Blowfish.

Список літератури

1. Мохамад Гани Абу Таам математическое моделирование технологии передачи сигнатур в облачные антивирусные системы / Мохамад Гани Абу Таам, А.А. Смирнов // Збірник тез VI міжнародної науково-практичної конференції “Проблеми і перспективи розвитку ІТ-індустрії”. м. Харків. 17-18 квітня 2014 р. – Харків: ХНЕУ. – 2014. – С. 260.
2. Мохамад Гани Абу Таам анализ требований к качеству обслуживания в информационно-телекоммуникационных системах / А.А. Смирнов, Мохамад Гани Абу Таам // Збірник тез XVI міжнародного науково-практичного семінару «Комбінаторні конфігурації та їх застосування». м. Кіровоград. 11-12 квітня 2014 р. – Кіровоград: КНТУ. – 2014. – С. 124-126.
3. Мохамад Гані Абу Таам Дослідження та реалізація GERT-моделі технології розповсюдження комп’ютерних вірусів для захисту телекомунікаційних систем / Мохамад Гані Абу Таам, С.А. Смирнов // Збірник тез науково-практичної конференції «Інформаційні технології та комп’ютерна інженерія». м. Кіровоград. 4 грудня 2014 р. – Кіровоград: КНТУ. – 2014. – С. 168.
4. Мохамад Гани Абу Таам Исследование математических моделей технологии распространения компьютерных вирусов / А.А. Смирнов, Мохамад Гани Абу Таам, С.А. Смирнов // Збірник наукових праць міжнародної науково-практичної конференції «Актуальні питання забезпечення кібернетичної безпеки та захисту інформації». м. Київ. 25-28 лютого 2015 р. – Київ: Європейський університет. – 2015. – С. 90-91.
5. Мохамад Гани Абу Таам Метод управления доступом к «облачным» ресурсам для защиты телекоммуникационных систем / Мохамад Гани Абу Таам, А.А. Смирнов, С.А. Смирнов // Збірник тез всеукраїнської науково-практичної конференції «Інформаційна безпека держави, суспільства та особистості». м. Кіровоград. 16 квітня 2015. – Кіровоград: КНТУ. – 2015. – С. 50-52.
6. Мохамад Гани Абу Таам Разработка метода управления доступом в интеллектуальных узлах коммутации / А.А. Смирнов, Мохамад Гани Абу Таам, С.А. Смирнов // Збірник тез VII міжнародної науково-практичної конференції “Проблеми і перспективи розвитку ІТ-індустрії”. м. Харків. 17-18 квітня 2015 р. – Харків: ХНЕУ. – 2015. – С. 14.
7. Мохамад Гани Абу Таам Реализация метода управления доступом в интеллектуальных узлах коммутации / А.А. Смирнов, Мохамад Гани Абу Таам // Збірник тез XVII міжнародного науково-практичного семінару «Комбінаторні конфігурації та їх застосування». м. Кіровоград. 17-18 квітня 2015 р. – Кіровоград: КНТУ. – 2015. – С. 91-92.
8. Мохамад Гани Абу Таам Реализация математической модели интеллектуального узла коммутации **для обеспечения защищенности телекоммуникационной сети** / Мохамад Гани Абу Таам, А.А. Смирнов, С.А. Смирнов // Збірник тез II Міжнародної науково-практичної Інтернет-конференції «Інформаційна та економічна безпека» (INFECO-2015)». м. Харків. 21-22 травня 2015 р. – Харків: ХІБС УБС НБУ. – 2015. – С. 20-24.
9. Мохамад Гани Абу Таам Разработка математической модели технологии распространения компьютерных вирусов в информационно-телекоммуникационных сетях / Мохамад Гани Абу Таам, А.А. Смирнов, С.А. Смирнов // Сборник тезисов XI международной конференции "Стратегия качества в промышленности и образовании". г. Варна. Болгария. 01 – 06 июня 2015 г – Варна. ТУВ. – 2015. – С. 488-491
10. Мохамад Гани Абу Таам Метод управления доступом к облачным телекоммуникационным ресурсам для обеспечения защиты данных / Мохамад Гани Абу Таам, А.А. Смирнов, С.А. Смирнов // Збірник тез Міжнародної науково-практичної конференції «Комп'ютерні технології та інформаційна безпека». м. Кіровоград. 2-3 липня 2015 р. – Кіровоград: КНТУ. – 2015. – С. 4-5.

УДК 004

В. Тіщенко, магістр гр. КН-18-1,4
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ ПІДВИЩЕННЯ ЯКОСТІ КЕРУВАННЯ ПРОДУКТИВНОСТІ КОРПОРАТИВНИХ МЕРЕЖ З ВИКОРИСТАННЯМ КОМУТАТОРІВ DMS-1100-10TS ТА DMS-1100-10TP СТАНДАРТУ ETHERNET 2.5GBASE-T

У статті розроблено програмне забезпечення, яке призначено для системи підвищення якості керування продуктивності корпоративних мереж з використанням комутаторів DMS-1100-10TS та DMS-1100-10TP стандарту Ethernet 2.5GBase-T. Метою розробки є дослідження та програмна реалізація системи підвищення якості керування продуктивності корпоративних мереж з використанням комутаторів DMS-1100-10TS та DMS-1100-10TP стандарту Ethernet 2.5GBase-T. Об'єктом дослідження є процес підвищення якості керування продуктивності корпоративних мереж з використанням комутаторів DMS-1100-10TS та DMS-1100-10TP стандарту Ethernet 2.5GBase-T. Предметом дослідження є методи підвищення якості керування продуктивності корпоративних мереж з використанням комутаторів DMS-1100-10TS та DMS-1100-10TP стандарту Ethernet 2.5GBase-T. Методи дослідження базуються на методах теорії телекомунікації, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи підвищення якості керування продуктивності корпоративних мереж з використанням комутаторів DMS-1100-10TS та DMS-1100-10TP стандарту Ethernet 2.5GBase-T. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення. Розроблено зручний інтерфейс користувача. Наведені інструкції по роботі з програмними засобами.

комп'ютерні науки, якість керування, продуктивність, корпоративні мережі

Постановка проблеми. Важливою умовою підвищення конкурентоспроможності української економіки в умовах ринку є впровадження на вітчизняних підприємствах інформаційних технологій (IT). Основою інфраструктури сучасних підприємств є корпоративні мережі передачі даних, що забезпечують транспорт для переносу інформації між різними застосунками інформаційних систем. На них опираються підсистеми телефонії, охорони, відеоспостереження й ін.

У цей час на зміну спеціалізованим мережам (телефонним, охоронним і ін.) приходять мультисервісні корпоративні мережі. Нові технології (NGN і MPLS) дозволяють створювати ефективні, надійні й безпечні мережі будь-якого масштабу. Для забезпечення зростаючих потреб українських підприємств вимоги до мультисервісної корпоративної мережі, як до середовища передачі інформації для забезпечення роботи різних застосунків, безупинно зростають. Великого значення набуває час реакції застосунків – при динамічному ринку для успішної боротьби з конкурентами рішення необхідно приймати в реальному масштабі часу, що вимагає відповідної організації корпоративної мережі і її застосунків. Вимоги роботи в реальному часі стали для багатьох підприємств нагальною потребою й одним з основних вимог, пропонованих до корпоративних мереж і корпоративних застосунків.

У той же час у реальній корпоративній мережі забезпечити гарний час реакції особливо складно – цьому заважає висока інтенсивність і розмаїтість потоків даних, створюваних сотнями й тисячами співробітників корпорації, необхідність робити пошук даних у базах великої розмірності, складна взаємодія розподілених застосунків, невисока швидкість глобальних ліній зв'язку між відділеннями корпорації, зі швидкості взаємодії в

шлюзах, що погодять неоднорідні компоненти різних під мереж.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи підвищення якості керування продуктивності корпоративних мереж з використанням комутаторів DMS-1100-10TS та DMS-1100-10TP стандарту Ethernet 2.5GBase-T.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи підвищення якості керування продуктивності корпоративних мереж з використанням комутаторів DMS-1100-10TS та DMS-1100-10TP стандарту Ethernet 2.5GBase-T.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем підвищення якості керування продуктивності корпоративних мереж з використанням комутаторів DMS-1100-10TS та DMS-1100-10TP стандарту Ethernet 2.5GBase-T.

– Дослідження системи підвищення якості керування продуктивності корпоративних мереж з використанням комутаторів DMS-1100-10TS та DMS-1100-10TP стандарту Ethernet 2.5GBase-T.

– Програмна реалізація системи підвищення якості керування продуктивності корпоративних мереж з використанням комутаторів DMS-1100-10TS та DMS-1100-10TP стандарту Ethernet 2.5GBase-T.

Об'єктом дослідження є процес підвищення якості керування продуктивності корпоративних мереж з використанням комутаторів DMS-1100-10TS та DMS-1100-10TP стандарту Ethernet 2.5GBase-T.

Предметом дослідження є методи підвищення якості керування продуктивності корпоративних мереж з використанням комутаторів DMS-1100-10TS та DMS-1100-10TP стандарту Ethernet 2.5GBase-T.

Методи дослідження базуються на методах теорії телекомунікації, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Одним з основних напрямків інформатизації є створення й подальше вдосконалювання корпоративної мережі (скорочено EWN). Зазначена мережа є складною технічною програмно-апаратною системою з розгалуженою інфраструктурою й транспортними засобами передачі інформації.

До якості мережної інфраструктури й параметрів угоди про рівень мережних сервісів пред'являються підвищені вимоги. Як правило, адміністраторів корпоративних мереж або мережних інтеграторів цікавить пошук раціональних варіантів рішення завдання оптимізації мережі для підвищення якості її роботи. Пошук полягає в аналізі (вимірі, діагностиці, локалізації помилок) і синтезі (ухваленні рішення про те, які зміни треба внести в роботу мережі). При цьому завдання аналізу вимагає більше активної участі людини й використання таких складних засобів, як експертні системи, які інтегрують практичний досвід багатьох фахівців даної області. Завдання ж синтезу раціонального варіанта по оцінці якості мережі найчастіше пов'язана з вибором великої й різнорідної безлічі параметрів. Завдання ускладнюється, коли рішення доводиться приймати при використанні інформації високого ступеня гранульованості. Така ситуація виникає дуже часто, тому що причини, що впливають на вибір, у цілому носять не тільки технічний характер, але й залежать від ряду обставин, що мають комерційний, політичний і тому подібний характер.

Ціль дослідження – створення нечітко-логічної системи оцінки й керування якістю EWN. Для досягнення поставленої мети сформульована й вирішена наступне завдання. Розробити методологію нечіткого моделювання оцінки й керування якістю корпоративної інформаційно-обчислювальної мережі, що включає метод оцінки якості на основі нечіткої моделі, що дозволяє для кількісної змінної формувати лінгвістичне подання в природно-язикових категоріях; а також метод прийняття рішень про керування якістю на основі його кількісної оцінки.

Багато підприємств мають свої філії практично по всій території країни. У міру росту бізнесу, розвитку підприємства, збільшення чисельності персоналу, підвищення вимог до організації зв'язку між офісами стає актуальним питання про об'єднання всіх існуючих ресурсів у єдину корпоративну мережу. При цьому одного об'єднання й створення корпоративної мережі для ефективної роботи підприємства протягом хоча б п'яти-десяти років недостатньо. Необхідно, по-перше, корелювати напрямок розвитку EWN підприємства з розвитком науково-технічного прогресу, з розвитком усього мережного світу, а по-друге, знайти компроміс між потребами підприємства в обробці циркулюючої інформації, його фінансовими можливостями й можливостями мережних і інформаційних технологій у сьогоденні й майбутньому.

Підприємство має розподілену структуру й хоче підвищити організацію зв'язку й передачу даних у свої підрозділи шляхом побудови корпоративної мережі. Перед авторами було поставлене наступне завдання. Необхідно розробити систему оцінки й керування якістю проектованої EWN. Під системою оцінки й керування якістю розуміється система конфігурації, що дозволяє оцінити якість і описати політикові якості мережі, за допомогою визначення класів сервісу, параметрів, норм і дій у випадку їхнього порушення. Відповідно до Серії Міжнародних Стандартів ISO 9000, якість – це сукупність властивостей системи, що дозволяють задовольняти потреби й очікування споживача. На сучасному етапі висувають високі вимоги до готовності мережі, її пропускної здатності й інтелектуальності, тобто здатності гнучко і якісно обробляти трафік різного типу (дані, голос, відео).

Підприємство висуває наступні вимоги до проектованої мережі:

– інтеграція з існуючими мережами, іншими технологіями й забезпечення сумісності продукції різних фірм-виробників;

– розширення видів послуг, насамперед передачі голоси, даних бізнес-застосунків, конференцзв’язок, видеоконференцзв’язок і ін.;

– можливість надання каналу зв'язку з гарантованими значеннями (можливість керування якістю обслуговування);

– забезпечення високих швидкостей передачі інформації й малий час затримки сигналу;

– достатній запас по основних технічних параметрах для розвитку EWN щонайменше на найближчі п'ять-десять років.

Підхід до рішення даного завдання може бути самим різним і в дуже великому ступені залежить від конкретних переваг підприємства. Необхідно знайти найкращий варіант із погляду якості функціонування, що забезпечував би на всьому протязі мережі, незалежно від її масштабів і використовуваних протоколів, циркуляцію даних у рамках певних параметрів якості. Для цього минулого виявлені основні параметри, що визначають якість EWN. Ними, на думку експертів, стали:

– готовність мережі (availability);
– пропускна здатність (throughput);
– затримка (delay);
– варіація затримки (jitter);
– втрати пакетів (packet loss).

Нижче приводиться коротка характеристика кожного із зазначених параметрів.

Готовність мережі – доступність мережного ресурсу протягом усього строку експлуатації. Готовність мережі оцінюється часом простою підприємства в рік: чим менше час простою, тим вище готовність мережі. Час простою в результаті виходу з ладу або погіршення роботи мережі відбивається безпосередньо на доходах підприємства. Пропускна здатність – це максимально можлива швидкість передачі інформації в мережі. Вона є одним з основних параметрів, тому що для корпоративних мереж характерна нерівномірна структура трафіку, сплески й падіння. Тому якщо порт невеликої пропускної здатності, то в ті моменти, коли трафік великий і мережа випробовує навантаження, якість передачі буде падати.

Затримка характеризує інтервал між прийомом і передачею пакетів. Варіація затримки – параметр, що описує можливі відхилення від часу затримки при передачі пакетів. Втрати пакетів виникають, коли один або більше пакетів з даними, переданими по мережі, не доходить до свого адресата.

До змін цих параметрів мережні сервіси чутливі в різному ступені. У моменти перевантажень у мережі параметри починають погіршуватися, і в підсумку страждають всі критично важливі мережні сервіси. Фахівці підприємства припускають реалізувати політикові диференційованого обслуговування трафіку мережних сервісів (Quality of Service, скорочено QoS), що дозволить забезпечити функціонування критичних сервісів за рахунок обмеження трафіку менш важливих мережних застосунків. Однак для забезпечення якісного функціонування критично важливих для підприємства застосунків у корпоративній мережі реалізації тільки політики диференційованого обслуговування недостатньо. Навіть при успішній роботі QoS у моменти перевантажень перед компанією виникнуть завдання, які не вирішуються необхідним налаштуванням QoS. До таких завдань відносяться наступні: перевірити, чи задовольняють параметри якості встановленим вимогам; виявити причини виходу якого-небудь параметра за встановлені межі; визначити локалізацію проблеми в мережі й комплекс мер по її усуненню. Тому для забезпечення якісного функціонування мережі необхідний комплекс технічних заходів щодо реалізації політики обслуговування мережі, а також система моніторингу й керування якістю. З огляду на вимоги й можливості підприємства, для побудови мережі обране рішення на базі послуги IP VPN (Virtual Private Network – віртуальна приватна мережа), заснованої на технології MPLS (Multi Protocol Label Switching – мультипротокольна комутація по мітках). У мережі зможуть функціонувати будь-які системи, що підтримують IP-протокол, тобто переважна більшість існуючих застосунків. До переваг технології MPLS відносяться гнучке визначення топології мережі; можливість призначати різний пріоритет пропуску трафіку.

Підприємство провело класифікацію трафіку EWN і, оскільки деякі сегменти мережі планується орендувати в оператора зв'язку, погодило прийняту класифікацію з підтримуваними їм класами обслуговування в такий спосіб: перший клас – клас обслуговування з високим пріоритетом – відповідає трафіку відеоконференцій і ряду застосунків, для якого затримки критичні; другий клас – клас обслуговування із середнім пріоритетом – відповідає трафіку телефонії й застосунків, для якого втрати пакетів критичний; третій клас – клас обслуговування з низьким пріоритетом – відповідає звичайному бізнес-трафіку, до якого особливих вимог не пред'являється.

Якість роботи розглянутої EWN характеризується набором технічних параметрів, які умовно можна розділити на параметри якості транспортування мережних сервісів і основні параметри якості мережі. Якість транспортування мережних сервісів визначається параметрами: затримка, варіація затримки, втрати пакетів. До основних параметрів якості віднесені: готовність мережі і її пропускна здатність.

Моделювання оцінки якості

Модель кількісної оцінки узагальненої якості K представляє собою функцію наступного виду:

$$||K||: X_1 \times ... \times X_{11} \rightarrow [0; 1],$$

де

– $X_1 \times ... \times X_7 = \{(Г, ПЗ, З_1, ВЗ_1, ВП_1, З_2, ВЗ_2, ВП_2, З_3, ВЗ_3, ВП_3) \mid (Г \in X_1; ПЗ \in X_2; З_1 \in X_3; ВЗ_1 \in X_4; ВП_1 \in X_5; З_2 \in X_6; ВЗ_2 \in X_7; ВП_2 \in X_8; З_3 \in X_9; ВЗ_3 \in X_{10}; ВП_3 \in X_{11}\}$; $(Г, ПЗ, З_1, ВЗ_1, ВП_1, З_2, ВЗ_2, ВП_2, З_3, ВЗ_3, ВП_3)$ – вектор показників узагальненої якості мережі;

– Г – готовність;

– ПЗ – пропускна здатність;

– $З_i$, $ВЗ_i$, $ВП_i$ – відповідно затримка, варіація затримки, втрати пакетів в і-м класі, і = 1; 2; 3.

Таким чином, кількісною оцінкою узагальненої якості EWN є число, що належить відрізку [0; 1]. Оцінка ||K|| використовується при прийнятті одного з наступних рішень: S_1 – поліпшення якості EWN не потрібно; S_2 – поліпшення якості потрібно й можливо; S_3 – поліпшення якості потрібно, але воно неможливо.

Модель кількісної оцінки основної якості $K_{осн}$ представляє собою функцію виду:

$$||K_{осн}||: X_1 \times X_2 \rightarrow [0; 1],$$

де $X_1 \times X_2 = \{(Г, ПЗ) \mid Г \in X_1; ПЗ \in X_2\}$.

Модель кількісної оцінки якості транспортування мережних сервісів $K_т$ – функція виду:

$$||K_т||: X_3 \times ... \times X_{11} \rightarrow [0; 1],$$

де $X_3 \times ... \times X_{11} = \{(З_1, ВЗ_1, ВП_1, З_2, ВЗ_2, ВП_2, З_3, ВЗ_3, ВП_3) \mid З_1 \in X_3; ВЗ_1 \in X_4; ВП_1 \in X_5; З_2 \in X_6; ВЗ_2 \in X_7; ВП2 \in X_8; З_3 \in X_9; ВЗ_3 \in X_{10}; ВП_3 \in X_{11}\}$.

Модель кількісної оцінки якості обслуговування K_i в і-м класі (i = 1; 2; 3) – функція виду

$$||K_i||: \{(З_i, ВЗ_i, ВП_i)\} \rightarrow [0; 1].$$

Ієрархічний взаємозв'язок між вхідними змінними, класами вхідних змінних і вихідним змінної (інтегральним показником) представимо у вигляді дерева логічного виводу.

Елементи дерева інтерпретуються в такий спосіб. Корінь дерева – кількісна оцінка узагальненої якості K; термінальні вершини Г, П, $З_1$, $ВЗ_1$, $ВП_1$, $З_2$, $ВЗ_2$, $ВП_2$, $З_3$, $ВЗ_3$, $ВП_3$ – частки показники; нетермінальні вершини $f(K_{осн})$, $f(K_1)$, $f(K_2)$, $f(K_3)$ – згортки приватних показників; дуги $K_{осн}$,K_1, K_2, K_3 – укрупнені показники; нетермінальні вершини $f(K_т)$ і f(K) – згортки укрупнених показників; дуга $K_т$ – укрупнений показник. Кожний приватний, а також кожний укрупнений показник розглядається як лінгвістична змінна.

Кожна зі згорток $f(K_{осн})$, $f(K_1)$, $f(K_2)$, $f(K_3)$, $f(K_т)$ і f(K) виробляється за допомогою логічного виводу по експертних нечітких базах знань типу Мамдані. При визначенні форми функцій приналежності, асоційованих з кожної змінної, експерти вибрали трикутну [5]. Як нечіткі бази знань, що є носієм експертної інформації, були сформульовані логічні правила, які виражаються у вигляді пар посилок і висновків типу «ЯКЩО..., ТО...». Елементи антецедентів нечітких правил зв'язані логічною операцією И.

Комп'ютерна реалізація моделі

Розглянемо завдання оцінки якості транспортування мережних сервісів для класу обслуговування з високим пріоритетом. Для створення СНЛВ (системи нечіткого логічного виводу), додаючи вхідні змінні, одержуємо наступну структуру СНЛВ: три входи (затримка, варіація затримки, втрати пакетів), механізм нечіткого виводу Мамдані, один вихід (якість K_1). Кожн вхідний і вихідний змінної ставимо у відповідність набір функцій приналежності (ФП) типу trimf. Для змінної $З_1$ був визначений діапазон значень від 0 до 80 (одиниця виміру – миллисекунда). Для змінної $ВЗ_1$ діапазон значень склав відрізок від 0 до 60 (одиниця виміру – миллисекунда). Для змінної $ВП_1$ діапазон значень був обраний від 0 до 2 (одиниця виміру – відсоток). Як лінгвістичні терми-множин змінних, крім K_1, експерти вказали {низька(і), середня(і), висока(і)}.Терм-множина змінної K_1було задано як {неприйнятно низьке, низьке, середнє, вище за середнє, високе}. Значення вихідного змінного минулого визначені в діапазоні від 0 до 1 (одиниця виміру – дійсне число); потім були додані п'ять ФП типу trimf. Як база знань були сформульовані 27 правил керування. За допомогою засобу перегляду правил виводу вводяться значення вхідних даних, відображається процес нечіткого виводу й результат. Аналогічним образом були розроблені СНЛВ для оцінок якостей K_2 і K_3. Отримані значення оцінок якостей K_1, K_2 і K_3 минулого уведені як значення вхідних даних у СНЛВ для оцінки якості Кт.

Для створення СНЛВ оцінки якості $K_{осн}$ використовувалися вхідні змінні: готовність: діапазон значень [0; 1000] (одиниця виміру – мінута), терм-безлічі {низька, середня, висока} і відповідні значення (200; 1000; 1000), (25; 53; 303), (0; 0; 65); пропускна здатність: діапазон значень [64;2048] (одиниця виміру – Кбіт/с), терм-безлічі {низька, середня, висока} і значення (64; 64; 260), (192; 768; 1200), (786; 2048; 2048). Як база знань були сформульовані

дев'ять правил керування. Поверхня виводу, що відповідає зазначеним правилам, наведена на мал. 2, а. Отримані значення оцінок якостей Кт і Косн були уведені як значення вхідних даних у СНЛВ для оцінки узагальненої якості К.

Якщо умова блоку «$\|K(\cdot)_{доп}\| \le \|K(\cdot)\|$» виконується, то перехід до блоку S_1 і вихід. Якщо ж умова блоку не виконується, то необхідно провести аналіз роботи мережі з метою підвищення її якості. Для цього необхідно з'ясувати, які з показників якості можна поліпшити – блок «Зміна параметрів якості $K(\cdot)$». Якщо умова цього блоку здійсненно, то – перехід до блоку S_2 (поліпшення якості мережі потрібно й можливо) і після зміни значень показників – повернення до блоку «Кількісна оцінка якості $K(\cdot)$», де виробляється оцінка якості після проведених заходів. Якщо коректування показників якості неможлива, то – перехід до блоку S_3 (поліпшення якості потрібно, але воно неможливо) – вихід.

Відповідно до алгоритму створеної системи, для керування якістю EWN необхідно: визначити поточне значення вихідний змінної $\|K\|$; зрівняти його із установленим припустимим значенням; підібрати значення керуючих змінних так, щоб досягти заданого припустимої якості (за умови, що такі значення можуть бути забезпечені).

У самому загальному розумінні, корпоративна мережа – це складний комплекс взаємозалежних і узгоджено функціонуючих програмних і апаратних компонентів, що забезпечує передачу інформації між різними віддаленими застосунками й системами, використовуваними на підприємстві. Через наявність декількох центрів обробки даних, корпоративні мережі відносяться до розподіленого (або децентралізованим) обчислювальним системам.

Корпоративну мережу необхідно розглядати в різних аспектах: структурному; функціональному; системно-технічному.

Зі структурної точки зору корпоративна мережа – мережа змішаної топології, у яку входять кілька локальних обчислювальних мереж. Корпоративна мережа поєднує філії корпорації, створюючи єдиний інформаційний корпоративний простір, і є власністю підприємства. Із цього погляду корпоративна мережа відбиває структуру підприємства. Залежно від масштабів підприємства розрізняють: мережі відділів, мережі будинків і кампусів, мережі масштабу підприємств.

З функціональної точки зору корпоративна мережа – це ефективне середовище передачі актуальної інформації, необхідної для рішення завдань корпорації.

Із системно-технічної точки зору корпоративна мережа являє собою цілісну структуру, що складається з декількох взаємозалежних і взаємодіючих рівнів, представлених на мал. 1. Таким чином, із системно-технічної точки зору корпоративна мережа – це система, що надає користувачам і програмам набір корисних у роботі послуг (сервісів), загальносистемних і спеціалізованих застосунків, що володіє набором корисних якостей (властивостей) і утримуюча в собі служби, що гарантують нормальне функціонування корпоративної мережі.

Сучасний корпоративний сегмент має потребу у використанні мультисервісних мереж, основна тенденція яких – конвергенція пакетних систем передачі даних і мультимедійних мереж. Як наслідок – різке зростання обсягу інформації, переданого по мережах, споконвічно призначених для передачі тільки одного виду трафіку, перевантаження мережного устаткування, відмови різних ділянок мережі.

Багато корпоративних мереж створювалися шляхом хаотичного й непродуманого об'єднання різнотипних ліній зв'язку, у результаті виходили ненадійні мережі, що не справляються зі зростаючими з кожним днем навантаженнями. Постійне зростання обсягу трафіку й недосконалість існуючих корпоративних мереж роблять завдання модернізації гранично актуальної. При модернізації корпоративних мереж доводиться вирішувати завдання їхньої оптимальної побудови: вибирати між прокладкою оптичного волокна, установкою радіорелейного устаткування або застосування апаратури, що передає цифрові сигнали по існуючому мідному кабелі; вибирати сучасне устаткування, що оптимально

сполучить функціональність і вартість, а також взаємодіюче з існуючими елементами мережі.

Стратегічні проблеми модернізації транспортної системи корпоративних мереж

При модернізації транспортної системи корпоративних мереж у стратегічні питання її планування включають у першу чергу наступні.

1. Створення транспортної інфраструктури з масштабованою продуктивністю для складних локальних мереж.

2. Вибір технології магістралі для великих локальних мереж підприємства. Технологія визначається використовуваними протоколами нижнього рівня, такими як Ethernet, Token Ring, FDDI, Fast Ethernet, і істотно впливає на типи використовуваного в мережі комунікаційного устаткування. Магістраль, як правило, є однієї з найбільш дорогих частин будь-якої мережі. Крім того, тому що через неї проходить значна частина трафіку мережі, те її властивості позначаються практично на всіх сервісах корпоративної мережі, якими користуються кінцеві користувачі.

3. Визначення раціональної структури магістралі. Ця структура буде потім покладена в основу структури кабельної системи, вартість якої може становити 15% і більше відсотків всієї вартості мережі. Раціональна структура магістралі повинна забезпечити компроміс між якістю передачі трафіку (пропускна здатність, затримки, пріоритети для відповідальних застосунків) і вартістю. На структуру магістралі найсильніший вплив робить обрана технологія, тому що вона визначає максимальні довжини кабелів, можливість використання резервних зв'язків, типи кабелів і т.п.

4. Вибір технології, структури зв'язків і комунікаційного устаткування для підмереж, що входять у велику локальну мережу. Для кожної підмережі це питання може вирішуватися автономно з урахуванням вимог і традицій кожного підрозділу підприємства. Однак, завжди потрібно враховувати наслідки, які пов'язані з вибором різних технологій у різних підмережах – складність об'єднання підмереж на магістралі не повинна бути надмірної.

5. Вибір способу об'єднання підмереж на магістралі, наприклад, за допомогою маршрутизації, за допомогою шлюзів або ж за допомогою комутаторів, що транслюють. При використанні у всіх підмережах однієї й тої ж технології (випадок досить рідкий для великої мережі) потреба в трансляції протоколів може відпасти, і тоді магістраль буде відрізнятися від підмереж тільки швидкістю й надійністю.

6. Вибір комунікаційного устаткування, що утворить магістраль. Після вибору способу об'єднання підмереж можна вибрати конкретні типи й моделі комунікаційного устаткування, що втілить обраний спосіб у життя.

Звичайно, крім перерахованих, існують і інші завдання, які можуть бути віднесені до стратегічного для транспортної системи корпоративної мережі того або іншого підприємства.

Математичний аспект оптимізації корпоративних мереж

Модернізація корпоративної мережі полягає в складанні плану оптимізації й розвитку мережі, виходячи із заданих обмежень на характеристики якості зв'язку й надійності, передбачуваний ріст трафіку, підключення нових вузлів зв'язку й мереж доступу, уведення в експлуатацію нових ліній зв'язку. Модернізація полягає в будівництві нових і цифровізації існуючих аналогових ліній, установці нового, заміні або переміщенні комутаційного й прикінцевого устаткування, перерозподіл існуючих інформаційних потоків.

Таке динамічне завдання пошуку оптимальної структури корпоративної мережі через ряд причин досить складна для рішення. Основна причина, що викликає утруднення при рішенні завдання – її NP-повнота, і, отже, експонентний ріст часу пошуку оптимальної структури при збільшенні числа вузлів мережі. Друга проблема – більша розмірність реальних корпоративних мереж, що робить практично неможливим пошук оптимального рішення за прийнятний час. Таким чином, можна зробити вивід про необхідність розробки обчислювального алгоритму пошуку оптимальних рішень.

У корпоративних мережах можна виділити дві складові частини – підмережа доступу й магістральну підмережа. Через підмережі доступу до корпоративної мережі підключаються користувачі. Прикладами підмереж доступу є локальні обчислювальні мережі й установські телефонні мережі. Магістральна підмережа передає транзитний трафік між підмережами доступу. Магістральна підмережа дозволяє організувати взаємодію між абонентами на більших географічних відстанях. Довжина її може становити сотні й тисячі кілометрів (вузли корпоративної мережі можуть розташовуватися в різних містах або країнах).

З математичної точки зору завдання оптимізації зводиться до пошуку мінімуму або максимуму цільової функції багатьох змінних при обмеженнях на їхні значення й функціональні зв'язки. Завдання оптимального проектування корпоративної мережі являє собою завдання нелінійного цілочисельного програмування, тому що цільова функція й обмеження є нелінійними вираженнями, у яких присутні цілочисельні змінні. Наявність значних труднощів і специфічних особливостей у рішенні цілочисельних і комбінаторних завдань оптимізації породило велику кількість методів і алгоритмів.

Розроблені методи, залежно від необхідної якості одержання результату, можна віднести до одному із двох класів:

– методи, які завжди приводять до знаходження оптимального рішення, але при реальних завданнях вимагають неприпустимо великої кількості операцій;

– методи, які не завжди приводять до знаходження оптимального рішення, але вимагають прийнятного числа операцій.

Точні методи є найбільш загальними, їх застосовують при невеликій розмірності завдання, причому час роботи алгоритму перебуває в експонентній залежності від її розмірності.

При рішенні завдань нелінійної цілочисельної оптимізації гарні результати показують методи еволюційного моделювання, а точніше один з таких методів – генетичний алгоритм. Відповідно до цього методу, корпоративна мережа представляється у вигляді ненаправленого графа, у якому вершини інтерпретуються як пристрої зв'язку, ребра – лінії зв'язку, ваги ребер – співвідношення продуктивності й пропускної здатності каналів зв'язку. Ефективність роботи генетичного алгоритму в значній мірі залежить від коректного вибору його параметрів – ймовірностей застосування генетичних операторів, методів відбору в наступні покоління, виборі потужності популяції й моменту закінчення пошуку рішення. Неправильне визначення цих параметрів може привести до збільшення часу пошуку або істотному погіршенню якості рішення, що знаходиться.

Місце проблеми інформаційної безпеки в процесі модернізації корпоративних мереж

Можна виділити цілий ряд причин, по яких варто задуматися про інформаційну безпеку корпоративної мережі.

По-перше, різноманітними функціями забезпечення інформаційної безпеки нині в достатній мері постачені існуючі продукти й технології побудови корпоративних інформаційних і телекомунікаційних систем, і ігнорувати ці можливості було б просто нерозумно.

По-друге, сучасний бізнес немислимий без активного використання публічних сервісів, надаваних відкритими мережами зв'язку, і насамперед Інтернетом. Із цієї причини корпоративна мережа повинна бути підключена до відкритих мереж, що знову ж вимагає забезпечення безпеки цього з'єднання.

По-третє, грамотно спроектована й акуратно реалізована підсистема інформаційної безпеки може істотно розширити функціональні можливості самої корпоративної мережі: побудова системи віддаленого захищеного доступу мобільних співробітників до інформаційних ресурсів корпоративної мережі; використання дешевих

Інтернет-комунікацій для передачі інформації між різними підрозділами компанії; побудова системи комп'ютерної телефонії й т.д. І нарешті, найчастіше варто просто згадати про чималу вартість накопичених за багато років інформаційних ресурсів, збережених і

оброблюваних у рамках корпоративної мережі, або про ступінь впливу оперативності й вірогідності одержуваної інформації на якість прийнятих рішень.

На практиці більшість підсистем інформаційної безпеки корпоративних мереж будується по чотирьохрівневої моделі безпеки.

Побудова будь-якої корпоративної мережі починається з установки робочих станцій, отже, підсистема інформаційної безпеки корпоративної мережі починається із захисту саме цих об'єктів. Для цього використовуються:

- штатні засоби захисту операційних систем;
- антивірусні пакети;
- додаткові пристрої автентифікації користувача;
- засоби захисту робочих станцій від несанкціонованого доступу; засобу шифрування прикладного рівня т.д.

На базі перерахованих засобів захисту інформації стоїться перший рівень підсистеми інформаційної безпеки корпоративної мережі – рівень захисту робочих станцій мережі.

На другому етапі розвитку корпоративної мережі (на практиці він часто відбувається одночасно з першим) окремі робочі станції поєднуються в локальні мережі, установлюються виділені сервери й організується вихід з локальної мережі в Інтернет. На даному етапі як засоби захисту інформації виступають:

- засоби безпеки мережних операційних систем;
- засоби розмежування доступу до поділюваних ресурсів;
- засоби захисту домену локальної мережі;
- сервери автентифікації користувачів; міжмережеві екрани й proxy-сервери;
- засоби організації VLAN;
- засоби виявлення атак і уразливості захисту локальної мережі.

Засобу захисту інформації другого рівня набагато більше складні технологічно, ніж такі засоби першого рівня, що, природно, відбивається на їхній вартості й трудомісткості установки й супроводу.

Третій етап розвитку корпоративної мережі складається в об'єднанні локальних мереж декількох філій компанії в загальну корпоративну мережу на базі сучасних IT-технологій підтримки QoS (ATM, Frame Relay, DiffServ, MPLS і ін.), з використанням як комунікаційне середовище публічних мереж, включаючи, звичайно, і Інтернет. При цьому безпека обміну інформацією через відкриті мережі забезпечується застосуванням технологій Virtual Private Network (VPN), які й становлять основу третього рівня підсистеми інформаційної безпеки корпоративної мережі. Технології VPN, як правило, досить глибоко інтегровані із засобу захисту інформації першого (засобу автентифікації користувача й захисти від несанкціонованого доступу) і другого (міжмережеві екрани й мережні операційні системи) рівнів, і захищений VPN-канал може «доходити» не тільки до маршрутизаторів доступу й прикордонних міжмережевих екранів, але й до конкретних серверів і робочих станцій локальної мережі, становлячи, таким чином, свого роду кістяк підсистеми інформаційної безпеки корпоративної мережі.

Четвертим етапом розвитку й організації захищеного міжкорпоративного обміну інформацією є група технологій і методів, що дозволяють будувати системи керування публічними ключами й сертифікатами – Public Key Infrastructure (PKI), завданнями якої є:

– створення й підпис сертифікатів, що вимагає наявності ієрархічної системи нотаріусів, тому що користувач VPN повинен одержувати свій сертифікат за місцем роботи;

– передача сертифікатів на електронний носій користувача й публікація їх на сервері сертифікатів для того, щоб будь-який учасник VPN міг легко одержати сертифікат свого партнера;

– реєстрація фактів компрометації й публікація «чорних» списків відкликаних сертифікатів.

VPN повинна взаємодіяти з PKI у цілому ряді крапок (передача сертифіката на підпис, одержання сертифіката й «чорного» списку при встановленні взаємодії й т.п.). Очевидно, що ця взаємодія з далекої стосовно VPN системою може здійснюватися тільки за умови повної підтримки міжнародних стандартів, яким відповідають більшість сучасних PKI систем.

Вертаючись до моделі підсистеми інформаційної безпеки корпоративної мережі, хочеться підкреслити ще один важливий момент. Перші три рівні «піраміди» можна віднести до засобів захисту інформації в традиційному їхньому розумінні, оскільки ці засоби покликані забезпечити власну інформаційну безпеку корпоративної мережі. Верхні два рівні явно відносяться вже до забезпечення е-бізнесу, оскільки VPN служать для побудови захищеного обміну інформацією між компаніями, а PKI надає VPN-пристроям необхідні для формування захищених каналів ключі й сертифікати. Таким чином, як ми бачимо, що VPN-технології історично позиціоновані як сполучний елемент між чисто внутрикорпоративним завданням – забезпеченням інформаційної безпеки розподіленої корпоративної мережі й глобальної бізнес-завданням компанії – забезпеченням інтеграції в систему світового електронного бізнесу XXI століття.

Складання економічного обґрунтування модернізації корпоративної мережі

Практичне обґрунтування процесу модернізації корпоративної мережі вимагає відповіді на три питання: чи дозволить модернізація заощадити компанії гроші, чи допоможе вона робити компанії гроші й чи буде вона сприяти підвищенню рівня конкурентоспроможності компанії?

Одним з популярних і порівняно простих методів оцінки є аналіз витрат, при якому загальна вартість модернізації рівняється з очікуваними вигодами. Якщо вартість модернізації виглядає прийнятної, то пропоноване проектне рішення йде на виконання. При аналізі витрат важливо також розглянути наслідку відмови від пропонованої моделі модернізації або проведення іншої модернізації. Таким чином, необхідно змоделювати кілька сценаріїв і провести аналіз для кожного з них.

Щоб установити, які будуть витрати на проект, необхідно з'ясувати загальну вартість володіння з урахуванням вартості модернізації, що течуть операцій і обслуговування й т.п. Загальна вартість володіння для кожної мережі своя, тому необхідно зібрати інформацію про специфічні для мережі витратах. У багатьох моделях загальної вартості володіння враховуються тільки витрати на мережне устаткування, що може привести до неправильних виводів. Для одержання більше коректної оцінки необхідно також розглянути первісні капітальні витрати на модернізацію мережі, включаючи витрати на залучення консультантів, навчання й висновок контрактів.

Ще однією важливою статтею витрат є витрати на експлуатацію й обслуговування. До них відносяться заробітна плата персоналу, плата за оренду приміщень, комунальні й інші послуги, страховка, штрафи за невиконання зобов'язань і недоодержання прибутку.

Незважаючи на всі труднощі фінансового обґрунтування модернізації, аналіз повинен проводитися з таким ступенем подробиці, що у стані витримати перевірку часом.

Комутатори DMS-1100-10TS і DMS-1100-10TP с підтримкою стандарту Ethernet 2.5 GBase-T

Нові мультигігабітні комутатори DMS-1100-10TS і DMS-1100-10TP с підтримкою стандарту Ethernet 2.5 GBase-T дозволяють збільшити пропускну здатність корпоративних мереж до 2,5 Гбіт/с без модернізації існуючої кабельної інфраструктури CAT5e/6

Серія DMS-1100 призначена для застосування на рівні доступу при побудові й модернізації корпоративних обчислювальних мереж, а також при створенні або модернізації корпоративних бездротових мереж на основі стандарту 802.11ac Wave 2. Комутатори оснащені 2 оптичними портами для каскадування 10Gb SFP+ і 8 портами 100/1000/2.5 GBase-T з автовизначенням швидкості з'єднання. Модель DMS-1100-10P підтримує стандарт 802.3at PoE, забезпечуючи потужність до 30 Вт на порт при загальному бюджеті PoE 240 Вт. Для підключення серверів до нових комутаторів рекомендується мережний адаптер PCI Express з 1 портом 10Gb SFP+ DXE-810S.

Конструктивно комутатори виконані в металевому корпусі з можливістю установки в 19-дюймову стійку. Кріплення входять у комплект поставки. У системі охолодження використовуються вентилятори з автоматичним керуванням швидкістю обертання. Пристрою забезпечують роботу в розширеному температурному діапазоні від -5 до 50°С.

Комутатори серії DMS-1100 підтримують функції резервування й підвищення відказостійкості мережі. Функція Loopback Detection тимчасово блокує порти комутатора, на яких виявлені петлі. Функція агрегування каналів зв'язку 802.1AX/802.3ad забезпечує балансування навантаження й збільшує пропускну здатність. Автоматичне резервування з'єднань здійснюється за допомогою протоколів STP (802.1D, 802.1w). Для швидкого відновлення зв'язку при відмові однієї з ліній у кільці (50 – 200 мс). реалізовано протокол ERPS (Ethernet Ring Protection Switching

Серія DMS-1100 підтримує 802.1p QoS, 802.1Q VLAN (до 4K груп), захист від штормів і IGMP/MLD Snooping для керування багатоадресного розсиланням. У наступній версії ПЗ буде реалізована підтримка Auto Surveillance VLAN, що забезпечує підвищення якості обслуговування трафіку відеоспостереження. Розмір таблиці комутації нових пристроїв становить 16K MAC-адрес.

Первісне налаштування комутаторів серії DMS-1100 можуть виконуватися за допомогою безкоштовної багатофункціональної утиліти D-Link Network Assistant, що дозволяє знаходити й підключатися до комутаторів, що перебувають в одному сегменті мережі, D-Link без необхідності зміни налаштувань IP-адреси комп'ютера. Основне налаштування й керування здійснюються за допомогою Web-інтерфейсу, протоколу SNMP або програмного забезпечення D-View 7 для централізованого керування мережною інфраструктурою по SNMP.

Комутатори відповідають стандарту енергоефективності Ethernet IEEE 802.3az і підтримують розширений функціонал оптимізації енергоспоживання, у т.ч. визначення поточного статусу з'єднання й довжини кабелю, відключення живлення неактивних портів і світлодіодних індикаторів, а також переклад пристрою в режим збереження електроенергії. PoE-комутатор DMS-1100-10P підтримує роботу з розкладу.

Рекомендована ціна для кінцевого користувача: DMS-1100-10TS – $615, DMS-1100-10TP – $844.

Комутатори D-Link DMS-1100 підтримують стандарт 2.5 GBase-T

Розробка структурної схеми

Виділення в системах керування типових груп функцій і розбивка цих функцій на рівні ще не дає відповіді на питання, яким же образом улаштовані системи керування, з яких елементів вони складаються і які архітектури зв'язків цих елементів використовуються на практиці.

Схема менеджер – агент

В основі будь-якої системи керування мережею лежить елементарна схема взаємодії агента з менеджером. На основі цієї схеми можуть бути побудовані системи практично будь-якої складності з більшою кількістю агентів і менеджерів різного типу.

Агент є посередником між керованим ресурсом і основною керуючою програмою-менеджером. Щоб той самий менеджер міг управляти різними реальними ресурсами, створюється деяка модель керованого ресурсу, що відбиває тільки ті характеристики ресурсу, які потрібні для його контролю й керування. Наприклад, модель маршрутизатора звичайно включає такі характеристики, як кількість портів, їхній тип, таблицю маршрутизації, кількість кадрів і пакетів протоколів канального, мережного й транспортного рівнів, що пройшли через ці порти.

Менеджер одержує від агента тільки ті дані, які описуються моделлю ресурсу. Агент же є деяким екраном, що звільняє менеджера від непотрібної інформації про деталі реалізації ресурсу. Агент поставляє менеджерові оброблену й представлену в нормалізованому вигляді інформацію. На основі цієї інформації менеджер ухвалює рішення щодо керування, а також

виконує подальше узагальнення даних про стан керованого ресурсу, наприклад, будує залежність завантаження порту від часу.

Для одержання необхідних даних від об'єкта, а також для видачі на нього керуючих впливів агент взаємодіє з реальним ресурсом деяким нестандартним способом. Коли агенти вбудовуються в комунікаційне устаткування, то розроблювач устаткування передбачає крапки й способи взаємодії внутрішніх вузлів пристрою з агентом. При розробці агента для операційної системи розроблювач агента користується тими інтерфейсами, які існують у цієї ОС, наприклад інтерфейсами ядра, драйверів і застосунків. Агент може забезпечуватися спеціальними датчиками для одержання інформації, наприклад датчиками релейних контактів або датчиками температури.

Менеджер і агент повинні розташовувати однієї й тією же моделлю керованого ресурсу, інакше вони не зможуть зрозуміти один одного. Однак у використанні цієї моделі агентом і менеджером є істотне розходження. Агент наповнює модель керованого ресурсу поточними значеннями характеристик даного ресурсу, і у зв'язку із цим модель агента називають базою даних керуючої інформації – Management Information Base, MIB. Менеджер використовує модель, щоб знати про те, чим характеризується ресурс, які характеристики він може запросити в агента і яких параметрів можна управляти.

Менеджер взаємодіє з агентами по стандартному протоколі. Цей протокол повинен дозволяти менеджерові запитувати значення параметрів, що зберігаються в базі MIB, а також передавати агентові керуючу інформацію, на основі якої той повинен управляти пристроєм. Розрізняють керування inband, тобто по тому же каналі, по якому передаються користувальницькі дані, і керування out-of-band, тобто поза каналом, по якому передаються користувальницькі дані. Наприклад, якщо менеджер взаємодіє з агентом, убудованим у маршрутизатор, за протоколом SNMP, переданому по тій же локальній мережі, що й користувальницькі дані, те це буде керування inband. Якщо ж менеджер контролює комутатор первинної мережі, що працює за технологією частотного ущільнення FDM, за допомогою окремої мережі X.25, до якої підключений агент, то це буде керування out-of-band. Керування по тому же каналі, по якому працює мережа, більш економічно, тому що не вимагає створення окремої інфраструктури передачі керуючих даних. Однак спосіб out-of-band більше надійний, тому що він надає можливість управляти устаткуванням мережі й тоді, коли якісь елементи мережі вийшли з ладу й по основних каналах устаткування недоступно. Стандарт багаторівневої системи керування TMN має у своїй назві слово Network, що підкреслює, що в загальному випадку для керування телекомунікаційною мережею створюється окрема керуюча мережа, що забезпечує режим out-of-band.

Звичайно менеджер працює з декількома агентами, обробляючи одержувані від них дані й видаючи на них керуючі впливи. Агенти можуть вбудовуватися в кероване устаткування, а можуть і працювати на окремому комп'ютері, пов'язаному з керованим устаткуванням по якому-небудь інтерфейсі. Менеджер звичайно працює на окремому комп'ютері, що виконує також роль консолі керування для оператора або адміністратора системи.

Модель менеджер – агент лежить в основі таких популярних стандартів керування, як стандарти Internet на основі протоколу SNMP і стандарти керування ISO/OSI на основі протоколу CMIP.

Агенти можуть відрізнятися різним рівнем інтелекту – вони можуть володіти як самим мінімальним інтелектом, необхідним для підрахунку минаючих через устаткування кадрів і пакетів, так і досить високим, достатнім для виконання самостійних дій по виконанню послідовності керуючих дій в аварійних ситуаціях, побудові тимчасових залежностей, фільтрації аварійних повідомлень і т.п.

Структури розподілених систем керування

У великій корпоративній мережі повністю централізована система керування, побудована на базі єдиного менеджера, навряд чи буде працювати добре з кількох причин:

– По-перше, такий варіант не забезпечує необхідної масштабованості по продуктивності, тому що єдиний менеджер змушений буде обробляти весь потік повідомлень від всіх агентів, що при декількох тисячах керованих об'єктів зажадає дуже високопродуктивної платформи для роботи менеджера й перевантажить службовою керуючою інформацією канали передачі даних у тій мережі, де буде розташований менеджер.

– По-друге, таке рішення не забезпечить необхідного рівня надійності, тому що при відмові єдиного менеджера буде загублене керування мережею.

– По-третє, у великій розподіленій мережі доцільно розташовувати в кожному географічному пункті окремим оператором або адміністратором, що управляє своєю частиною мережі, а це зручніше реалізувати за допомогою окремих менеджерів для кожного оператора.

Схема «менеджер – агент» дозволяє будувати досить складні в структурному відношенні розподілені системи керування.

Звичайно розподілена система керування включає велику кількість зв'язувань менеджер – агент, які доповнюються робочими станціями операторів мережі, за допомогою яких вони одержують доступ до менеджерів.

Кожний агент збирає дані й управляє певним елементом мережі. Менеджери, іноді також називані серверами системи керування, збирають дані від своїх агентів, узагальнюють їх і зберігають у базі даних. Оператори, що працюють за робочими станціями, можуть з'єднатися з кожним з менеджерів і за допомогою графічного інтерфейсу переглянути дані про керовану мережу, а також видати менеджерові деякі директиви по керуванню мережею або її елементами.

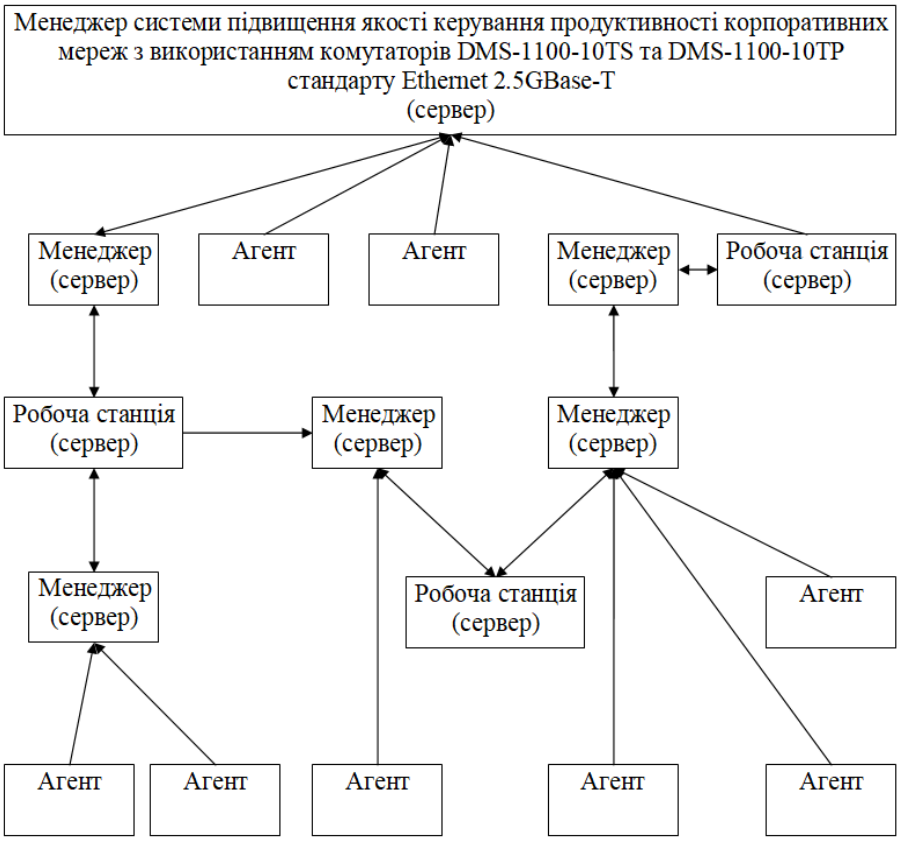


Рисунок 1 – Структурна схема системи

Наявність декількох менеджерів дозволяє розподілити між ними навантаження по обробці даних керування, забезпечуючи масштабованість системи.

Як правило, зв'язки між агентами й менеджерами носять більше впорядкований характер, ніж той, котрий показаний вище. Найчастіше використовуються два підходи до їхнього з'єднання – одноранговий і ієрархічний.

У випадку однорангових зв'язків кожний менеджер управляє своєю частиною мережі на основі інформації, одержуваної від нижчележачих агентів. Центральний менеджер відсутній. Координація роботи менеджерів досягається за рахунок обміну інформацією між базами даних кожного менеджера.

Однорангова побудова системи керування сьогодні вважається неефективним і застарілим. Звичайно воно викликано тим обставиною, що елементарні системи керування побудовані як монолітні системи, які спочатку не були орієнтовані на модульність системи (наприклад, багато систем керування, розроблені виробниками устаткування, не підтримують стандартні інтерфейси для взаємодії з іншими системами керування). Потім ці менеджери нижнього рівня стали поєднуватися для створення інтегрованої системи керування мережею, але зв'язки між ними виявилося можливим створювати тільки на рівні обміну між базами даних, що досить повільно. Крім того, у базах даних таких менеджерів накопичується занадто детальна інформація про керовані елементи мережі (тому що спочатку ці менеджери розроблялися як менеджери нижнього рівня), внаслідок чого така інформація малопригодна для координації роботи всієї мережі в цілому. Такий підхід до побудови системи керування називається підходом «знизу нагору».

Набагато більше гнучким є ієрархічна побудова зв'язків між менеджерами. Кожний менеджер нижнього рівня виконує також функції агента для менеджера верхнього рівня. Такий агент працює вже з набагато більше укрупненою моделлю (MIB) своєї частини мережі, у якій збирається саме та інформація, що потрібна менеджерові верхнього рівня для керування мережею в цілому. Звичайно для розробки моделей мережі на різних рівнях проектування починають із верхнього рівня, на якому визначається состав інформації, необхідної від менеджерів-агентів більше низького рівня, тому такий підхід названий підходом «зверху долілиць». Він скорочує обсяги інформації, що циркулює між рівнями системи керування, і приводить до набагато більше ефективної системи керування.

Модель TMN найбільшою мірою відповідає ієрархічній архітектурі зв'язків між менеджерами, хоча відомі реалізації принципів TMN і в однорівневих архітектурах.

Платформний підхід

При побудові систем керування великими локальними й корпоративними мережами звичайно використовується платформний підхід, коли індивідуальні програми керування розробляються не «з нуля», а використовують служби й примітиви, надавані спеціально розробленим для цих цілей програмним продуктом – платформою.

Ці платформи створюють загальне операційне середовище для застосунків системи керування точно так само, як універсальні операційні системи, такі як Unix або Windows NT, створюють операційне середовище для застосунків будь-якого типу, таких як MS Word, Oracle і т.п. Платформа звичайно включає підтримку протоколів взаємодії менеджера з агентами – SNMP і рідше CMIP, набір базових засобів для побудови менеджерів і агентів, а також засобу графічного інтерфейсу для створення консолі керування. У набір базових засобів звичайно входять функції, необхідні для побудови карти мережі, засобу фільтрації повідомлень від агентів, засобу ведення бази даних. Набір інтерфейсних функцій платформи утворить інтерфейс прикладного програмування (API) системи керування. Користуючись цим API, розроблювачі із третіх фірм створюють закінчені системи керування, які можуть управляти специфічним устаткуванням відповідно до п'яти основних груп функцій.

Звичайно платформа керування поставляється з яким-небудь універсальним менеджером, що може виконувати деякі базові функції керування без програмування. Найчастіше до цих функцій відносяться функції побудови карти мережі (група Configuration Management), а також функції відображення стану керованих пристроїв і функції фільтрації повідомлень про помилки (група Fault Management).

Чим більше функцій виконує платформа, тим краще. У тому числі й таких, які потрібні для розробки будь-яких аспектів роботи застосунків, прямо не зв'язаних зі специфікою керування. З рештою, застосунки системи керування – це насамперед застосунки, а потім уже застосунки системи керування. Тому корисні будь-які засоби, надавані платформою, які прискорюють розробку застосунків взагалі й розподілених застосунків зокрема.

Компанії, які роблять комунікаційне устаткування, розробляють додаткові менеджери для популярних платформ, які виконують функції керування устаткуванням даного виробника більш повно.

Висновок. У статті розглянуто та проаналізовано програмне забезпечення, яке призначено для системи підвищення якості керування продуктивності корпоративних мереж з використанням комутаторів DMS-1100-10TS та DMS-1100-10TP стандарту Ethernet 2.5GBase-T. В межах України в недостатній мірі представлені вітчизняні розробки в цій області. У роботі наведені теоретичне узагальнення й рішення наукового завдання дослідження методів підвищення якості керування продуктивності корпоративних мереж з використанням комутаторів DMS-1100-10TS та DMS-1100-10TP стандарту Ethernet 2.5GBase-T. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем підвищення якості керування продуктивності корпоративних мереж з використанням комутаторів DMS-1100-10TS та DMS-1100-10TP стандарту Ethernet 2.5GBase-T; Досліджена система підвищення якості керування продуктивності корпоративних мереж з використанням комутаторів DMS-1100-10TS та DMS-1100-10TP стандарту Ethernet 2.5GBase-T; На основі отриманих результатів досліджень створена програмна реалізація системи підвищення якості керування продуктивності корпоративних мереж з використанням комутаторів DMS-1100-10TS та DMS-1100-10TP стандарту Ethernet 2.5GBase-T. Розроблені під час виконання роботи алгоритми дозволяють успішно вирішувати завдання підвищення якості керування продуктивності корпоративних мереж з використанням комутаторів DMS-1100-10TS та DMS-1100-10TP стандарту Ethernet 2.5GBase-T. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки. Розроблене програмне забезпечення має простий, дружній та зручний інтерфейс користувача, що забезпечує легкість у освоєнні роботи програмного продукту, зручність у використанні, і не потребує особливих спеціальних знань. При створені програмного забезпечення було використано об’єктно-орієнтований підхід, що відповідає сучасним тенденціям у галузі розробки комерційних програмних систем. Програма реалізована на мові високого рівня Delphi 10.2 Tokyo. Дана мова програмування дозволяє найбільш ефективно обробляти дані. Це дозволило мінімізувати строк розробки програмного забезпечення, і, як слід, зменшити витрати на його розробку. Запропоноване програмне забезпечення ділиться на загальне програмне забезпечення, що поставляється із засобами обчислювальної техніки й спеціальне програмне забезпечення, що спеціально розроблене для даної конкретної системи й включає програми, що реалізують її функції. Даються необхідні рекомендації з установки розробленого програмного забезпечення. Для підвищення рівня безпеки запропоновано застосовувати алгоритм Md5. В цілому створене програмне забезпечення підтверджує правильність використаних проектних рішень та повністю відповідає вимогам технічного завдання. Створене програмне забезпечення має потенційну можливість для подальшого вдосконалення і застосування у різних галузях.

Список літератури

1. Босько В.В. Анализ и сравнительное исследование перспективных направлений развития цифровых телекоммуникационных систем и сетей / Смирнов А.А., Босько В.В., Мелешко Е.В. // Системи обробки інформації. – Х.: ХУ ПС, 2008. – Вип.7(74). – С.120-123.

2. Босько В.В. Разработка методики оценки среднего времени обслуживания информационных пакетов в телекоммуникационной сети / Смирнов А.А., Босько В.В., Мелешко Е.В. // Системи управління, навігації та зв'язку. – Київ: ДП «Центральний науково-дослідний інститут навігації і управління», 2009. – Вип. 2(10). – С.162-165.
3. Босько В.В. Разработка математической модели процесса динамического управления маршрутизацией данных в телекоммуникационной сети / Смирнов А.А., Босько В.В. // Системи управління, навігації та зв'язку. – К.: ДП «ЦНДІ навігації і управління», 2009. – Вип. 3(11). – С.208-210.
4. Босько В.В. Разработка метода определения оптимального множества путей передачи информации в телекоммуникационной сети / Смирнов А.А., Босько В.В. // Збірник наукових праць. – Х.: ХУПС, 2009. – Вип. 3(21). – С.102-108.
5. В.В. Босько. Разработка метода прогнозирования поведения информационного потока в телекоммуникационной сети // Збірник наукових праць. Харківського університету Повітряних Сил: – Х.:ХУ ПС, – 2010.-Вип. 3 (25) .- С.126-130.
6. Босько В.В. Исследование особенностей построения современных телекоммуникационных систем и сетей / Смирнов А.А., Босько В.В. // Проблемы информатики и моделирования. Материалы восьмой международной научно-технической конференции 26-28 ноября. – Х.: НТУ "ХПИ", 2008. – С.54.
7. Босько В.В. Исследование влияния времени мониторинга телекоммуникационной сети на точность прогнозирования поведения трафика / Смирнов А.А., Босько В.В. // Перша міжнародна науково-практична конференція "Проблеми й перспективи розвитку IT-індустрії" м. Харків , 18-19 листопада 2009р. – С.198-200.
8. Босько В.В. Анализ математических моделей телекоммуникационной сети / Смирнов А.А., Босько В.В. // Проблемы информатики и моделирования. Материалы девятой международной научно-технической конференции 26-28 ноября. – Х.: НТУ "ХПИ", 2009. – С.52-53.
9. Босько В.В. Метод повышения оперативности передачи данных в телекоммуникационной сети / Смирнов А.А., Босько В.В. // Збірник тез доповідей науково-практичної конференції "Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку" 24-25 березня. – Х.: АВВ МВС України, 2010. – С.54.
10. Босько В.В. Динамическое управление процессом маршрутизации данных в телекоммуникационной сети / Смирнов А.А., Босько В.В. // Тези доповідей Міжнародної науково-практичної конференції м. Вінниця, Україна 19-21 травня 2010 року. – Вінниця: ВНТУ, 2010. – С.231-232.

УДК 004

Р. Ткачук, магістр гр. КН-18М-1,4
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ РОЗГАЛУЖЕНОЇ ОБЧИСЛЮВАЛЬНОЇ СИСТЕМИ НА ARM КОНТРОЛЕРАХ

У статті розроблено програмне забезпечення, яке призначено для розгалуженої обчислювальної системи на ARM контролерах. Метою розробки є дослідження та програмна реалізація розгалуженої обчислювальної системи на ARM контролерах. Об'єктом дослідження є процес реалізації розгалуженої обчислювальної системи на ARM контролерах. Предметом дослідження є метод забезпечення реалізації розгалуженої обчислювальної системи на ARM контролерах. Методи дослідження базуються на методах теорії побудови мереж, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація розгалуженої обчислювальної системи на ARM контролерах. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення. Розроблено зручний інтерфейс користувача. Наведені інструкції по роботі з програмними засобами. Програма може використовуватися на ПЕОМ архітектури IBM PC з ОС Windows XP/Vista/7/8/10. Програму розроблено в середовищі Delphi XE7.
комп'ютерні науки, якість керування, продуктивність, корпоративні мережі

Постановка проблеми. Аналіз нештатних ситуацій для систем критичного застосування (СКЗ) в аерокосмічній галузі показує, що більше 50% з них носять технічний

характер (пов'язані з різними відмовами і несправностями технічних систем, з порушенням їх функціонування або руйнуванням внаслідок помилкових дій персоналу), причому більше 20% пов'язані з нестачею інформації про повітряну обстановку або несвоєчасним її отриманням. У ряді випадків (складні метеорологічні умови, наявність активних і пасивних перешкод тощо) для безпосереднього управління польотами авіації і забезпечення необхідної повноти інформації виникає необхідність в постачанні суміжним центрам управління повітряним рухом початкової (необробленої) радіолокаційної інформації (РЛІ), яка може бути класифікована як відеоінформація про повітряну обстановку. Інтенсивність інформаційних потоків при передачі цієї інформації для різних радіолокаційних станцій (РЛС) може складати від 1 до 3 Мбіт/с, що в 100 і більше разів перевищує інтенсивність обробленої радіолокаційної інформації, яка передається на даний час. Але рівень пропускної спроможності існуючих каналів зв'язку комп'ютерних мереж (КМ) СКЗ залишається незмінним. Виникає протиріччя між зростаючими об'ємами інформації, яка повинна передаватися в низькопродуктивних КМ СКЗ, і обмеженням на час її передачі.

До основних шляхів забезпечення необхідної своєчасності передачі цифрової інформації в КМ СКЗ при заданому жорстко регламентованому циклі безпосереднього управління польотами відносяться розробка і застосування методів динамічного розподілу мережевого ресурсу через програмну реалізацію розгалуженої обчислювальної системи на ARM контролерах.

Таким чином, розробка розгалуженої обчислювальної системи на ARM контролерах є актуальною задачею та складає напрямок роботи.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні розгалуженої обчислювальної системи на ARM контролерах.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація розгалуженої обчислювальної системи на ARM контролерах.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– провести порівняльний аналіз існуючих способів та методів реалізації розгалуженої обчислювальної системи на ARM контролерах;

– розробити математичну модель процесу статистичного мультиплексування в КМ СКЗ;

– розробити метод визначення множини шляхів передачі інформації в КМ СКЗ, що задовольняє вимогам своєчасності передачі цифрової інформації через розгалужену обчислювальну систему на ARM контролерах;

– розвинути метод оптимізації множини маршрутів передачі інформації в КМ СКЗ, що забезпечує мінімальне значення ймовірності спотворення інформаційних пакетів при урахуванні обмеження, яке накладається на ймовірність їх доставки до одержувача за час, який не перевищує допустиме значення;

– створити процедуру розподілу інформаційних пакетів за знайденою множиною маршрутів в КМ СКЗ, що забезпечує «збалансоване» завантаження каналів зв'язку через розгалужену обчислювальну систему на ARM контролерах;

Об'єктом дослідження є процес реалізації розгалуженої обчислювальної системи на ARM контролерах.

Предметом дослідження є метод забезпечення реалізації розгалуженої обчислювальної системи на ARM контролерах.

Методи дослідження базуються на методах теорії побудови мереж, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Проведемо аналіз системи управління авіаперевезеннями на загальнодержавному, регіональному та місцевому рівнях, означимо місце та роль розподілу мережевого ресурсу в процесі розробки розгалуженої обчислювальної системи на ARM контролерах в КМ аерокосмічних СКЗ, обґрунтуємо

вимоги до якості зв'язку при передачі інформації в КМ СКЗ та проведемо аналіз відомих методів розподілу мережевого ресурсу, а також моделей комп'ютерної мережі.

З'ясовано, що одним з основних параметрів якості зв'язку при передачі інформації в КМ СКЗ є своєчасність. Встановлено, що для забезпечення своєчасної передачі інформації про повітряну обстановку допустимий час $T_д$ доставки інформаційного пакету повинен бути не більш 0,5 с, а ймовірність ($Q^{(сч)}$) доставки інформаційного пакету до одержувача за час, який не перевищує допустиме значення, повинна бути не менш ніж 0,9.

Визначено, що найбільш ефективними та такими, які використовуються на практиці, є методи розподілу мережевого ресурсу на основі графових та потокових моделей комп'ютерної мережі.

Удосконалимо аналітичний вираз для розрахунку середнього часу $\bar{t}_{обс}^{(об)}$ обслуговування інформаційних пакетів в КМ СКЗ та визначено шляхи його зменшення. Розробимо математичну модель процесу статистичного мультиплексування в КМ СКЗ. Підтвердимо результат про те, що об'єднана система обслуговування є більш ефективною, ніж система з розділеними ресурсами (за критерієм мінімуму середнього часу доставки інформаційних пакетів). Кількісно оцінимо виграш для конкретних розподілів і значень їх параметрів. Проведено математичне моделювання процесу доставки інформації в КМ СКЗ за допомогою багатошляхової маршрутизації та визначена цільова функція задачі оптимізації.

В умовах циркуляції в КМ СКЗ однорідного трафіку задачу управління інформаційними потоками при комутації вирішують за допомогою відомих методів, але забезпечення якості зв'язку при передачі різнорідної інформації від декількох джерел представляється більш складною задачею, яка вимагає використання методу динамічного розподілу мережевого ресурсу. Припустимо, що на вхід мультиплексора надходять два потоки з різними статистичними характеристиками. Розподіли кількості вимог, що поступають в одиницю часу, описуються законами $P_1(k)$ і $P_2(k)$ з інтенсивностями λ_1 і λ_2; розподіли довжин інформаційних пакетів описуються законами $P_1(\ell_p)$ і $P_2(\ell_p)$ з середніми значеннями $\overline{\ell}_p^{(1)}$ і $\overline{\ell}_p^{(2)}$ відповідно. Пропускна спроможність вихідного каналу зв'язку обмежена фіксованою величиною ρ. Потоки можуть обслуговуватися двома мультиплексорами з пропускними спроможностями вихідних каналів ρ_1і ρ_2, або одним мультиплексором із спільним ресурсом вихідного каналу $\rho_\Sigma = \rho_1 + \rho_2$.

Припустимо, що потоки описуються однаковими законами надходження вимог і законами розподілу довжин та розрізняються лише в перші моменти $(\lambda_1 \neq \lambda_2,\ \overline{\ell}_1 \neq \overline{\ell}_2)$, що є цілком типовим для термінальних ділянок мереж.

Вирішуючи задачу про доцільність об'єднаного або роздільного обслуговування двох статистично різних потоків, використаємо критерій мінімального середнього часу $T_{срд}$ доставки інформаційних пакетів. Припустимо, що на вхід системи обслуговування, яка моделює мультиплексор, надходять пуасоновські потоки з довільним законом розподілу довжин.

Доведено, що для системи, в якій потоки обслуговуються двома роздільними мультиплексорами середній час обслуговування інформаційних пакетів в цілому розраховується як

$$\bar{t}_{обс}^{(P)} = \frac{\lambda_1}{\lambda_1 + \lambda_2} \cdot \bar{t}_{обс}^{(1)} + \frac{\lambda_2}{\lambda_1 + \lambda_2} \cdot \bar{t}_{обс}^{(2)}, \quad (1)$$

а для об'єднаної системи мультиплексування з пропускною спроможністю вихідного каналу ρ_Σ як:

$$\bar{t}_{обс}^{(об)} = t_k^{(об)} + \frac{\frac{\lambda_1}{\lambda^{(об)}}\ell_p^{(1)} + \frac{\lambda_2}{\lambda^{(об)}}\ell_p^{(2)}}{\rho_\Sigma - \left((\lambda_1+\lambda_2)\cdot k_s^{(i)}\cdot\left(\frac{\lambda_1}{\lambda^{(об)}}\ell_p^{(1)} + \frac{\lambda_2}{\lambda^{(об)}}\ell_p^{(2)}\right)\right)}, \quad (2)$$

де $t_к^{(об)}$ – інтервал часу між моментами прийому інформаційного пакету в *i*- му мультиплексорі і його встановлення в чергу на подальшу передачу; λ_i – інтенсивність вхідного потоку інформації в *i*-й мультиплексор.

Визначено, що система мультиплексування із спільним канальним ресурсом при пуасонівському вхідному потоці й експоненціальному обслуговуванні (2) завжди краще (за критерієм мінімуму середнього часу доставки інформаційних пакетів), ніж система з роздільним обслуговуванням (1). На рисунку 1 наведені криві залежності $\Delta\bar{t}_{обс} = \bar{t}_{обс}^{(P)} - \bar{t}_{обс}^{(об)}$ з параметром сімейства $\bar{\ell}_p$ від завантаження системи. При розрахунках були прийняті наступні початкові дані: $\rho_\Sigma = 400$ Кбит / с; $\lambda_1 = \lambda_2$.

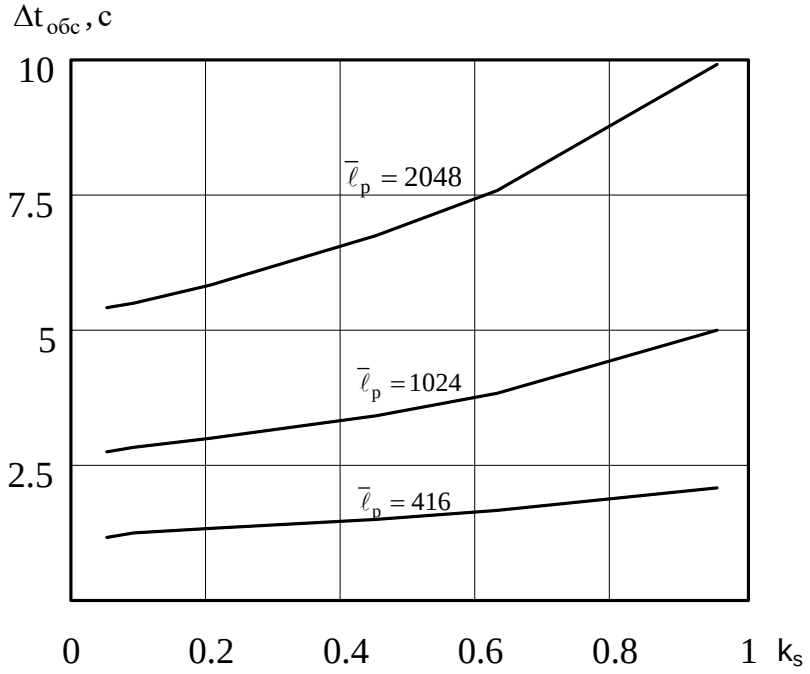


Рисунок 1 – Залежність $\Delta\bar{t}_{обс}$

З рисунку 1 видно, що виграш в часі обслуговування зростає із збільшенням завантаження, і виявляється особливо суттєвим в режимі великих завантажень. Але для фіксованого ρ_Σ виграш в часі обслуговування падає із зменшенням довжини інформаційного пакету. Це пояснюється тим, що абсолютні значенн $\bar{t}_{об\,с}^{(P)}$ і $\bar{t}_{обс}^{(об)}$ також стають незначними.

Таким чином, проведений аналіз показав, що об'єднана система обслуговування є більш ефективною, ніж система з розділеними ресурсами (за критерієм мінімального середнього часу доставки інформаційних пакетів). Представлені результати дозволяють кількісно оцінити отриманий виграш для конкретних розподілів і значень їх параметрів. Вдосконалення аналітичного виразу дозволило до 4 разів підвищити точність оцінки середнього часу обслуговування інформаційних пакетів у вузлах зв'язку КМ СКЗ.

Для визначення обмежень використання багатошляхової маршрутизації розроблена математична модель процесу доставки інформації в КМ СКЗ. Провівши перетворення Лапласа-стілтьєса ймовірність $Q^{(сч)}$ доставки інформації до одержувача за час, що не перевищує допустиме значення, розрахуємо як:

$$Q^{(сч)} = Q_{осн}^{(\mathrm{i,\,j})} \cdot P_{осн}^{(вм)} + Q_m^{(i,\,j)} \cdot \left(1 - P_{осн}^{(вм)}\right),\ m=M\text{-}1, \qquad (3)$$

де $Q_{осн}^{(\mathrm{i,\,j})} = \frac{1}{1+\gamma} \cdot \frac{1}{1+\mu} \cdot \frac{\rho_e - \lambda_{\mathrm{i,\,j}}}{\rho_e - \lambda_{\mathrm{i,\,j}} + \nu_e}$ – ймовірність доставки інформації до одержувача за час, якій не перевищує допустиме значення, за маршрутом, що складається тільки з одного каналу зв'язку $(\mathrm{i},\ \mathrm{j})$; $Q_m^{(i,\,j)} = \frac{1}{1+\gamma} \cdot \frac{1}{1+\mu} \cdot \left(\frac{e^{-\nu_e/(m\cdot\rho_э)}\left(1 - \frac{\lambda_m^{(\mathrm{i,\,j})}}{m\cdot\rho_e}\right)}{1 - \frac{\lambda_m^{(\mathrm{i,\,j})}}{\nu_e}\left(1 - e^{-\nu_e/(m\cdot\rho_e)}\right)} \right)^n$ – ймовірність доставки інформації до одержувача за час, якій не перевищує допустиме значення, по іншим маршрутам, що складаються в середньому з n вузлів зв'язку в кожному; $p_{осн}^{(вм)}$ – ймовірність вибору основного маршруту; $\rho_e = \rho_s^{(c)} \cdot k_{\mathrm{гот}}$ – експлуатаційна пропускна спроможність c-го каналу зв'язку s-го маршруту; $\lambda_{\mathrm{i,\,j}} = k_{i,\,j} \cdot \lambda$ – інтенсивність потоку інформації в каналі зв'язку $(\mathrm{i},\ \mathrm{j})$; $\nu_e = \nu \cdot \left(\frac{1 + \rho_e k_{\mathrm{пр}}}{\nu k_{\mathrm{гот}} + \mathrm{d}} \right)$ – еквівалентна інтенсивність старіння; $\nu = 1/T_{доп}$ – інтенсивність старіння; d – інтенсивність відновлення каналів зв'язку; $k_{гот}$ – коефіцієнт готовності каналу зв'язку; $\gamma = \nu / r$ – відносна інтенсивність старіння за інтенсивністю комутації; $\mu = \nu / z$ – відносна інтенсивність старіння за інтенсивністю розповсюдження; $k_{\mathrm{пр}} = 1 - k_{\mathrm{гот}}$ – коефіцієнт простою каналу зв'язку.

Проведене моделювання процесу передачі інформації та аналіз його результатів показали зменшення ймовірності $Q^{(сч)}$ доставки інформації до одержувача за час, який не перевищує допустиме значення, при зменшенні кількості маршрутів передачі інформації та збільшенні інтенсивності потоку інформації в каналі зв'язку, що ілюструє рисунок 2. Таким чином, проведене моделювання визначило необхідність застосування багатошляхової маршрутизації при високому навантаженні на КМ СКЗ.

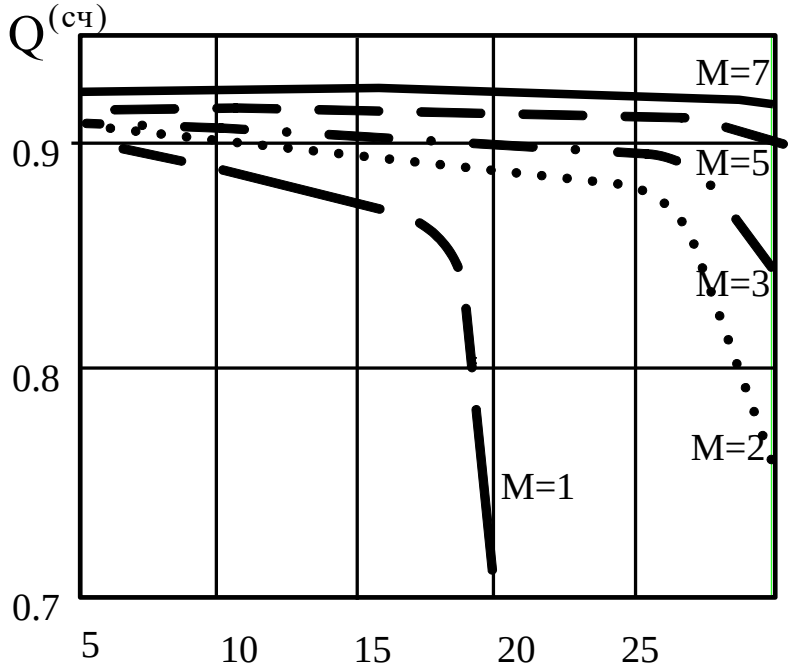


Рисунок 2 – Залежність ймовірності $Q^{(сч)}$ від кількості M маршрутів передачі інформації та інтенсивності λ

Аналіз виразу (2) та врахування того, що основним параметром, який впливає на своєчасність передачі цифрової інформації про повітряну обстановку, є середній час доставки інформаційного пакету, дозволяють вибрати цільову функцію завдання маршрутизації і розподілу інформаційних потоків у вигляді

$$\max_{s}\left\{k_s\sum_{c=1}^{\Psi_s}\left(\frac{\ell_p\cdot k_s^{(c)}}{k_s^{(c)}\cdot\rho_s^{(c)}-\lambda\cdot\ell_p\cdot k_s}\right)\right\}. \qquad (4)$$

Розробка структурної схеми

Запропонуємо метод розгалуженої обчислювальної системи на ARM контролерах в КМ СКЗ.

Джерелом інформації в КМ СКЗ є *i*-й вузол зв'язку (ВЗ), щодо якого розглянуті такі множини: $U=\{u_\alpha \mid \aleph(u_\alpha)\subset\aleph\}$ – рівні ієрархії на дереві допустимих маршрутів; $\aleph_{баз}=\bigcup_{u_\alpha=1}^{|U|}\aleph(u_\alpha)$ – найдені шляхи передачі інформації, де u_α – номер рівня ієрархії. Формування множини $\aleph_{баз}$ для кожного вузла «*i*» є ітераційним процесом покрокового додавання вузлів з відповідним рівнем ієрархії із множини U, що збільшує число альтернативних шляхів передачі інформації з вузла «*i*» та створює передумову мінімізації середнього часу $T_{срд}$ доставки інформаційних пакетів в КМ СКЗ. Але збільшення числа рівнів ієрархії призводить до ускладнення алгоритмів розрахунку топології, що, в свою чергу, викликає зростання часу формування множини $\aleph_{баз}$. Тому після кожного кроку додавання вузлів відповідного рівня ієрархії доцільно перевіряти можливість забезпечення своєчасності передачі інформації знайденими на цьому кроці маршрутами з урахуванням коефіцієнта $k_s^{(баз)}=(k_1^{(баз)},...,k_M^{(баз)})$. Це дозволить розподілити інформаційні пакети в залежності від «відстаней» $T_{i,j}=(T_{i,j}^{(1)},...,T_{i,j}^{(M)})$ кожного з маршрутів (i, j). Припущення, які були зроблені, дозволяють сформулювати оптимізаційну задачу пошуку значень $\aleph(u_\alpha)$:

$$U=\{u_\alpha \mid \aleph(u_\alpha)\subset\aleph\}\to min; \qquad (5)$$

$$\aleph_{баз} = \bigcup_{u_\alpha=1}^{|U|} \aleph(u_\alpha), \quad |U| \geq 1, \quad |U| < \max_{\eta_m \in \aleph} |\eta_m|; \tag{6}$$

$$k_s^{(баз)} = T_{i,j}^{(s)} / \sum_{s=1}^{M} T_{i,j}^{(s)}; \tag{7}$$

$$T_{\text{срд}}(\bigcup_{u'_\alpha \leq u_\alpha} \aleph(u'_\alpha)) \leq T_{доп} \quad \forall u_\alpha \in U; \tag{8}$$

$$Q^{(сч)}(\bigcup_{u'_\alpha \leq u_\alpha} \aleph(u'_\alpha)) \geq Q_{доп}. \tag{9}$$

Незважаючи на переваги (використання множини шляхів передачі інформації, пропорційний розподіл потоку інформації по каналах зв'язку), такий підхід до розподілу мережевого ресурсу має ряд недоліків, зокрема відсутність врахування ймовірності спотворення інформації на базовій множині маршрутів, що росте із збільшенням $|\aleph_{баз}|$ і структурних особливостей вибраних маршрутів. Для усунення вказаних недоліків на наступному етапі рішення задачі забезпечення своєчасності необхідно знайти оптимальну множину маршрутів передачі інформації.

Встановлено, що для каналу $c \in \Im$ маршруту $s \in \aleph_{баз}$ ймовірність спотворення одного біта рівно $q_s^{(c)}$, тобто ймовірність неспотворення біта дорівнює $p_s^{(c)} = 1 - q_s^{(c)}$. Тоді для пуассонівського потоку інформації інтенсивністю $\lambda \cdot k_s$ з пакетом довжиною ℓ_p, що проходить *c*-м каналом зв'язку *s*-го маршруту, за час Δt ймовірність неспотворення інформації дорівнює $p_s^{(c)}(\Delta t) = (1 - q_s^{(c)})^{\lambda k_s \ell_p \Delta t}$. Відповідно, ймовірність $p_s(\Delta t)$ неспотворення інформації при передачі її *s*-м маршрутом за час Δt дорівнює $p_s(\Delta t) = \prod_{c \in \eta_s} (1 - q_s^{(c)})^{\lambda k_s \ell_p \Delta t}$, тобто при передачі інформаційного потоку інтенсивністю λ з використанням багатошляхової маршрутизації на базовій множині $\aleph_{баз}$ маршрутів ймовірність $p(\aleph_{баз}, \Delta t)$ неспотворення дорівнює $p(\aleph_{баз}, \Delta t) = \prod_{s \in \aleph_{баз}} \prod_{c \in \eta_s} (1 - q_s^{(c)})^{\lambda k_s \ell_p \Delta t}$ і, відповідно, ймовірність $q(\aleph_{баз}, \Delta t)$ спотворення за тих самих умов дорівнює

$$q(\aleph_{баз}, \Delta t) = 1 - \prod_{s \in \aleph_{баз}} \prod_{c \in \eta_s} (1 - q_s^{(c)})^{\lambda k_s \ell_p \Delta t}. \tag{10}$$

Враховуючи, що в запропонованому підході знаходження базової множини маршрутів при багатошляховій маршрутизації необхідно понизити рівень спотворення передачі інформації про повітряну обстановку, задача оптимізації розподілу потоку інтенсивністю λ в середовищі базової множини маршрутів $\aleph_{баз}$ формулюється таким чином:

$$q(\aleph_{баз}, \Delta t) \xrightarrow{\aleph_{вб}} min; \tag{11}$$

при:

$$k_s = \frac{1 - t_s / \sum_{s \in \aleph_{вб}} t_s}{|\aleph_{вб}| - 1}, \quad \aleph_{вб} \subset \aleph_{баз}; \tag{12}$$

$$T_{\text{срд}}(\aleph_{баз}) \leq T_{доп}; \tag{13}$$

$$Q^{(сч)}(\aleph_{баз}) \geq Q_{доп}; \tag{14}$$

$$p_s(\Delta t) \geq p_{доп}(\Delta t); \tag{15}$$

де $\aleph_{вб}$ – множина маршрутів передачі інформації, вибраних з множини $\aleph_{баз}$ для зменшення ймовірності $q(\aleph_{баз}, \Delta t)$; t_s – «відстань» від джерела до адресата на s-му маршруті; $p_{доп}(\Delta t)$ – допустима ймовірність неспотворення біта інформації переданого маршрутом за час Δt.

При незнаходженні жодного розподілу з множиною $\aleph_{баз}$, що задовольняє обмеженням (14) – (18), розширюємо $\aleph_{баз}$ шляхом його об'єднання з множиною маршрутів наступного рівня ієрархії відповідно до виразів (8) – (12).

Таким чином, рішення задачі розгалуженої обчислювальної системи на ARM контролерах в КМ СКЗ складається з чотирьох етапів:

– визначення множини $\aleph_{баз}$ маршрутів передачі інформації;

– знаходження оптимальної множини маршрутів передачі цифрової інформації в телекомунікаційній мережі $\aleph_{вб}$;

– обчислення коефіцієнтів $\tilde{k}_s$ розподілу інформаційного потоку і управління навантаженням КМ СКЗ;

– створення та оновлення таблиці маршрутизації.

Структурна схема методу розгалуженої обчислювальної системи на ARM контролерах наведена на рисунку 3.

При рішенні задачі визначення множини $\aleph_{баз}$ шляхів передачі інформації в КМ СКЗ для ВЗ «*i*» та «*j*» з множини $\Re$ вузлів зв'язку спочатку необхідно знайти найкоротшу «відстань» (мінімальний час передачі інформаційних пакетів) $T_{i,j\,min}$ від джерела «*i*» до адресата «*j*» і множини $S_j^{(i)}$ вузлів, найближчих ВЗ «*i*» за напрямом руху потоку до «*j*» (множина «вузлів-наступників») у порядку рівнів ієрархії дерева допустимих маршрутів множини U.

При рішенні поставленої в (11) – (15) задачі відомими алгоритмами пошуку найкоротших шляхів в більшості практичних випадків маємо проблему «зациклення» при передачі інформації в знайдених шляхах. Це призводить до збільшення часу передачі інформаційних пакетів, а деколи і до їх втрати. Уникнути «зациклення» при передачі інформації пропонується шляхом додання обмежень (умова постійної відсутності циклів), які надані у вигляді виразів:

$$T_{k,j} \le T_{i,j\,min}; \tag{16}$$

$$T_{k,j\,min} \le T_{i,k,j},\ k \subset R, \tag{17}$$

де $T_{k,j\,min}$ – найкоротша «відстань» (мінімальний час передачі інформаційних пакетів) від вузла «*k*» до адресата «*j*»; $T_{i,k,j}$ – «відстань» (час передачі інформаційних пакетів) від вузла «*i*» до адресата «*j*» через вузол «*k*».

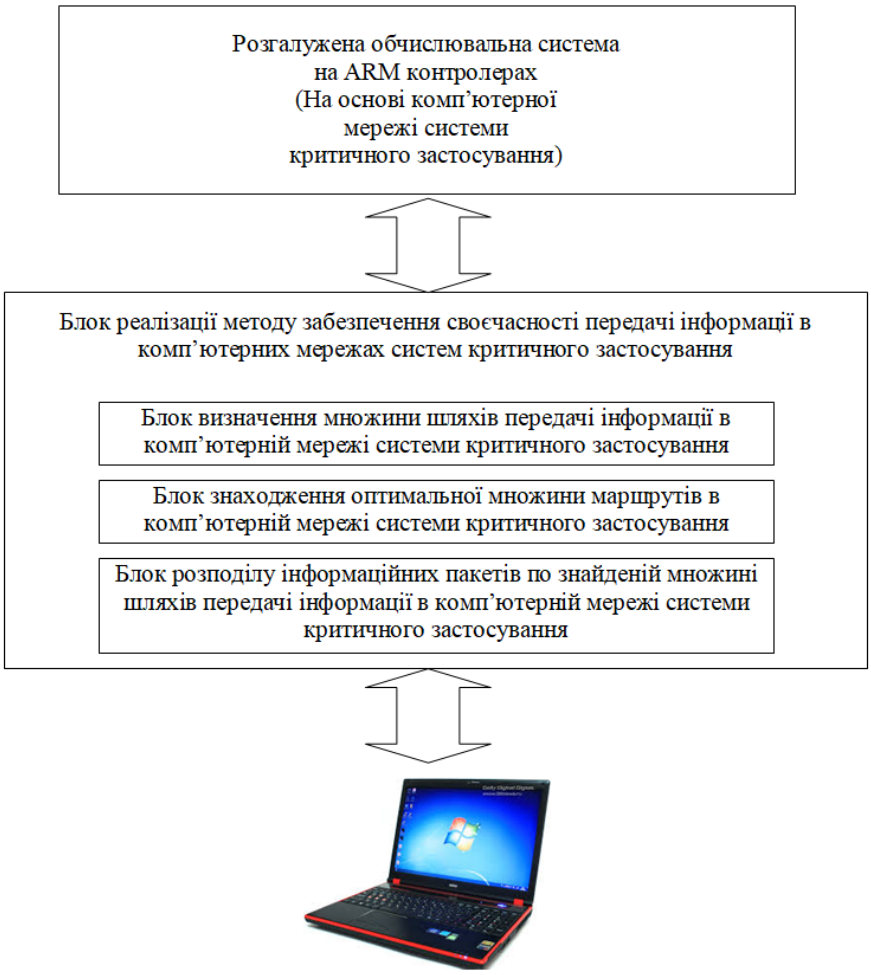


Рисунок 3 – Структурна схема системи

Рішення задачі пошуку множини шляхів, що виключають «цикли», складається з двох етапів: визначення найкоротшої «відстані» $T_{i,j\,min}$ від джерела «*i*» до адресата «*j*»; знаходження множини $S_j^{(i)}$ «вузлів-наступників» на маршрутах, що виключають «циклічність», для довільних джерел «*i*» та адресатів «*j*» за порядком множини U рівнів ієрархії дерева вибору допустимих маршрутів.

На першому етапі для визначення найкоротшої «відстані» $T_{i,j\,min}$ доцільно використати алгоритм розрахунку попередньої топології, який забезпечує вузли зв'язку інформацією про стан зв'язків для обчислення найкоротших шляхів до адресатів. Алгоритм створено на основі відомих алгоритмів стану зв'язків. На відміну від відомих, в цьому алгоритмі враховується ієрархічність побудови КМ СКЗ (визначаються «відстані» від «вузла-джерела» *i* до «адресата» *j* відповідно до існуючих рівнів ієрархії), що надалі дозволить здійснити пропорційний (з урахуванням коефіцієнтів k_s і $k_s^{(c)}$) розподіл інформації по знайдених маршрутах.

На другому етапі для знаходження множини шляхів передачі інформації, що виключають «циклічність», використовується алгоритм розповсюдження попередньої топології множини шляхів. На відміну від відомих алгоритмів, в яких не враховується поточний стан ВЗ «*i*» обов'язкова синхронізація обміну службовими повідомленнями про стан зв'язків по всій мережі, в алгоритмі розповсюдження попередньої топології множини шляхів такій синхронізації підлягає тільки один перехід між сусідніми вузлами. Це значно спрощує

роботу вузлів зв'язку і скорочує час збіжності алгоритмів. Сукупність алгоритмів розрахунку попередньої топології і розповсюдження попередньої топології множини шляхів є основою способу визначення множини шляхів передачі інформації. Запропонований спосіб (крива 3, рисунок 4, а) за відсутністю флуктуацій трафіку зіставлений з аналогічними (крива 1 – спосіб Галлагера, крива 2 – модифікований дистанційно-векторний (MDVA)) за часом затримки передачі інформації, проте у декілька разів перевершує їх при різких флуктуаціях вхідного трафіку (рисунок 4, б).

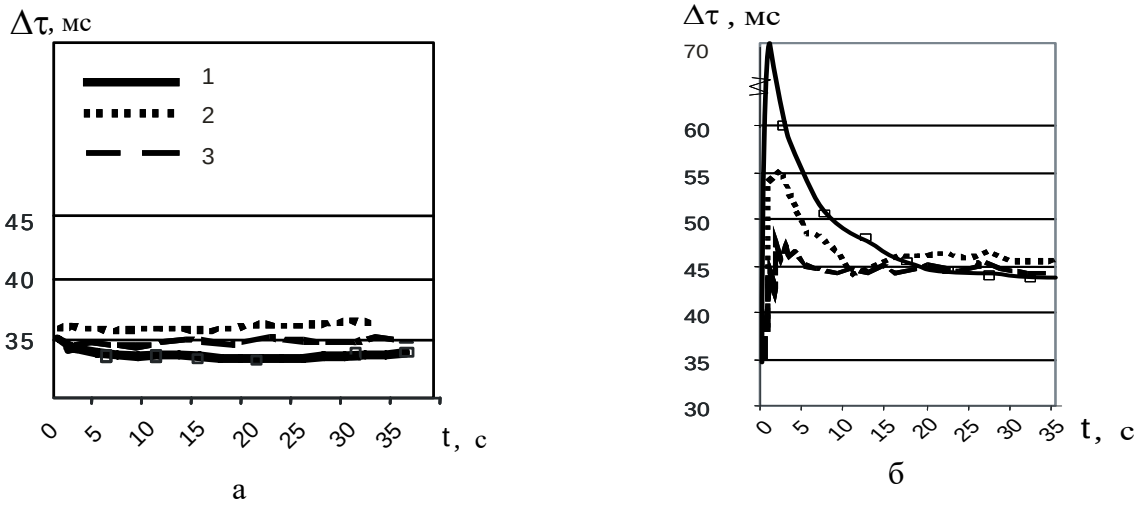


Рисунок 4 – Час затримки інформації: а – при статичному трафіку, б – при флуктуації трафіку від 3 до 10 Мбіт/с

Безпосереднє використання всієї знайденої множини $\aleph_{баз}$ шляхів передачі інформації розробленим способом не завжди є виправданим, особливо у разі високої пропускної спроможності декількох з наявних каналів зв'язку, здатних забезпечити виконання вимог (8), (9) при передачі інформації про повітряну обстановку. Розширення такої множини призводить до збільшення таблиць маршрутизації вузлів зв'язку, ускладнення процесу розподілу інформації і, як наслідок, до зниження достовірності передачі цифрової інформації. Тому виникає необхідність в знаходженні такої топології підмережі, тобто у виборі зі всієї знайденої множини $\aleph_{баз}$ шляхів деякої (оптимальної) сукупності $\aleph_{вб}$ маршрутів, використання якої в умовах обмежень, що накладаються, дозволить забезпечити максимально можливу достовірність передачі інформації.

З урахуванням (10) в умовах, описаних вище, одержані і наведені на рисунку 5 криві залежності ймовірності $q(\aleph_{баз}, \Delta t)$ від λ. Збільшення числа *M* використаних маршрутів, призводить до істотного (у 2,3…3,4 разів) збільшення ймовірності $q(\aleph_{баз}, \Delta t)$ спотворення інформації в процесі її передачі. Слід особливо відзначити, що для відомих методів розподілу характерна відсутність моніторингу поточного завантаження маршрутів, змін вхідного потоку інформації, а інколи і технічного стану каналів зв'язку. Принцип рівномірного завантаження вибраних *M* маршрутів, який використовується в таких методах, призводить до перевантаження одних і до неефективного використання інших маршрутів.

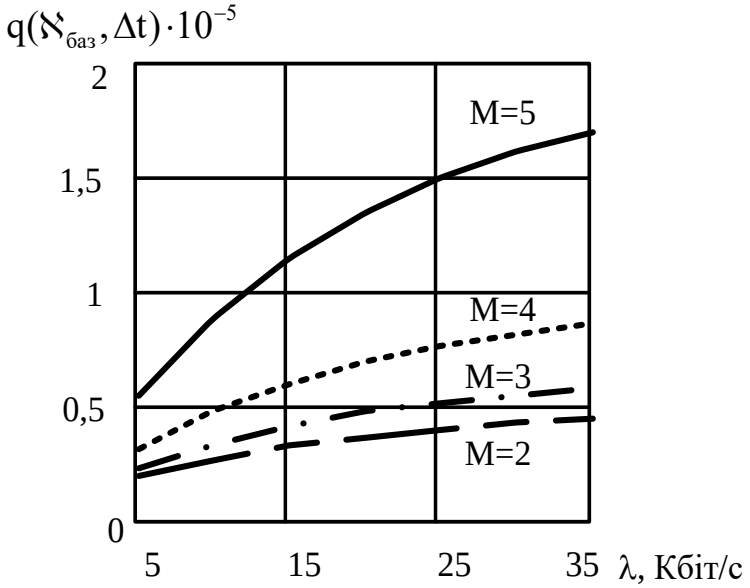


Рисунок 5 – Залежність ймовірності $q(\aleph_{баз}, \Delta t)$ спотворення інформаційних пакетів від інтенсивності λ вхідного потоку інформації

Для визначення початкового завантаження підмережі КМ СКЗ пропонується проводити розрахунок коефіцієнтів $k_s^{i,k,j}$ розподілу потоку інформації від джерела «*i*» до адресата «*j*» між «вузлами-наступниками» «*k*» з *M*-мірної множини $S_j^{(i)}$ залежно від значень «відстані» (часу передачі пакетів) між ВЗ на маршруті за співвідношенням:

$$k_s^{i,k,j} = \left(1 - \left(T_{k,j} + t_{i,k}\right) \Big/ \sum_{\xi \in S_j^{(i)}} \left(T_{\xi,j} + t_{i,\xi}\right)\right) \Big/ \left(\left|S_j^{(i)}\right| - 1\right), \quad k \in S_j^{(i)}, \tag{18}$$

де $T_{k,j}$ – час передачі пакетів від «вузла-наступника» «*k*» до адресата «*j*» на маршруті (i, j); $t_{i,k}$ – «відстань» від джерела «i» до «вузла-наступника» «*k*»; $\left|S_j^{(i)}\right|$ – потужність множини $S_j^{(i)}$.

На рисунку 6 і 7 наведені відповідно залежності середнього часу $T_{срд}$ доставки інформаційних пакетів в КМ СКЗ і ймовірність $Q^{(сч)}$ їхньої доставки за час, що не перевищує допустиме значення, від інтенсивності λ вхідного потоку інформації для повнозв'язного фрагменту КМ СКЗ в умовах мінімальної $(\rho_{min} = 16\ \text{Кбіт/с})$, максимальної $(\rho_{\max} = 30\ \text{Кбіт/с})$, середньої $(\rho_z = 19\ \text{Кбіт/с})$ пропускної спроможності каналів зв'язку (умови (I) – суцільні криві), $\rho_{min} = 14\ \text{Кбіт/с}$, $\rho_{\max} = 300\ \text{Кбіт/с}$, $\rho_z = 70\ \text{Кбіт/с}$ (умови (II) – пунктирні криві) при кількості маршрутів *M*=5. Параметром сімейства кривих є метод розподілу мережевого ресурсу в КМ СКЗ («1» – статичний метод, «2» і «3» – відповідно відомий (MDVA) і адаптивний до умов початкового завантаження мережі методи розподілу).

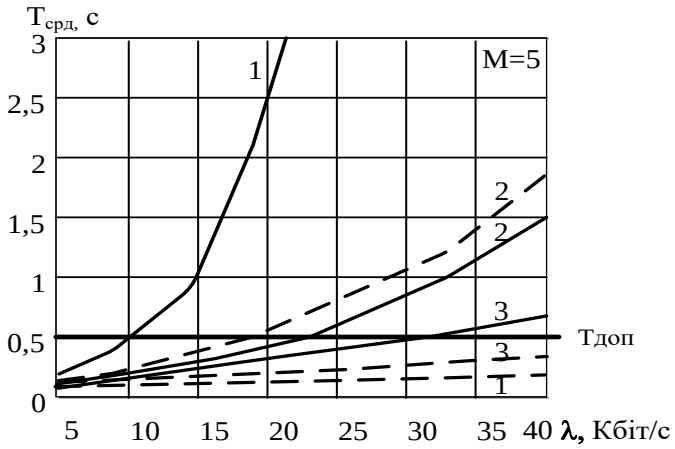


Рисунок 6 – Залежності середнього часу $T_{срд}$ від інтенсивності λ

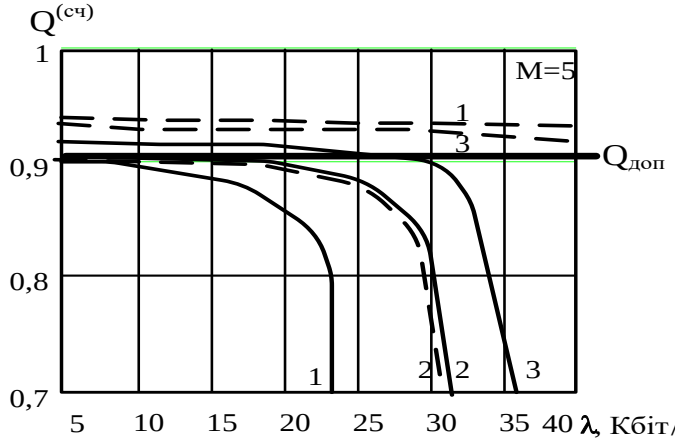


Рисунок 7 – Залежності ймовірності $Q^{(сч)}$ від інтенсивності λ

Аналіз залежностей показав, що у деяких ситуаціях адаптивний розподіл потоку інформації дозволяє «заощадити» 2 і більш маршрутів і тим самим додатково понизити ймовірність $q(\aleph_{баз}, \Delta t)$ порівняно з відомими методами управління, що свідчить про необхідність оптимізації топології підмережі КМ СКЗ. В роботі пропонується метод знаходження оптимальної множини маршрутів в КМ СКЗ, який включає постановку завдання та процедуру знаходження оптимальної множини маршрутів в КМ СКЗ. При цьому визначення початкового завантаження підмережі дозволяє найкращим чином розподілити потік пакетів, тим самим мінімізуючи $T_{срд}$ і максимізуючи $Q^{(сч)}$ в даних умовах.

В подальшому, для передачі інформації про повітряну обстановку та забезпечення «збалансування» загрузки при флуктуаціях трафіку виконується процедура розподілу інформаційних пакетів за оптимальною множиною маршрутів в КМ СКЗ.

Висновок. У статті розглянуто та проаналізовано програмне забезпечення, яке призначено для методу забезпечення своєчасності передачі інформації в комп'ютерних мережах систем критичного застосування. В межах України в недостатній мірі представлені вітчизняні розробки в цій області. Основні висновки роботи: 1. Проведено огляд існуючих методів управління мережними ресурсами КМ СКЗ. Зроблено висновок, що одним з ефективних шляхів забезпечення необхідної своєчасності передачі інформації про повітряну обстановку є динамічний розподіл. Порівняльний аналіз існуючих методів розподілу показав, що ряд їх недоліків ускладнює рішення цієї задачі. Тому одним з перспективних

напрямів розвитку методів розподілу мережевого ресурсу є адаптація цього процесу до динамічних змін інтенсивності потоку інформації про повітряну обстановку. 2. Розроблено математичну модель процесу статистичного мультиплексування в КМ СКЗ. Дана модель відрізняється від відомих тим, що в ній враховано вплив інтенсивності інформаційних потоків в каналах зв'язку, їх залишкова пропускна спроможність та особливості статистичного мультиплексування. Введення нормуючих коефіцієнтів розподілу потоків цифрової інформації у аналітичний вираз для розрахунку середнього часу обслуговування інформаційних пакетів в КМ СКЗ дозволило до 4 разів підвищити точність оцінки середнього часу обслуговування інформаційних пакетів у вузлах зв'язку КМ СКЗ.3. Розроблено метод визначення множини шляхів передачі інформації в КМ СКЗ, який полягає в комплексному використанні алгоритмів побудови попередньої топології і знаходження «вузлів-наступників» на маршрутах до кожного адресата для виключення «зациклення» при передачі інформації в КМ СКЗ, що дозволить до 2…4 разів скоротити інтервал стабілізації часу затримки пакетів при різких флуктуаціях трафіку. 4. Запропоновано метод оптимізації множини маршрутів передачі інформації в КМ СКЗ, який забезпечує мінімальне значення ймовірності спотворення інформаційних пакетів при урахуванні обмеження, що накладається на ймовірність їх доставки до одержувача за час, який не перевищує допустиме значення. Це дозволить до 2…3 разів зменшити ймовірність спотворення інформаційних пакетів при забезпеченні необхідної своєчасності передачі цифрової інформації.5. Створена процедура розподілу інформаційних пакетів за знайденою множиною маршрутів в КМ СКЗ, які базуються на методах:управління навантаженням підмережі КМ СКЗ – дозволяє своєчасно реагувати на динамічні зміни параметрів комп'ютерної мережі та здійснювати перерозподіл інформаційних потоків за множиною маршрутів КМ СКЗ і зберігає «збалансованість» каналів зв'язку, яка досягнута на етапі реалізації методу; фрагментації інформаційних пакетів – здійснюється при необхідності передачі інформаційних пакетів великого розміру мережею, що вимагає його зменшення; модифікації таблиці маршрутизації – полягає в доповненні таблиці маршрутизації інформацією про значення інтенсивності потоку інформації, розподіленої по маршрутах. 6. Розроблені практичні рекомендації щодо використання методу забезпечення своєчасності передачі інформації в КМ СКЗ в процесі управління повітряним рухом. Проведена оцінка ефективності розробленого методу при передачі інформації про повітряну обстановку. Показано, що використовування останнього при передачі інформації про повітряну обстановку в КМ СКЗ дозволить: до 3 раз підвищити ймовірність доставки інформації за час, що не перевищує допустиме значення; до 3…15 разів знизити середній час доставки інформаційних пакетів. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки. Розроблене програмне забезпечення має простий, дружній та зручний інтерфейс користувача, що забезпечує легкість у освоєнні роботи програмного продукту, зручність у використанні, і не потребує особливих спеціальних знань. При створені програмного забезпечення було використано об’єктно-орієнтований підхід, що відповідає сучасним тенденціям у галузі розробки комерційних програмних систем. Програма реалізована на мові високого рівня Delphi XE7. Дана мова програмування дозволяє найбільш ефективно обробляти дані. Це дозволило мінімізувати строк розробки програмного забезпечення, і, як слід, зменшити витрати на його розробку. Запропоноване програмне забезпечення ділиться на загальне програмне забезпечення, що поставляється із засобами обчислювальної техніки й спеціальне програмне забезпечення, що спеціально розроблене для даної конкретної системи й включає програми, що реалізують її функції. Програма призначена для виконання під управлінням багатозадачної операційної системи Windows XP/Vista/7/8/10. Даються необхідні рекомендації з розгортання системи для методу забезпечення своєчасності передачі інформації в комп’ютерних мережах систем критичного застосування. Для підвищення рівня безпеки запропоновано застосовувати алгоритм DSA. В цілому створене програмне

забезпечення підтверджує правильність використаних проектних рішень та повністю відповідає вимогам технічного завдання. Створене програмне забезпечення має потенційну можливість для подальшого вдосконалення і застосування у різних галузях.

Список літератури

1. Босько В.В. Анализ и сравнительное исследование перспективных направлений развития цифровых телекоммуникационных систем и сетей / Смирнов А.А., Босько В.В., Мелешко Е.В. // Системи обробки інформації. – Х.: ХУ ПС, 2008. – Вип.7(74). – С.120-123.
2. Босько В.В. Разработка методики оценки середнего времени обслуживания информационных пакетов в телекоммуникационной сети / Смирнов А.А., Босько В.В., Мелешко Е.В. // Системи управління, навігації та зв'язку. – Київ: ДП «Центральний науково-дослідний інститут навігації і управління», 2009. – Вип. 2(10). – С.162-165.
3. Босько В.В. Разработка математической модели процесса динамического управления маршрутизацией данных в телекоммуникационной сети / Смирнов А.А., Босько В.В. // Системи управління, навігації та зв'язку. – К.: ДП «ЦНДІ навігації і управління», 2009. – Вип. 3(11). – С.208-210.
4. Босько В.В. Разработка метода определения оптимального множества путей передачи информации в телекоммуникационной сети / Смирнов А.А., Босько В.В. // Збірник наукових праць. – Х.: ХУПС, 2009. – Вип. 3(21). – С.102-108.
5. В.В. Босько. Разработка метода прогнозирования поведения информационного потока в телекоммуникационной сети // Збірник наукових праць. Харківського університету Повітряних Сил: - Х.:ХУ ПС, - 2010.-Вип. 3 (25) .- С.126-130.
6. Босько В.В. Исследование особенностей построения современных телекоммуникационных систем и сетей / Смирнов А.А., Босько В.В. // Проблемы информатики и моделирования. Материалы восьмой международной научно-технической конференции 26-28 ноября. – Х.: НТУ "ХПИ", 2008. – С.54.
7. Босько В.В. Исследование влияния времени мониторинга телекоммуникационной сети на точность прогнозирования поведения трафика / Смирнов А.А., Босько В.В. // Перша міжнародна науково-практична конференція "Проблеми й перспективи розвитку IT-індустрії" м. Харків , 18-19 листопада 2009р. – С.198-200.
8. Босько В.В. Анализ математических моделей телекоммуникационной сети / Смирнов А.А., Босько В.В. // Проблемы информатики и моделирования. Материалы девятой международной научно-технической конференции 26-28 ноября. – Х.: НТУ "ХПИ", 2009. – С.52-53.
9. Босько В.В. Метод повышения оперативности передачи данных в телекоммуникационной сети / Смирнов А.А., Босько В.В. // Збірник тез доповідей науково-практичної конференції "Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку" 24-25 березня. – Х.: АВВ МВС України, 2010. – С.54.
10. Босько В.В. Динамическое управление процессом маршрутизации данных в телекоммуникационной сети / Смирнов А.А., Босько В.В. // Тези доповідей Міжнародної науково-практичної конференції м. Вінниця, Україна 19-21 травня 2010 року. – Вінниця: ВНТУ, 2010. – С.231-232.

УДК 631. 37

О. Тулицький, магістр гр. АТ-18М(1,9)
Центральноукраїнський національний технічний університет

ФАКТОРИ, ЩО ВПЛИВАЮТЬ НА ВИТРАТИ ПАЛИВА АВТОМОБІЛІВ

Розглянуті основні фактори, що впливають на витрати палива автомобілів. З метою систематизації шляхів і джерел економії палива, запропонована класифікація факторів, що впливають на витрати палива автомобілів. Зроблений висновок, що ефективне використання палива на автомобільному транспорті може бути досягнуто за рахунок комплексних конструкторських, технологічних і організаційних заходів на етапі проектування, виготовлення, експлуатації та обслуговування автомобілів
витрати палива, автомобіль, фактори, економія, ефективність

Економне та раціональне використання паливно-енергетичних ресурсів - одна з найбільш важливих світових проблем. Особливо гостро ця проблема стоїть на автомобільному транспорті, що належить до найбільш енергоємних галузей. Ефективне використання палива на автомобільному транспорті може бути досягнуто за рахунок спеціальних конструкторських, технологічних заходів при розробці, створенні, експлуатації і обслуговуванні автомобіля, вдосконаленні організаційно-технічних служб, раціональним управлінням автомобілями та ін. Враховуючи усе різноманіття чинників, що впливають на витрату палива автомобіля, запропонована їх класифікувати виходячи з таких показників [1-7]:

- конструкційні;
- технологічні;
- експлуатаційні;
- організаційні;
- природно-кліматичні.

Основними конструкційними факторами, що впливають на паливну економічність автомобіля, є: тип і конструктивні особливості двигуна [1]. Так мінімальні витрати палива у дизелів приблизно на 30% нижче, ніж у карбюраторних двигунів. Переваги дизелів полягають в меншій залежності питомих витрат від міри використання потужності двигуна. Значний вплив на витрати палива мають також маса автомобіля та його розміри, від яких залежать сили опору руху. Оскільки сила опору прямо пропорційна масі автомобіля, то збільшення маси автомобіля призводить відповідно до збільшення витрати палива. До конструктивних факторів слід також віднести ефективність конструкції, якість проектування вузлів і агрегатів, якість виготовлення деталей, якість збирання вузлів і агрегатів та в цілому автомобіля.

Вплив технологічних факторів на витрату палива пов'язані, в основному, з величиною допусків і якості обробки основних елементів автомобіля, з якістю проведення складальних і контрольно-регулювальних операцій, а також з ефективністю метрологічного забезпечення автомобілебудівних і ремонтних заводів, автотранспортних підприємств і СТО. До цієї групи факторів слід також віднести забезпечення автопідприємства персоналом, кваліфікація персоналу, застосування раціональних норм витрат палива, вдосконалення технології ТО і ПР [2, 3].

До найбільш важливих експлуатаційних факторів, що визначають ефективність паливовикористання в умовах транспортного процесу, відносять: організацію дорожнього руху; технічний стан рухомого складу і автомобільних доріг; майстерність водіїв; атмосферні умови; коефіцієнти використання вантажопідйомності і пробігу автомобіля та ін. До експлуатаційних факторів слід також віднести швидкісний режим руху, довжину перегону

технологічного циклу, частоту планових і позапланових зупинок, інтенсивність руху транспортного потоку та кількість поворотів траси маршрутів [4]. Доведено [5], що з експлуатаційних факторів найбільший вплив на паливну економічність мають швидкість руху, міра використання вантажопідйомності та вибір передачі.

Не менш важливими факторами, що впливають на витрати палива, є чинники організаційної групи [6]:

- контроль за отримуваним паливом (його відсутність може сприяти появі фактів розкрадання палива);
- контроль за переміщенням транспорту (його відсутність може сприяти появі несанкціонованих рейсів);
- контроль за ефективністю використання техніки (низьке завантаження автомобіля, необґрунтований простій машини, нераціональне планування маршрутів та ін.).

До природно-кліматичних факторів слід віднести температуру довкілля та їх кількість [7]. Ця група чинників об'єктивно існують, є некерованими, проте повинні враховуватися при визначенні і нормуванні маршрутної витрати палива автомобілів з обліком ситуації, що склалися, і порі року.

Аналіз і систематизація факторів, що впливають на витрату палива автомобілів показали, що для ефективного використання паливно-мастильного матеріалів необхідно враховувати комплекс показників, які досягаються на етапі проектування, виготовлення, експлуатації та обслуговування автомобілів. Сукупність усіх заходів з економії палива складають комплексну програму, яка забезпечує в цілому підвищення ефективності використання автомобілів.

Список литератури

1. Сафиуллин Р.Н., Афанасьев А.С., Сафиуллин Р.Р. Конструкция, расчет и эксплуатация транспортных средств: Учебное пособие / Р.Н. Сафиуллин, А.С. Афанасьев, Р.Р. Сафиуллин; под общ. ред. проф. Р.Н. Сафиуллина – Москва; Берлин: Директ-Медиа, 2018. – 313 с.
2. Карбанович И.И. Экономия автомобильного топлива: опыт и проблемы. - М.: Транспорт, 1992. - 145 с.
3. Кузнецов Е.С. Управление техническими системами: Учебное пособие. - М.: МАДИ (ГТУ), 2003. - 247 с.
4. Михайлов А.В., Максимов В.А. Факторы, определяющие маршрутный расход топлива городских автобусов. / Сб. тр. Проблемы технической эксплуатации и автосервиса подвижного состава автомобильного транспорта. - М.: МАДИ (ГТУ), 2008. - С.93-97.
5. Парсаданов И.В. Повышение качества и конкурентоспособности дизелей на основе комплексного топливно-экологического критерия / И.В. Парсаданов. – Харьков: НТУ «ХПИ», 2003. – 244 с.
6. Гурова Е.А. Факторы, влияющие на расход горюче-смазочных материалов на автомобильном транспорте / Учет, анализ и аудит: проблемы теории и практики. – Красноярск, 2015. – №15. – С.62-65.
7. Баженов С.П., Казьмин С.П., Носов С.В. Основы эксплуатации автомобилей и тракторов: Учебное пособие / С.П. Баженов, С.П. Казьмин, С.В. Носов. - М.: Академия, 2014. - 384 с.

УДК 004

О. Ушаков, магістр гр. КІ-18М-1,4
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ СЕГМЕНТАЦІЇ МЕРЕЖІ ЗА ДОПОМОГОЮ ТЕХНОЛОГІЇ TRUSTSEC

У статті розроблено програмне забезпечення, яке призначено для системи сегментації мережі за допомогою технології TrustSec. Метою розробки є дослідження та програмна реалізація системи сегментації

мережі за допомогою технології TrustSec. Об’єктом дослідження є процес сегментації мережі за допомогою технології TrustSec. Предметом дослідження є методи сегментації мережі за допомогою технології TrustSec. Методи дослідження базуються на методах теорії телетрафіку, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи сегментації мережі за допомогою технології TrustSec. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

комп’ютерна інженерія, сегментація мережі, TrustSec

Постановка проблеми. Сегментація мережі – важливий інструмент забезпечення інформаційної безпеки, що дозволяє значно знизити ймовірність небезпечних інцидентів і пов'язаний з ними збиток, навіть якщо зловмисники зуміють проникнути усередину периметра корпоративної мережі.

Однієї з популярних мір, спрямованих на зниження збитку від проникнення зловмисника в корпоративну IT-інфраструктуру, служить сегментація мережі. Вона допомагає обмежити можливості нанесення шкоди й тим самим значно знизити ризики інформаційної безпеки (ІБ).

Попереднім етапом сегментації є поділ користувачів і ресурсів мережі на ізольовані (закриті) групи. Обмін даними між цими групами жорстко контролюється або взагалі блокується залежно від вимог політики безпеки організації.

Принципи такого поділу визначаються прийнятої в організації політикою безпеки. Користувачі й пристрої можуть бути розділені по категоріях, наприклад, у такий спосіб: співробітники, тимчасовий персонал, гості, користувачі пристроїв, що не відповідають корпоративній політиці (карантин), інженерні підсистеми будинків і т.д. У свою чергу, співробітники можуть ділитися на кілька груп – скажемо, рядові працівники, керівництво, топ-менеджмент, бухгалтерія й т.п.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи сегментації мережі за допомогою технології TrustSec.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи сегментації мережі за допомогою технології TrustSec.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем сегментації мережі за допомогою технології TrustSec.
– Дослідження системи сегментації мережі за допомогою технології TrustSec.
– Програмна реалізація системи сегментації мережі за допомогою технології TrustSec.

Об’єктом дослідження є процес сегментації мережі за допомогою технології TrustSec.

Предметом дослідження є методи сегментації мережі за допомогою технології TrustSec.

Методи дослідження базуються на методах теорії телетрафіку, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Політикою безпеки організації може передбачатися, що співробітники різних категорій мають доступ тільки до тих корпоративним ресурсам, які необхідні їм для виконання роботи. Наприклад, доступ до групи серверів системи ERP з конфіденційної бізнес-інформацією буде надаватися тільки керівництву, а до баз HR – співробітникам відділу кадрів і, можливо, керівництву. У той же час персоналу нижчої ланки або тимчасових співробітників дозволять звертатися лише до обмеженого набору корпоративних додатків, наприклад до корпоративної системи CRM і електронній пошті.

Сегментація мережі вкрай бажана при реалізації цілого набору бізнес-процесів. До них відносяться процеси, для виконання яких доступ у корпоративну мережу надається користувачам, що не є співробітниками організації. Типовим прикладом є надання доступу в мережу (або в Інтернет) так званим гостьовим користувачам. Крім цього, до мережі часто

може знадобитися підключити співробітників компанії-партнера, аудиторів, а також пристрою, що належать іншим організаціям (банкомати, цифрові вивіски, платіжні термінали). Ще одним сценарієм, при якому рекомендується використання сегментації, є розмежування доступу між співробітниками афілійованих структур, що використовують ту саму мережа. Подібних сценаріїв може бути багато.

Традиційні методи сегментації мережі

При сегментації мережі необхідно вирішити три ключові завдання:

– визначити приналежність користувача до потрібної групи при його підключенні до мережі;

– ізолювати трафік користувача однієї групи від трафіку інших груп;

– забезпечити доступ користувача до тих ресурсам, до яких йому дозволено підключатися й, як правило, заблокувати до всім іншим.

Перше завдання звичайно вирішується за допомогою автентифікації й авторизації за допомогою протоколу 802.1x на сервері RADIUS (часто з використанням даних з корпоративної служби каталогів, наприклад Active Directory). Можливе застосування й інші методи – статичного розподілу користувачів і ресурсів по групах на підставі порту підключення, VLAN, IP-підмережі, MAC-адреси й т.д. – залежно від можливостей наявного сервера AAA і встаткування.

Друге завдання традиційно вирішується шляхом створення окремих віртуальних топологій для кожної групи користувачів. Як правило, це робиться за допомогою тих або інших засобів віртуалізації мережі. У невеликих мережах це віртуальні мережі VLAN і транки 802.1Q. Крім того, часто прибігають до технологій третього рівня, наприклад Multi-VRF CE (VRF-Lite). Для масштабних мереж характерне застосування MPLS VPN.

При рішенні третього завдання звичайно здійснюється пакетна фільтрація на основі IP-адрес. Контроль доступу може бути реалізований як «грубими» засобами (наприклад, списки контролю доступу (ACL) на елементах мережної інфраструктури), так і «тонкою» фільтрацією в системах захисту нового покоління (NGFW, NGIPS). Але фундаментальний принцип залишається тим же: базовим критерієм для ухвалення рішення про допуск/недопуску служить IP-адреса. Фільтрація проводиться на одному або декількох вузлах, призначених для обміну трафіком між групами користувачів.

Іноді пакетну фільтрацію використовують без створення віртуальних топологій, тобто пакетні фільтри служать для рішення одночасно й другий, і третього завдання.

Обмеження традиційних методів сегментації

При традиційних підходах для рішення двох останніх завдань дуже багато чого прийде виконувати вручну, особливо в процесі експлуатації мережі. Ця обставина стає тим відчутніше, ніж більш динамічна сегментована середовище. Наприклад, можуть змінюватися:

– правила контролю доступу – у зв'язку з відновленням як вимог служби безпеки, так і состава ресурсів і користувачів;

– состав груп користувачів – у результаті реорганізації усередині компанії, розширень або скорочень ресурсів мережі й т.д.;

– місцезнаходження груп користувачів, у зв'язку із чим може знадобитися поширення сегментації на нові частини мережі.

Підтримка сегментації стає тим складніше, ніж з більшою кількістю закритих груп користувачів доводиться мати справа.

Ситуація збільшується тим, що правила контролю доступу опираються на IP-адреси. З такими правилами важко працювати й легко помилитися. Крім того, застосування IP-адрес як базового критерію для контролю доступу значно обмежує можливості внесення змін у схему адресації, а в деяких випадках робить їх практично нездійсненними. Крім того, IP-адреса не може ідентифікувати користувача/пристрій/стан і його легко підмінити.

Найчастіше кількість списків контролю доступу стає занадто більшим, а самі вони містять так багато рядків (Access Control Entries, ACE), що адміністратори утрудняються згадати, для чого конкретно потрібна той або інший рядок, і побоюються міняти або видаляти неї. Згодом обслуговування списків тільки ускладнюється.

Працемісткість роботи зі списками контролю доступу іноді приводить до того, що деякі організації взагалі не використовують сегментацію або відмовляються від її в процесі росту мережі. Ті ж, хто використовують сегментацію, змушені витрачати багато часу й сил на координацію між департаментами IT, ІБ і бізнесу, на обмін заявками й т.д.

У підсумку персонал служб IT і ІБ змушений значну частину свого робочого часу займатися рутинними, але відповідальної й потребуючої великої концентрації уваги операціями. Це приводить до того, що:

– ростуть ризики ІБ через можливі помилки й «дір», що виникають у результаті виправлень списків контролю доступу вручну;

– збільшується ймовірність збоїв бізнес-процесів через некоректне внесення змін у конфігурації встаткування;

– багато часу йде на підтримку сегментації в актуальному стані;

– більше сил витрачається на запуск нових додатків або досягнення бізнес-результатів, у тім або іншому ступені пов'язаних із сегментацією мережі.

Займатися важливими, але нетерміновими справами ніколи, тому найчастіше вони й не робляться. Бракує часу для рішення стратегічних, творчих завдань, наприклад, пов'язаних з розвитком мережі, плануванням, оптимізацією підтримки бізнес-процесів, для поліпшення роботи мережі й навіть для підтримки документації в актуальному стані, що знову підвищує ризики ІБ і збоїв бізнес-процесів.

Розробка структурної схеми

TrustSec – це технологія сегментації, розроблена компанією Cisco і що дозволяє перебороти розглянуті вище труднощі за допомогою автоматизації.

Як і у випадку традиційних методів, віднесення користувача до потрібної групи (завдання 1, класифікація в термінології TrustSec) здійснюється шляхом його автентифікації й авторизації за протоколом 802.1x за допомогою сервера контролю доступу, у якості якого виступає Cisco Identity Services Engine (ISE). Для цього сервер Cisco ISE може звертатися як до внутрішньої бази даних користувачів, так і до зовнішніх каталогів, наприклад AD. TrustSec не вимагає застосування яких-небудь певних типів облікових даних – це може бути, наприклад MSCHAPv2, Generic Token Card (GTC), одноразовий пароль RSA і т.д. Крім того, можливі альтернативні методи: MAC Authentication Bypass, Web Authentication, Passive Identity (Easy Connect) на основі AD і т.п., а також статичні методи на основі VLAN, IP-адрес, інтерфейсів і т.п.

Але далі підходи принципово розрізняються. При підключенні до мережі, точніше при вході в межі домену TrustSec, трафіку кожної закритої групи користувачів призначається 16-розрядна мітка безпеки (Security Group Tag, SGT). Звичайно це робиться на комутаторі доступу або іншому пристрої на границі корпоративної мережі. Завдяки багатству можливостей класифікації й призначення влучне, TrustSec дозволяє створити єдину, всеосяжну політику доступу.

Мітка SGT призначається динамічно сервером Cisco ISE або статично елементом мережної інфраструктури. У цьому й полягає принципова відмінність способу ізоляції трафіку (завдання 2, Propagation, або поширення, у термінології TrustSec). При традиційному підході для цього необхідно створити віртуальну топологію для кожної групи. У випадку TrustSec це не потрібно, що значно спрощує мережа: всі закриті групи користувачів можуть працювати на базі єдиної мережної топології.

Крім того, TrustSec пропонує принципово інше, більше просте й ефективне, рішення завдання контролю доступу (завдання 3, Enforcement, або застосування політик, у термінології TrustSec). Традиційний підхід припускає застосування списків контролю доступу, заснованих на IP-адресах (ACL), а TrustSec працює зі списками контролю доступу,

створеними на основі міток SGT, – вони називаються Cisco TrustSec Security Group ACL (SGACL). Використання SGACL дозволяє значно спростити роботу: замість численних і важких у супроводі ACL адміністратори мають справу з SGACL, які залежать від міток груп, а не від адрес або віртуальних топологій.

Ця концепція реалізована в матриці доступу TrustSec Policy сервера Cisco ISE. Замість безлічі розрізнених списків контролю доступу адміністратор працює із централізованою матрицею (див. таблицю). Ряди матриці являють собою групи джерел трафіку (sources), колонки – групи адресатів (destinations). Політики доступу задаються в осередках, де вони перетинаються, у вигляді правил SGACL. Можливі як найпростіші правила (permit/deny для будь-якого трафіку), так і більше складні – з деталізацією що дозволяється й що забороняється трафіку аналогічно тому, як це робиться в ACL, тільки джерела й адресати визначаються мітками SGT, а не IP-адресами. Заповнювати всі осередки матриці необов'язково, незаповнені клітки мають на увазі політикові за замовчуванням: весь трафік або забороняється, або дозволяється.

Концепція матриці доступу й динамічне призначення міток дозволяють реалізувати політикові доступу централізовано, зручно, узгоджено. TrustSec поширює цю політику по мережі шляхом динамічної передачі міток SGT і правил SGACL. Мітки SGT можуть поширюватися по мережі трьома способами: від вузла до вузла в складі заголовків кадрів або пакетів переданого трафіку (метод inline), за допомогою протоколу SGT Exchange Protocol (SXP), що працює поверх TCP, або за допомогою технології Cisco Platform Exchange Grid (pxGrid).

Перший спосіб забезпечує дуже високу масштабованість і зручність, тому що мітки передаються разом із трафіком, але пристрій повинне вміти працювати з мітками, вставленими в кадри або пакети. Це можливо не завжди, особливо у випадку міток у складі кадрів Ethernet, оскільки потрібна апаратна реалізація в мікросхемах ASIC. Крім того, TrustSec може підтримуватися не всіма пристроями мережі, і тоді виникає необхідність в об'єднанні «ізольованих областей» TrustSec. Для таких випадків передбачений другий спосіб – передача міток за протоколом SXP. Третій спосіб – на базі pxGrid – забезпечує інтеграцію з іншими рішеннями ІБ компанії Cisco і її партнерів.

На даний момент Cisco реалізувала технологію TrustSec уже в десятках лінійок своїх продуктів, у тому числі в комутаторах для корпоративних і промислових мереж і ЦОДів, у міжмережних екранах, маршрутизаторах, контролерах WLAN і т.д. Крім того, в 2014 році вона опублікувала інформаційний драфт IETF з описом протоколу SXP, відкривши тим самим функціонал TrustSec іншим вендорам.

Що стосується поширення правил SGACL, те елементи мережної інфраструктури автоматично завантажують їх із сервера Cisco ISE. При внесенні змін у політики TrustSec адміністратор може негайно поширити їх по мережі, скориставшись push-командою в інтерфейсі Cisco ISE. Крім того, політика TrustSec може бути оновлена локально на пристрої за допомогою команди в CLI. До того ж пристрою періодично запитують нові політики в міру їхнього старіння (expiry timeout).

Переваги використання TrustSec для сегментації мережі

Гроші. Фінансовий ефект досягається за рахунок зниження ризиків ІБ і скорочення простоїв бізнес-процесів.

Людино-години. Зниження витрат робочого часу персоналу досягається завдяки зменшенню обсягів рутинної роботи. У результаті з'являється можливість зосередитися на рішенні стратегічних, творчих завдань, які часто відкладаються або взагалі не виконуються.

Час. Прискорення запуску нових сервісів/додатків на кілька днів і тижнів у порівнянні з колишніми затримками сприяє більше швидкому одержанню очікуваних бізнес-результатів.

Реалізований у роботі приклад застосування політики TrustSec

Розглянемо застосування політики TrustSec на конкретному прикладі (див. рис. 1). Користувач Аліса підключилася до мережі, пройшла автентифікацію й авторизацію на

сервері Cisco ISE і була віднесена до групи 5 (Marketing). Комутатор доступу призначає пакетам, що надходять у мережу від її комп'ютера, мітку SGT 5. Для простоти припустимо, що всі зображені на рисунку комутатори входять у домен TrustSec, а політики TrustSec застосовуються на інтерфейсах комутатора Nexus_SGACL, до яких підключені комутатори Nexus1 і Nexus2. Політику доступу, зображену в таблиці на рис. 1, адміністратор налаштував на Cisco ISE і поширив у домені TrustSec.

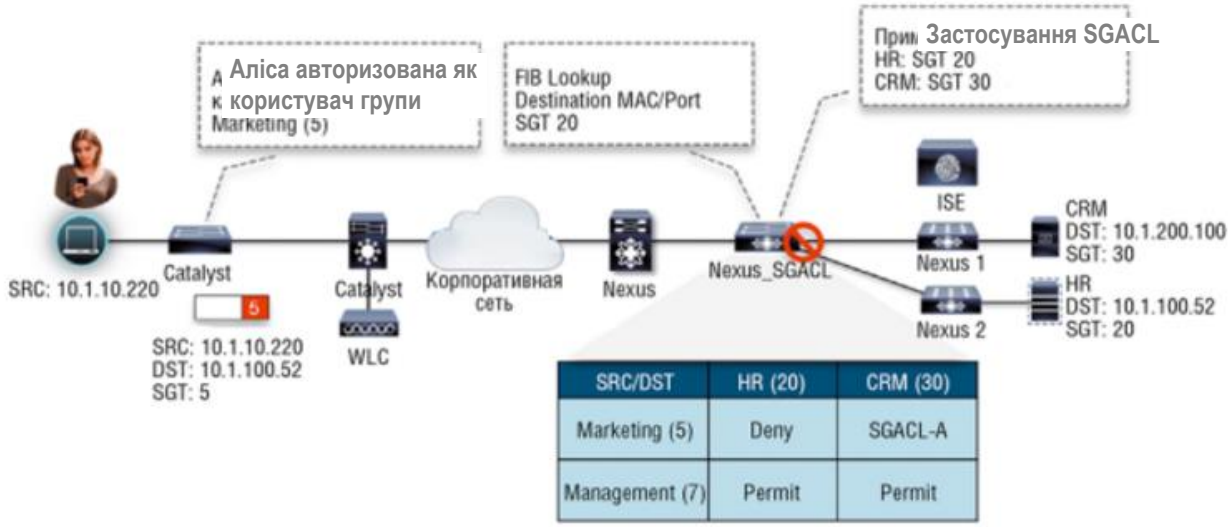


Рисунок 1 – Структурна схема системи

Припустимо, комп'ютер Аліси відправив IP-пакет серверу групи HR. Пакет передається через мережу й приходить на комутатор Nexus_SGACL, що застосовує вже завантажену із сервера Cisco ISE політикові. Матриця доступу передбачає «Відмову» (Deny) для всього трафіку групи Marketing (мітка 5), спрямованого адресатам групи HR (мітка 20). Оскільки сервер HR з адресою 10.1.100.52 належить групі HR, комутатор видаляє пакет Аліси, виконуючи в такий спосіб вимога політики сегментації. Комутатори застосовують SGACL апаратно на швидкості каналу підключення, тому фільтрація на базі міток не впливає на продуктивність комутації.

Cisco TrustSec охоплює не тільки мережну інфраструктуру й сервер Cisco ISE. Інтерфейс pxGrid забезпечує інтеграцію TrustSec з іншими рішеннями Cisco (і її партнерів) – наприклад, Cisco Firepower, Web Security Appliance (WSA), Stealthwatch і т.д. Така інтеграція дозволяє створити на базі міток SGT досить тонкі й деталізовані політики доступу до додатків і мікрододатків, для чого є цілий арсенал функцій міжмережних екранів наступного покоління Cisco Firepower.

Інші приклади: надання на базі міток SGT різних привілеїв доступу до Web-ресурсів за допомогою Cisco WSA; розробка політик Stealthwatch для боротьби зі спрямованими погрозами з урахуванням приналежності користувача до тієї або іншої групи SGT; окремий випадок можливостей рішення Cisco Rapid Threat Containment. В останньому прикладі при виявленні погрози ІБ (наприклад, інфікованого комп'ютера) на Cisco ISE передається запит про обмеження доступу для даного комп'ютера за допомогою інструментарію TrustSec (динамічне приміщення в карантинну групу).

Крім того, TrustSec, будучи, по суті, технологією програмно обумовленої сегментації, інтегрується з архітектурою програмно обумовленого ЦОДа Cisco Application Centric Infrastructure (ACI). Інтеграція встановлює взаємну відповідність між закритими групами користувачів, сегментованих за допомогою міток SGT, і додатками з їхніми компонентами, розділеними на групи Endpoint Groups (EPG) технології ACI. У результаті з'являється можливість створити наскрізні програмно обумовлені політики безпеки, що охоплюють і мережа, і ЦОД. Обидві технології, TrustSec і ACI, спрямовані на оптимізацію й автоматизацію процесів у сфері забезпечення безпеки й у ЦОДе. У цьому змісті вони

доповнюють один одного й, коли використовуються разом, надають додаткові синергетичні вигоди.

Розглянемо ряд типових завдань департаментів IT і ІБ і зрівняємо очікувані результати від реалізації сегментації мережі за допомогою традиційних методів (умовно назвемо таку мережу AS-IS) і на базі технології TrustSec (мережа TO-BE).

Припустимо, що в обох сценаріях користувачі містяться в потрібну групу (завдання 1) по завершенні автентифікації й авторизації 802.1x на сервері RADIUS з використанням служби каталогів AD. Таким чином, рішення цього завдання в обох сценаріях принципово не відрізняється. Але ізоляція трафіку користувачів (завдання 2) реалізується в мережі AS-IS шляхом створення віртуальних топологій або застосування ACL, а в мережі TO-BE – шляхом призначення кадрам міток SGT. Контроль доступу (завдання 3) у сценарії мережі AS-IS здійснюється за допомогою ACL, а в сценарії мережі TO-BE – за допомогою SGACL, які динамічно поширюються по мережі із сервера Cisco ISE.

Сценарій 1. Створення/зміна/видалення списків контролю доступу (ACL)

До завдань цього виду відносяться операції, пов'язані з контролем доступу вже наявних користувачів до ресурсів мережі. У вихідній мережі (AS-IS) це робиться вручну шляхом внесення виправлень у списки ACL, настроєні на одному або на багатьох елементах мережної інфраструктури. Особливо багато виправлень потрібно при використанні ACL і для ізоляції трафіку (замість віртуальних топологій), і для контролю доступу.

Щоб упоратися з більшою кількістю ACL у рамках традиційного підходу, можна спробувати централізувати їхнє застосування до трафіку. Для цього необхідно реалізувати, по-перше, віртуальні топології для ізоляції трафіку закритих груп користувачів (рішення завдання 2), а по-друге, обмін трафіком між цими топологіями із застосуванням ACL (рішення завдання 3) у мінімально прийнятній кількості точок мережі.

За допомогою подібної централізації обміну трафіком можна скоротити кількість ACL, але проблема традиційного підходу повністю не усувається. Крім того, є небезпека виникнення додаткових «пляшкових горлечок» у мережі, а також неоптимальних маршрутів трафіку між групами, які можуть з'явитися через необхідність проходження через точку обміну, що перебуває не на найкоротшому шляху.

У мережі з TrustSec (TO-BE) рішення цього завдання автоматизує. Контроль доступу до ресурсів забезпечується шляхом налаштовування матриці TrustSec Policy Management Matrix, централізованої на сервері контролю доступу Cisco ISE. Політики доступу динамічно поширюються по елементах мережної інфраструктури й реалізуються в SGACL.

Крім того, немає необхідності задавати певні ACL на відповідних інтерфейсах, як було в мережі AS-IS. Замість цього на інтерфейсах активується застосування політик TrustSec, але самі правила SGACL пристрою одержують динамічно. Тому централізувати обмін трафіком між групами вже не потрібно, і можна його зробити розподіленим. У результаті вдається оптимізувати шляхи обміну трафіком між групами й зменшити кількість «пляшкових горлечок».

Сценарій 2. Створення/зміна/видалення ресурсів і закритих груп користувачів

Завдання цього типу можуть бути пов'язані зі створенням або видаленням закритих груп користувачів, запуском або видаленням ресурсів мережі, зміною географічного охвату груп користувачів. Такі завдання можуть виникати в числі іншого в рамках концепції agile office.

Створення/видалення закритих груп користувачів

У мережі AS-IS закриті групи користувачів реалізуються шляхом створення віртуальних топологій за допомогою таких засобів, як VLAN, VRF, MPLS VPN, тунелі й т.п. Альтернативним варіантом є застосування ACL і для сегментації, і для контролю доступу. Додавання нових груп або видалення старих вимагає значних витрат часу й ручної праці, а найчастіше пов'язане з помилками в налаштовуванні й простоями бізнес-процесів через людського фактора.

У мережі з TrustSec додавання або видалення закритої групи користувачів реалізується шляхом створення або видалення мітки групи (SGT) на сервері Cisco ISE і включення користувачів у потрібні групи. При цьому вносити зміни в конфігурацію мережі, як правило, не потрібно.

У результаті витрати часу обслуговуючого персоналу помітно скорочуються. При цьому створення нової закритої групи користувачів або новий бізнес-процесу, що опирається на сегментацію мережі, відбувається значно швидше. Нарешті, виключаються помилки, які можуть виникати при виконанні великої кількості рутинних операцій: перевірити матрицю доступу набагато простіше, ніж сотні записів ACE, розподілених між десятками списків ACL.

Зміна географічного охвату груп користувачів

Подібні завдання виникають, наприклад, коли в групу необхідно включити користувачів з іншого будинку, міста, при переїзді компанії в інший офіс або змінах у складі відділів і т.п.

У мережі AS-IS недостатньо один раз виконати комплекс робіт із сегментації, об'єднанню різних VLAN і VRF у віртуальні топології, по застосуванню ACL (можливо, на численних мережних інтерфейсах) і т.п. – при змінах у політику сегментації всі ці дії прийдеться повторювати. Тому якщо споконвічно реалізувати сегментацію для всіх груп у всій мережі, то за це прийде заплатити ще більш високою працемісткістю її експлуатації.

Здавалося б, гостроту проблеми можна знизити, якщо впровадити сегментацію лише частково, прокладаючи віртуальні топології тільки в ті частини мережі й для тих груп, яким це необхідно в цей момент. Але коли вимоги до географії груп поміняються, прийде витратити чимало часу й сил, щоб впровадити сегментацію в потрібній області мережі, змінити конфігурацію, не помилитися в налаштовуваннях і уникнути простоїв бізнес-процесів.

TrustSec дозволяє звести працезатрати адміністраторів практично до нуля. Технологія впроваджується в мережі один раз, причому навіть на цьому етапі потрібно набагато менше зусиль, чим при створенні віртуальних топологій і/або безлічі ACL на елементах мережної інфраструктури. Переналаштовувати встаткування при зміні політики не знадобиться, тому міркування працемісткості експлуатації не заважають реалізувати TrustSec у всій мережі при її створенні або модернізації.

Але все-таки, якщо при зміні географії груп користувачів виявляється, що за якимись причинами впровадження TrustSec у потрібній частині мережі споконвічно не виконувалося, це можна зробити швидше, ніж у сценарії AS-IS, шляхом застосування набору команд, єдиного для всіх груп користувачів і не залежного від їхньої кількості. Якщо ж TrustSec уже впроваджений у потрібній частині мережі, то переналаштовувати встаткування не прийдеться, тому що політики TrustSec поширюються по мережі динамічно.

Сценарій 3. Запобігання інцидентів ІБ

TrustSec дозволяє реалізувати сегментацію користувачів і контроль доступу з набагато більше високою швидкістю й гранулярністю, чим базові засоби мережі AS-IS. Ефект від впровадження цієї технології тим більше, ніж більше динамічні зміни в конфігурації закритих груп користувачів, тому що TrustSec автоматизує їх.

Крім того, ефект від TrustSec тим помітніше, ніж більше гранулярна сегментація користувачів на групи. У випадку традиційної сегментації (на базі віртуальних топологій) зі збільшенням числа груп користувачів зростає розмаїтість топологій і, як наслідок, внесення змін мережі ускладнюється. У результаті кількість топологій (і груп користувачів) може виявитися неоптимальним з погляду безпеки, а виходить, прийде іти на компроміс між безпекою й працемісткістю.

TrustSec усуває це обмеження, дозволяючи створити єдину, всеосяжну політику доступу для всіх типів пристроїв і підключень, розділяючи користувачів саме на таку кількість груп, яке необхідно для забезпечення високого рівня безпеки. Серйозні додаткові можливості відкриває інтеграція TrustSec з іншими рішеннями ІБ завдяки технології pxGrid.

Крім того, TrustSec забезпечує підвищений рівень безпеки за рахунок строгої взаємної автентифікації елементів мережної інфраструктури й можливості шифрування трафіку на канальному рівні.

Завдяки описаним перевагам Cisco TrustSec, імовірність інцидентів ІБ і пов'язаний з ними збиток значно знижуються.

Сценарій 4. Усунення наслідків / розслідування інцидентів ІБ

TrustSec приносить більшу користь і при усуненні наслідків інцидентів ІБ, а також при їхньому розслідуванні.

Обмеження збитку від інфекції і її поширення

Тому що TrustSec дозволяє сегментувати користувачів, створюючи закриті групи з набагато більше високим ступенем деталізації, чим традиційні методи, у випадку виникнення інциденту ІБ (наприклад, при проникненні в мережу зловмисника або вірусу) очікуваний збиток буде набагато менше, ніж у мережі AS-IS. Крім того, TrustSec заощадить час персоналу, що буде займатися усуненням наслідків інциденту.

Інша перевага TrustSec полягає в тому, що при інциденті він дозволяє зберегти доступ користувачів у мережу, перевівши їх в окрему ізольовану групу. Це особливо важливо, коли мова йде про VIP-користувачів. Наприклад, при зараженні комп'ютерів топ-менеджерам буде як і раніше забезпечений доступ у мережу, причому з мінімальними ризиками для незаражених комп'ютерів.

Прискорення розслідування інцидентів ІБ

Оскільки TrustSec дозволяє реалізувати більше гранулярну, у порівнянні з мережею AS-IS, сегментацію користувачів, розслідування інцидентів зажадає аналізу стану меншої кількості пристроїв. У результаті можна значно прискорити й полегшити розслідування інцидентів.

Сучасний бізнес стає усе більше динамічним. Мережа, а також застосовувані в ній політики повинні оперативно адаптуватися до нових вимог, тому що зміни в політику безпеки, на реалізацію яких ідуть дні або тижні, більше не влаштовують бізнес.

Критично важливо й належне функціонування бізнес-процесів, що опираються на мережу й залежать від сегментації. Будь-які зміни політики сегментації повинні бути реалізовані не тільки швидко, але й надійно.

Оскільки традиційні засоби сегментації вже не відповідають ні поточним, ні прогнозованим запитам бізнесу, на допомогу приходить сучасна технологія сегментації мережі TrustSec. Пропонований нею інструментарій швидко, надійно й в автоматичному режимі реалізує зміни середовища сегментації й зводить до мінімуму недоліки людського фактора.

Висновок. У статті розглянуто та проаналізовано програмне забезпечення, яке призначено для операційної системи сегментації мережі за допомогою технології TrustSec. В межах України в недостатній мірі представлені вітчизняні розробки в цій області. У роботі наведені теоретичне узагальнення й рішення наукового завдання дослідження методів сегментації мережі за допомогою технології TrustSec. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем сегментації мережі за допомогою технології TrustSec; Досліджена система сегментації мережі за допомогою технології TrustSec; На основі отриманих результатів досліджень створена програмна реалізація системи сегментації мережі за допомогою технології TrustSec. Розроблені під час виконання роботи алгоритми дозволяють успішно вирішувати завдання сегментації мережі за допомогою технології TrustSec. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки. Розроблене програмне забезпечення має простий, дружній та зручний інтерфейс користувача, що забезпечує легкість у освоєнні роботи програмного продукту, зручність у використанні, і не потребує особливих спеціальних знань. При створені програмного забезпечення було використано об’єктно-орієнтований підхід, що відповідає

сучасним тенденціям у галузі розробки комерційних програмних систем. Програма реалізована на мові високого рівня Embarcadero Delphi 10.2. Дана мова програмування дозволяє найбільш ефективно обробляти дані. Це дозволило мінімізувати строк розробки програмного забезпечення, і, як слід, зменшити витрати на його розробку. Запропоноване програмне забезпечення ділиться на загальне програмне забезпечення, що поставляється із засобами обчислювальної техніки й спеціальне програмне забезпечення, що спеціально розроблене для даної конкретної системи й включає програми, що реалізують її функції. Даються необхідні рекомендації з установки розробленого програмного забезпечення. Для підвищення рівня безпеки запропоновано застосовувати алгоритм Md5.

Список літератури

1. Смирнов А.А. Анализ и сравнительное исследование перспективных направлений развития цифровых и телекомуникационных систем и сетей. / А.А. Смирнов, В.В. Босько, Е.В. Мелешко // Системи обробки інформації. – Вип. 7 (74). – Х.: ХУПС. – 2008. – С. 120-123.
2. Смирнов А.А. Разработка методики оценки среднего времени обслуживания информационных пакетов в телекоммуникационной сети / А.А. Смирнов, В.В. Босько, Е.В. Мелешко // Системи управління, навігації та зв'язку. – Вип. 2(10). – К.: ДП «ЦНДІНУ». – 2009. – С.162-165.
3. Семенов С.Г. Сравнительные исследования методов идентификации трафика в телекоммуникационной сети для повышения оперативности передачи данных / С.Г. Семенов, Е.В. Мелешко // Прикладная радиоэлектроника. – Том 9 №3. – Х.: ХНУРЕ. – 2010. – С.444-448.
4. Кузнецов А.А. Метод структурной идентификации информационных потоков в телекоммуникационных сетях на основе bds-тестирования / А.А. Кузнецов, С.Г. Семенов, С.Н. Симоненко, Е.В. Мелешко // Наука і техніка Повітряних Сил Збройних Сил України.–Вип. 2 (4).–Х.: ХУПС.– 2010.–С.131-137.
5. Мелешко Е.В. Математическая модель подсистемы управления и обслуживания в многопротокольном узле святи / Е.В. Мелешко // Збірник наукових праць Харківського університету повітряних сил. – Вип. 4(26). – Х.: ХУПС. – 2010. – С.124-128.
6. Мелешко Е.В. Методы идентификации трафика и динамического управления очередями в многопротокольных узлах связи и оценка их эффективности / Е.В. Мелешко // Системи обробки інформації. – Вип. 8 (89). – Х.: ХУПС. – 2010. – С.68-74.
7. Матип Эссунга Лазар Методика выбора количества приоритетных пользователей в корпоративных вычислительных сетях реального времени «Системы управления и информационные технологии», Воронеж 2008, №4.2(30). 261-264с
8. Матип Эссунга Лазар, к вопросу исследования эффективности подсистемы клиент-сервер средствами системы массового обслуживания и теории очередей Труды Новомосковского института Российского химико-технологического университета им. Д.и, Менделеева Новомосковск, 2004 г. выпуск № 3 (14) 240-243с
9. Матип Эссунга Лазар, Абросимов Л.И Задачи управления производительностью корпоративных вычислительных сетей XIII Международной научно-технической конференции студентов и аспирантов радиоэлектроника, электротехника и энергетика 1-2 марта 2007 г. тезисы докладов Изд-во МЭИ, том 1. 412-413с,
10. Матип Эссунга Лазар, Выбор количества приоритетных пользователей для управления производительностью КОМ на второй ежегодной международной конференции, организации сети Управления, "В IWAN '07", (Цюрих, Швейцария, 01-05 октября 2007) р. 312-314; Matip Essounga Lazare Users priority choice for management of performance of corporate computer network In Second annual International Working Conference on Active, Management Networking, «In IWAN'07», (Zurich, Switzerland, 01-05 October 2007) p. 312-314

УДК: 657

В. Хомич, магістр гр. ООУ -18-МЗ-1,9
Центральноукраїнський національний технічний університет

ЗАГАЛЬНОВИРОБНИЧІ ВИТРАТИ ЯК ЕКОНОМІЧНА КАТЕГОРІЯ ТА ОБ'ЄКТ ОБЛІКУ

У статті розкрито підходи науковців до розкриття сутності загальновиробничих витрат, їх складу та класифікації. Визначено сутність загальновиробничих витрат як об'єкта обліку
загальновиробничі витрати, постійні витрати, змінні витрати, розподіл загальновиробничих витрат

Актуальність дослідження. Виробничі підприємства поряд з витратами технологічного характеру, несуть значну частину витрат, пов'язаних з виконанням загальновиробничих функцій, зокрема забезпечують організацію, обслуговування виробництва і управління ним. Такого роду витрати мають також відображатися у складі собівартості продукції, тому велике значення має виважена і економічно обґрунтована методика їх обліку і розподілу. Розподіл загальновиробничих витрат часто викликає складність стосовно вибору бази розподілу. Це обумовлено, перш за все, тим, що існуюче законодавство неоднозначно трактує сутність категорії загальновиробничих витрат, що особливо стосується аграрної сфери; з іншого боку, розподіл загальновиробничих витрат може бути різним на різних підприємствах, залежно від особливостей їх діяльності.

Вагомий внесок у вирішення проблематики обліку і контролю витрат внесли такі вчені Бутинець Ф.Ф., Гончарук Я.А., Дерій В.А., Должанський А.М., Мужевич Н.В., Пушкар М.С., Римар Г А. Однак у них недостатньо приділено уваги саме загальновиробничим витратам. Проблему обліку та розподілу загальновиробничих витрат досліджували у своїх працях С.Ф. Голова [1], В.І. Довбуш [2], П.О. Куцика [3, 4], Л.В. Нападовської [5], Т.М. Сльозко та ін.

Мета, завдання, об'єкт дослідження. Мета дослідження полягає у вивченні сутності загальновиробничих витрат підприємств як економічної категорії та об'єкту.

Результати дослідження. Для забезпечення обґрунтованих підходів організації обліку та контролю загальновиробничих витрат і ефективного управління ними необхідно чітко розуміти сутність загальновиробничих витрат, їх склад та класифікацію. Проведений аналіз наявних наукових праць дає змогу узагальнити підходи вчених до трактування сутності загальновиробничих витрат.

Таблиця 1 – Погляди вчених на сутність загальновиробничих витрат

Автор	Трактування сутності загальновиробничих витрат
Сук Л.К.	непрямі витрати, пов'язані з організацією виробництва і керівництвом цехами, бригадами, відділеннями та іншими структурним підрозділами підприємства (цехові витрати)
Бутинець Ф. Ф.	витрати з обслуговування виробництва й управління роботою цехів та інших підрозділів основних і допоміжного виробництва
Мазуренко О.М.	витрати цехів, дільниць і підрозділів на організацію та управління процесом виробництва, витрати на утримання й експлуатацію машин та обладнання, будівель, споруд, які не можна прямо віднести на конкретний об'єкт витрат
Мервецька В.	непрямі витрати, пов'язані з організацією виробництва та управління цехами, бригадами, відділеннями та іншими підрозділами підприємства
Сіо С.С.	постійні загальновиробничі витрати – це ті витрати,

	які не змінюються безпосередньо зі зміною обсягів виробництва. Вони можуть змінюватись, але їх зміни не пов'язані зі зміною обсягів виробництва у короткостроковому періоді. Змінні загальновиробничі витрати залежать від багатьох факторів окрім обсягів випуску
Грабова Н. М.	витрати, пов'язані з процесом виробництва, які не можна віднести до певних виробів економічно доцільним шляхом

Нормативне визначення сутності загальновиробничих витрат є досить простим. Так у ПС(Б)О 16 "Витрати" визначено, що "загальновиробничі витрати є витратами на обслуговування та управління виробництвом" [6]. Інструкція № 291 про застосування Плану рахунків бухгалтерського обліку активів, капіталу, зобов'язань і господарських операцій підприємств і організацій зазначає, що "загальновиробничі витрати – це виробничі накладні витрати на організацію виробництва та управління цехами, дільницями, відділеннями, бригадами та іншими підрозділами основного й допоміжного виробництва" [7].

Загальновиробничі витрати пов'язані з виробництвом кількох видів продукції, а тому повинні бути враховані при обчисленні собівартості кожного виду продукції.

Виробнича собівартість продукції (робіт, послуг) включає тільки витрати, безпосередньо пов'язані з виробництвом продукції, обумовлені технологією й організацією виробництва, а в частині витрат на управління включає тільки загальновиробничі витрати. Отже, загальновиробничі витрати є об'єктом бухгалтерського обліку. Від їх рівня значною мірою залежать собівартість продукції та ефективність функціонування підприємства загалом.

Формування та облік витрат значною мірою залежить від їх чіткої та функціональної класифікації, а неоднорідність витрат, що входять до складу загальновиробничих витрат, обумовлює необхідність їх класифікації. Питання класифікації загальновиробничих витрат цікавить багатьох науковців, їх погляди багато у чому схожі, але в той же час різняться за деякими аспектами.

Науковці Ф.Ф. Бутинець та В.М. Кміть мають однаковий погляд на поділ загальновиробничих витрат і виокремлюють в них такі складові: витрати з утримання й експлуатації обладнання та цехові витрати [8, 9]. При цьому, В.М. Кміть деталізує групу цехових витрат, виокремлюючи такі складові: витрати на управління виробництвом і витрати на організацію та обслуговування виробництва.

У своїх працях Ю.Г. Давидов доповнює класифікацію загальновиробничих витрат такими ознаками: можливість регулювання, належність до обсягів виробництва, техніко-економічне призначення [10].

У нормативній базі загальновиробничі витрати класифікують за характером включення до собівартості продукції на постійні та змінні.

Рисунок 1 – Класифікація загальновиробничих витрат відповідно до нормативної бази

Перелік і склад змінних і постійних загальновиробничих витрат встановлюється підприємством. Характеристика постійних та змінних загальновиробничих витрат наведена в таблиці 2.

Таблиця 2 - Характеристика постійних і змінних загальновиробничих витрат

Види витрат	Характеристика
Змінні загально-виробничі витрати	Витрати на обслуговування і управління виробництвом (цехів, дільниць), що змінюються прямо (або майже прямо) пропорційно до зміни обсягу діяльності. Змінні загальновиробничі витрати розподіляються на кожен об'єкт витрат з використанням бази розподілу (годин праці, зар. плати, обсягу діяльності, прямих витрат тощо), виходячи з фактичної потужності звітного періоду
Постійні загально-виробничі витрати	Витрат відносяться витрати на обслуговування і управління виробництвом, що залишаються незмінними (або майже незмінними) при зміні обсягу діяльності. Постійні загальновиробничі витрати розподіляються на кожен об'єкт витрат з використанням бази розподілу (годин праці, зар. плати, обсягу діяльності, прямих витрат тощо) при нормальній потужності. Нерозподілені постійні загальновиробничі витрати включаються до складу собівартості реалізованої продукції (робіт, послуг) у періоді їх виникнення. Загальна сума розподілених та нерозподілених постійних загальновиробничих витрат не може перевищувати їх фактичну величину

Змінні витрати повністю включаються до витрат виробництва у період їх виникнення.

Проаналізувавши фахову літературу зазначимо, що переважна більшість авторів погоджуються із підходом до класифікації загальновиробничих витрат, наведеним у нормативних документах, тобто залежно від обсягів виробництва поділі їх на постійні та змінні. При цьому серед науковців побутує переконлива думка щодо умовності поділу витрат на постійні та змінні. Положення про те, що "постійні витрати при зміні обсягів виробництва залишаються незмінними, а змінні – лінійно зростають, дозволяє значно спростити роботу аналітика, але відомо, що реальні залежності складніші" [11]. Виходячи з цього, науковці вважають, а ми поділяємо їх думку, що коректніше говорити про умовно-змінні та умовно-постійні витрати.

Існують різні методи і підходи щодо поділу витрат на умовно-постійні й умовно-змінні. Вважаємо за доцільне коротко охарактеризувати їх та запропонувати оптимальний з них. Узагальнена характеристика цих методів і підходів наведена в таблицях

Таблиця 3 - Підходи до поділу витрат на умовно-постійні й умовно-змінні

Назва підходу	Сутність (характеристика)
Суб'єктивний	віднесення витрат до групи умовно-постійних або умовно-змінних, базуючись на неформальному досвіді дослідника
Статистичний	передбачає аналіз наявних статистичних даних, проведення експериментів, щоденне спостереження за реальним виробничим процесом

Сьогодні найбільш широко використовують два підходи: суб'єктивний і статистичний. Суб'єктивний підхід передбачає вольове віднесення витрат до групи умовно-постійних або умовно-змінних, базуючись на неформальному досвіді дослідника. Статистичний підхід передбачає аналіз наявних статистичних даних або, якщо отримання інформації за ряд попередніх років ускладнено, можуть проводитись керовані експерименти або щоденне спостереження за реальним виробничим процесом. У свою чергу статистичний

підхід передбачає використання різних методів. Сутність усіх методів, які застосовуються у рамках статистичного підходу, ґрунтується на визначенні в кінцевому результаті сумарних витрат шляхом апроксимації даних про витрати та обсяги виробництва за певний період часу. Крім статистичних методів можуть бути використані інші методи. С.Ф. Голов у своїх дослідженнях порядок визначення залежності між сумою витрат та обсягом виробництва пропонує здійснювати методами технологічного аналізу, аналізу бухгалтерських рахунків, візуального пристосування й обґрунтовувати свій вибір за допомогою коефіцієнта детермінації [1, с. 64-76].

Для оцінки оптимального співвідношення обсягу виробництва, витрат і прибутку О.О. Калініченко пропонує використовувати імовірнісний підхід до оцінки та прогнозування співвідношення витрат, обсягів виробництва та прибутку підприємства. На його думку, "реалізація запропонованого підходу щодо формування асортименту продукції потребує також всебічної оцінки зміни витрат – як змінної, так і постійної їх складової" [12].

Зазначимо, що всі методи зводяться до врахування змінної складової витрат. Дослідження підтверджують широке застосування методу визначення функції витрат за допомогою регресійного аналізу, який, на нашу думку є найточнішим.

Віднесенню до складу виробничої собівартості підлягає лише частина постійних ЗВВ (постійні розподілені ЗВВ), що відповідає нормальній потужності – тобто очікуваного середнього обсягу діяльності, що може бути досягнутий за умов звичайної діяльності підприємства протягом кількох років або операційних циклів з урахуванням запланованого обслуговування виробництва. Інша частина постійних ЗВВ (нерозподілені постійні ЗВВ) відноситься до собівартості реалізованої продукції.

Відповідно до П(С)БО 16 "Витрати", до складу виробничої собівартості можуть бути віднесені не всі витрати, зібрані підприємством протягом місяця на рахунку 91 «Загальновиробничі витрати». Загальновиробничі витрати повинні щомісяця розподілятися між рахунками 23 «Виробництво» і 90 «Собівартість реалізації».

За опомогою бази розподілу змінні і постійні витрати розподіляються на кожен об'єкт витрат. При цьому змінні витрати повністю списуються на виробничу собівартість продукції на рахунок 23 «Виробництво».

При розподілі загальновиробничих витрат основна частина цих витрат - постійні розподілені загальновиробничі витрати - включаються до собівартості конкретного виду продукції, тобто списуються на рахунок № 23 «Виробництво». А нерозподілені постійні загальновиробничі витрати збільшують собівартість реалізованої продукції того періоду, в якому такі витрати виникли, тобто списуються на рахунок 90 «Собівартість реалізації».

При організації обліку загальновиробничих витрат на підприємствах має бути забезпечено наступне: вірне, точне та своєчасне визначення розміру загальновиробничих витрат; наукове групування загальновиробничих витрат за єдиними для всіх галузей народного господарства ознаками; контроль за обсягом загальновиробничих витрат та їх розподілом; визначення ефективного методу та дотримання порядку розподілу загальновиробничих витрат; своєчасне подання інформації про загальновиробничі витрати з метою контролю та оперативного керівництва виробництвом.

Висновок. Загальновиробничі витрати є об'єктом бухгалтерського обліку та контролю, від їх рівня значною мірою залежать собівартість продукції та ефективність функціонування підприємства загалом.

Аналіз фахової літератури показав майже однозначність науковців стосовно визначення сутності загальновиробничих витрат та деяку варіативність щодо їх класифікації. Переважна більшість авторів погоджуються із затвердженим у нормативах, підходом до класифікації загальновиробничих витрат, тобто їх поділ на постійні та змінні.

Дослідження підходів та методів визначення умовно-змінних та умовно постійних витрат дав змогу висловити свою думку щодо їх застосування, вважаємо найдоцільнішим використовувати статистичний підхід та метод регресійного аналізу при визначенні умовно-змінних та умовно-постійних витрат.

Список літератури

1. Голов С.Ф. Управлінський облік / С.Ф. Голов. – К.:Лібра, 2003. – 704 с.
2. Довбуш В.І. Проблемні аспекти розподілу загальновиробничих витрат та їх облік на молокопереробних підприємствах / В.І. Довбуш // Формування ринкових відносин в Україні. – 2011. - № 10 (125). – С. 114 – 118.
3. Куцик П.О. Методика і організація обліку та розподілу непрямих витрат: теорія і практика / П.О. Куцик // Регіональні перспективи. – 2003. – № 2 – 3. – С. 66 – 70.
4. Куцик П.О. Загальновиробничі витрати: порядок формування та розподілу: / П.О.Куцик, О.М.Чабанюк // Вісник Львівської комерційної академії / [ред. кол.: Башнянін Г.І., Апопій В.В., Вовчак О.Д. та ін.]. – Вип. 35. – Серія економічна.– Львів: Видавництво Львівської комерційної академії, 2011. – С. 208 – 212.
5. Нападовська Л.В. Управлінський облік: [монографія] / Л.В. Нападовська. – Дніпропетровськ: Наука і освіта, 2000. – 450 с.
6. Положення (стандарт) бухгалтерського обліку 16 «Витрати», затверджено наказом Міністерства фінансів України від 31.12.99 р. № 318 . – [Електронний ресурс] – Режим доступу: http://zakon2.rada.gov.ua/laws/show/z0027-00.
7. Інструкція про застосування Плану рахунків бухгалтерського обліку активів, капіталу, зобов'язань і господарських операцій підприємств і організацій, затверджено наказом Міністерства фінансів України від 30.11.1999 за №291 із змінами, внесеними згідно з наказом Міністерства фінансів України №1012 від 9.12.2002р. – [Електронний ресурс] – Режим доступу: http://zakon2.rada.gov.ua/laws/show/z0893-99
8. Бутинець Ф.Ф. Бухгалтерський управлінський облік / Ф.Ф. Бутинець. – Житомир : ЖІТІ., 2000. – 448 с.
9. Кміть В.М. Проблеми методології розподілу накладних витрат на виробництво промислової продукції / В.М. Кміть // Формування ринкової економіки в Україні. Науковий збірник. Випуск 5. (Перехідна економіка: проблеми теорії і практики). – Львів: Інтереко, 1999. – С. 146-150.
10. Давидов Ю.Г. Вплив галузевих особливостей на формування і організацію непрямих витрат на підприємствах переробної промисловості України / Ю.Г. Давидов // Економіка: проблеми теорії та практики, випуск 114 – Дніпропетровськ: Наука і освіта – 2001. – С. 29-32.
11. Іванюта О. В. Економічний аналіз стану загальновиробничих витрат великих промислових підприємств [Електронний ресурс] / О. В. Іванюта // Вісник Житомирського державного технологічного університету. Серія : Економічні науки. - 2014. - № 2. - С. 41-53. - Режим доступу: http://nbuv.gov.ua/UJRN/Vzhdtu_econ_2014_2_9
12. Калиниченко Е.А. Экономико-математическое моделирование соотношения постоянных и переменных издержек / Е.А. Калиниченко // Зб. матер. IV науково-практичної конф. молодих економістів «Сучасні проблеми розвитку виробництва». – Харків: Модель Всесвіту, 2000. – С. 268 – 270.

УДК 004

Д. Чорновол, магістр гр. КІ-18М-1,9
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ РЕАЛІЗАЦІЇ МЕТОДІВ СОЦІАЛЬНОГО ІНЖИНІРИНГУ ЧЕРЕЗ АДРЕСУ E-MAIL

У статті розглянуто програмне забезпечення, яке призначено яке призначено для системи реалізації методів соціального інжинірингу через адресу e-mail. Метою розробки є дослідження та програмна реалізація системи реалізації методів соціального інжинірингу через адресу e-mail. Об'єктом дослідження є процес реалізації методів соціального інжинірингу через адресу e-mail. Предметом дослідження є методи реалізації методів соціального інжинірингу через адресу e-mail. Методи дослідження базуються на методах захисту інформації, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи реалізації методів соціального інжинірингу через адресу e-mail. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення. Розроблено зручний інтерфейс користувача. Наведені інструкції по роботі з програмними засобами.

комп'ютерна інженерія, соціальний інжиніринг

Постановка проблеми. Найбільш розвиненою формою шахрайства в Інтернеті, безсумнівно, є фішінг. Зловмисники використовують перехоплювачі клавіатури, поштові повідомлення, складені за всіма правилами соціальної інженерії, спеціально розроблені сайти й інші засоби. Усе більше винахідливими стають атакуючі, усе вище рівень їхньої підготовленості. Про цього вужа було сказано чимало. Нагадаю, що фішінг (phishing) – вид інтернет-шахрайства, що полягає в розсиланні електронних повідомлень із метою крадіжки конфіденційної інформації (як правило, фінансового характеру). Сюди ставляться крадіжки паролів, номерів кредитних карт, банківських рахунків і іншої конфіденційної інформації.

Фішінг-повідомлення складаються таким чином, щоб максимально походити на інформаційні листи від банківських структур або компаній з відомими брендами. Листи містять посилання на свідомо помилковий веб-ресурс, спеціально підготовлений зловмисниками і який є копією сайту організації, від імені якої відправлений лист. На даному фальшивому сайті користувачеві пропонується ввести, наприклад, номер своєї кредитної карти й іншу конфіденційну інформацію.

Фішінг являє собою підроблені повідомлення, що прийшли на пошту, від банків, провайдерів, платіжних систем і інших організацій про те, що з якої-небудь причини одержувачеві терміново потрібно передати / обновити особисті дані. Причини можуть називатися різні. Це може бути втрата даних, поломка в системі та інше.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини системи реалізації методів соціального інжинірингу через адресу e-mail.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи реалізації методів соціального інжинірингу через адресу e-mail.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем реалізації методів соціального інжинірингу через адресу e-mail.

– Дослідження системи реалізації методів соціального інжинірингу через адресу e-mail.

– Програмна реалізація системи реалізації методів соціального інжинірингу через адресу e-mail.

Об'єктом дослідження є процес реалізації методів соціального інжинірингу через адресу e-mail.

Предметом дослідження є методи реалізації методів соціального інжинірингу через адресу e-mail.

Методи дослідження базуються на методах захисту інформації, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу.

Опис функціонування системи

Приведемо ряд атак реалізованих за допомогою методів соціальної інженерії.

Скомпрометовані web-сайти для поширення шкідливого ПЗ під видом відновлень для Adobe Flash, Chrome і FireFox

Зловмисники використовують скомпрометовані web-сайти для поширення шкідливого ПЗ під видом відновлень для Adobe Flash, Chrome і FireFox:

– Після установки «відновлення» на пристрій користувача завантажується шкідливий файл JavaScript.

– Скрипт збирає системну інформацію й відправляє її на керуючий сервер, одержує додаткові команди, а потім завантажує шкідливу «корисне навантаження».

– Файл за назвою Update.js виконується з директорії %AppData% за допомогою wscript.exe.

Шкідливе навантаження містить у собі утиліти для розкрадання даних, а також NetSupport Manager – легітимну утиліту для вилученого доступу, за допомогою якої можна робити будь-які дії із системою.

Нова кампанія по поширенню шпигунського ПЗ FormBook використовує шкідливе розсилання із прикріпленими документами MS Word

– Документ не містить ні макросів, ні активних посилань, тому пісочниці й антивіруси вважають його «чистим».

– У документі присутні теги, що посилаються на інформацію з окремого файлу webSettings.xml.rels.

– Якщо переглядати таке вкладення в незахищеному режимі, активується скорочене посилання на командний сервер, з якого завантажується шкідливий RTF-Документ.

– При відкритті убудований у нього об'єкт переноситься в тимчасову папку, де створюється виконується файл, що, завантажуючий на комп'ютер жертви основне корисне навантаження – FormBook.

Зловмисне програмне забезпечення дозволяє записувати натискання клавіш і витягати дані із сеансів HTTP і буфера обміну, а також виконувати вступників з C&C-сервера команди: завантажувати і запускати файли, перезавантажувати й виключати систему, красти локальні паролі й файли cookie.

Зловмисне програмне забезпечення PUBG шифрує файли своїх жертв, але надає потерпілому можливість відразу розшифрувати файли, увівши код або погравши в гру

Зловмисне програмне забезпечення відслідковує процес, що містить в ім'ї «TslGame», і вважає, скільки часу жертва провела в грі, у підсумку розшифровуючи файли. При цьому не перевіряється, чи дійсно гра встановлена на зараженій машині й запущена. Значення має тільки ім'я процесу.

Дві нові варіації здирника Matrix атакують комп'ютери через протокол вилученого доступу (Remote Desktop Protocol, RDP) і можуть безповоротно знищити вміст жорсткого диску

– Шифрувальник поширюється через підбор паролів по RDP.

– Після установки на комп'ютер шифруються дані на жорсткому диску й вилучених мережних ресурсах, а також знищують тіньові копії томів, щоб позбавити користувача можливості відновити файли.

– Документам привласнюються закодовані імена й розширення, у яких зазначений один з email-адрес шахраїв. В одному випадку це .[Files4463@tuta.io], в іншому – .[RestorFile@tutanota.com].

– У папках із зашифрованими файлами здирник залишає повідомлення з вимогою викупу. Схоже послання відображається на робочому столі зараженого комп'ютера.

– Сума викупу в повідомленні не уточнюється й залежить від швидкості відповіді користувача. Як підтвердження, що врятувати документи можливо, пропонують безкоштовно розшифрувати три файли.

– Жертви одержують тиждень на ухвалення рішення, після чого зловмисники обіцяють видалити ключ.

Троян Rarog використовується для схованого майнингу Monero на Windows і поширюється через сайти на CMS Magento

Зловмисне програмне забезпечення регулює навантаження на процесор жертв і відслідковує результати криптомайнингу. Троян також намагається сховати роботу майнера від Диспетчера завдань Windows і спеціалізованих програм-аналізаторів запущених процесів.

Крім видобутку Monero і інших криптовалют, Rarog уміє:

– завантажувати й запускати додаткові шкідливі файли;
– самостійно обновлятися;
– проводити DDoS-атаки;
– заражати пристрою, що підключаються по USB.

Уразливість у системах аварійного оповіщення дозволяє хакерам дистанційно активувати сирени за допомогою радіосигналу

Атака, що одержала назву SirenJack Attack може бути виконана на сирени виробництва ATI Systems, які використовуються у великих містах, а також в університетах, військових і промислових об'єктах США.

У протоколі керування сиренами відсутнє шифрування, тому для експлуатації уразливості досить комп'ютера й ручної радіостанції вартістю 30 доларів США. При цьому хакер повинен перебувати в зоні досяжності й ідентифікувати радіочастоту, використовувану цільовою сиреною для відправлення спеціально сформованого повідомлення.

Шахраї використовували збій у роботі мессенджера Телеграм, що відбулася 29 березня 2018 року, для розкрадання криптовалюти в довірливих користувачів:

Під справжніми повідомленнями Павла Дурова в Twitter з'явилися фальшиві послання, відправлені з аккаунта PavelDurov (@durhiov), що говорять, що як вибачення користувачам Telegram буде запропонована компенсація в Ethereum-Еквіваленті.

– На шахрайському сайті ethg.st повідомлялося, що загальний розмін компенсації складе близько 5000 ETH, а для участі в акції потрібно перелічити від 0,5 до 5 ETH за адресою, зашифрованому в QR-коді.

– Довірливі користувачі протягом години перелічили шахраям близько 60 000 доларів США.

Банківський троян Buhtrap поширювався через заражені новині сайти

Шкідливий скрипт впроваджувався на головні сторінки ряду російськомовних новиних сайтів фінансової тематики. Після візиту на таку сторінку потенційна жертва непомітно перенаправлялася на підконтрольний злоумишленикам сервер, і проти її використовувався експлойт для браузера Internet Explorer.

Дані 37 мільйонів користувачів сайту мережі кафе Panera Bread (panerabread.com) були доступні будь-якому бажаючому у відкритому виді

Серед даних були імена користувачів, їх email-адреси й адреси доставки, дати народження, телефонні номери, останні чотири цифри з номерів банківських карт, а також номера карт лояльності. Зібрати повну базу даних можна було за допомогою найпростішого пошукового скрипту.

Компанія Under Armour повідомила про компрометацію 150 млн користувачів приналежного їй застосунка й сайту MyFitnessPal.

Невідомі зловмисники скомпрометували сервери MyFitnessPal і одержали доступ до email-адрес, логінам і гешованим паролям. Представники Under Armour просять користувачів поміняти паролі від MyFitnessPal і попереджають про можливі атаки фішерів.

Нова фішінговая атака на користувачів криптовалютної біржі Poloniex використовує шкідливий додаток для крадіжки даних

Злочинці використовують той факт, що, незважаючи на солідний статус і величезну кількість користувачів, в Poloniex відсутнє власний мобільний додаток.

HiddenMiner – новий шкідливий майнер для Android, що маскується під відновлення для Google Play Store

Зловмисне програмне забезпечення обманом змушує користувачів видати йому права адміністратора й майнит криптовалюту. Щоб сховатися від користувача, зловмисне програмне забезпечення створює прозору іконку для застосунка, а потім видаляє неї, запускаючи майнер у фоновому режимі:

У коді HiddenMiner не передбачені який-небудь контролер або оптимізатор, тобто додаток постійно майнить криптовалюту Monero, поки всі ресурси пристрою не будуть виснажені. Це може привести до перегріву й повної відмови пристрою.

Cisco Talos публікує докладне дослідження трояна KeyDroid, що маскується під «відновлення для Android»

Зловмисне програмне забезпечення повідомляє зловмисників інформацію про встановлені додатки, номер телефону, унікальному ідентифікаторі пристрою, місці

розташування, збережених контактах, а також передає СМС, запису розмов, електронні листи й фотографії.

Шахрайський додаток Pingu Cleans Up підписувало користувачів на дорогий сервіс, використовуючи легітимний спосіб оплати в Google Play і соціальну інженерію

Після установки на мобільний пристрій додаток пропонував користувачеві створити ігрового персонажа.

– На перших двох етапах його створення потенційна жертва вибирала потрібний атрибут і повинна була підтвердити свій вибір, нажавши на кнопку «Підтвердити» у спливаючому вікні.

– На третьому етапі користувач із банківською картою, прив'язаної до аккаунту Google Play, бачив вікно, що візуально нагадує попередні. Однак кнопка «Підтвердити» була замінена кнопкою «Підписатися».

– Нажавши на неї, користувач оформляв підписку вартістю 5,49 євро в тиждень. Платіж списувався з карти автоматично до моменту скасування підписки.

Уразливості в мессенджері Telegram дозволяють одержати доступ у приватні чати й редагувати чужі публікації в Telegraph

Особливості мессенджера WhatsApp можуть поставити під погрозу конфіденційність користувачів.

Кваліфікований користувач може одержати доступ до більших обсягів даних з публічних груп WhatsApp за допомогою малопотужного сервера, мобільного телефону, на якому встановлений мессенджер, і декількох скриптів і додатків.

Уразливості в електроенцефалографах Natus Xltek можуть привести до вилученого виконання коду, а також відмові в обслуговуванні.

Через помилки в убудованому ПЗ спеціально створений мережний пакет може викликати переповнення буфера й виконання довільного шкідливого коду. Зловмисники можуть змінювати показання приладів і одержати доступ до даних про стан здоров'я пацієнтів.

У голосовому помічнику Siri виявлена критичний пролом, що дозволяє прочитати сховані повідомлення на iPhone

Щоб одержати доступ до вмісту повідомлень на заблокованому екрані, потрібно розблокувати пристрій, однак знайдений пролом в Siri дозволяє обійти ці захисні міри. Однак якщо попросити Siri прочитати повідомлення вголос, вона охоче виконає прохання.

В macOS виявлена уразливість, що дозволяє одержати доступ до паролів від зашифрованих зовнішніх жорстких дисків APFS.

Щоб відтворити уразливість, потрібно

– Створити за допомогою Disk Utility «чистий» флеш-накопичувач у форматі Mac OS Extended (Journaled).

– Вибрати в меню опцію «Стерти» і створити тім Encrypted APFS з ім'ям SECRET_USB. 3. Нажати на «Стерти» і дочекатися закінчення операції.

– Поки операція виконується, запустити команду Термінала

– log stream -info -predicate 'eventMessage contains “newfs_”'

і одержати пароль.

Пароль виводиться при запуску команди з параметрами newfs_apfs і -S. Параметра -S офіційно не існує, тому що він відсутній у документації.

Комп'ютери адміністрації Атланти, штат Джорджія, піддалися атаці шифрувальника SamSam

В офіційному Twitter міста незабаром з'явилося повідомлення про те, що деякі клієнтські додатки можуть не працювати, і в користувачів можуть виникнути труднощі з оплатою рахунків і доступом до судових документів:

Інцидент торкнулися як публічні, так і внутрішні додатки, використовувані містом. Деякі дані виявилися зашифровані, однак влади поспішили завірити, що системи

забезпечення суспільної безпеки й водопостачання, а також міський аеропорт, працюють у штатному режимі.

За розблокування одного комп'ютера зловмисники вимагають 6800 доларів, а за розшифровку всіх даних – 51 000 доларів.

Описано нову атаку на процесори Intel, що одержав ім'я BranchScope

Як Meltdown і Spectre, BranchScope використовує в роботі особливості спекулятивного механізму виконання команд. Атака дозволяє атакуючий витягти з уразливого пристрою конфіденційні дані, які в нормальних обставинах не повинні бути доступні прямо. Щоб здійснити атаку, зловмисник повинен мати доступ до системи й можливість виконувати довільний код.

Виявлено шкідливу кампанію, у ході якої зловмисники розповсюджують шкідливе ПЗ й майнери криптовалюти через завантажники потенційно небажаних програм у спливаючих рекламних вікнах:

При натисканні на кнопку «Завантажити» на файлообміному сервісі відкривається нове рекламне вікно з посиланням на завантаження зловмисного програмного забезпечення ICLoader. Жертва думає, начебто це справжні файли із сайту, і клікає на посилання. Установившись на комп'ютері користувача, ICLoader може завантажувати небажане або шкідливе ПЗ.

Крім безкоштовних файлообмінників і сайтів для обміну зламаними програмами, ICLoader також поширюється через підроблені торрент-сайти. Посилання на завантаження на цих сайтах ведуть на сторінку завантаження ICLoader.

Сучасні кіберзлочинці практично не прибігають до злому, щоб викрасти гроші. У більшості случає їхньої жертви добровільно віддають доступ до своєму онлайн-банку або переказують гроші на потрібний рахунок. Це робиться за допомогою прийомів соціальної інженерії, що експерти по безпеці називають головною проблемою теперішнього часу.

У статті описано, як шахраї переконують віддавати їм гроші, а також головні міри захисту:

– Нікому й ніколи не повідомляйте паролі для входу в онлайн-банк, номер банківської карти, CVC-код і іншу інформацію, що дозволяє зробити списання. Навіть якщо що подзвонив представиться співробітником банку й буде мати про вас якусь інформацію (знати ПІБ, дату народження й т.д.).

– Переконаєтеся, що розмовляєте саме зі співробітником банку, МФО й т.д. Не впевнені – передзвоните самостійно в банк або МФО. У випадку можливих проблем з банківською картою краще дзвонити по телефонах, зазначеним на звороті карти.

– Не відкривайте повідомлення й не переходите по посиланнях від незнайомих осіб. Навіть якщо від знайомого приходить несподіване повідомлення (наприклад, від малознайомого колеги – текст типу «приколися, як я відриваюся») – уточните, дійсно він направляв вам це повідомлення або його поштова скринька була зламана.

– Те ж стосується повідомлень у соцмережах – якщо друг просить грошей у борг або поповнити йому телефон, переконаєтеся, що прохання виходить від друга, а не від взломавшего його аккаунт зловмисника.

– Вивчайте погрози, пов'язані із соціальною інженерією: читайте публікації, присвячені цьому питанню, у тому числі про нові методи зловмисників.

Кібермошенники використовують спеціалізований компонувальник ThreadKit для створення й розсилання документів, що експлуатують уразливості в MS Office.

З його допомогою роздавались банківські трояни Trickbot і Chthonic, викрадачі інформації FormBook і Loki Bot, а також зловмисне програмне забезпечення, якими оперує кримінальне угруповання Cobalt.

Зафіксовано декілька спам-кампаній з використанням ThreadKit. Одним з ланок ланцюжка зараження є HTA-файл, що завантажує маскувальний документ і VBS-скрипт для розпакування й запуску файлу, що виконується. У результаті експлойта на машину жертви

на той момент установлювався завантажник Smoke Loader, що накачував із зовнішнього ресурсу банкер Trickbot. Нові ThreadKit-кампанії поширюють ботів Neutrino, вони ж Kasidet.

Зловмисне програмне забезпечення Trojan.PWS.Stealer.23012 викрадає із зараженого пристрою файли й інша конфіденційна інформація. Витік цих даних може привести до крадіжки облікових записів жертви в соціальних мережах і інших онлайн-сервісах

Посилання на шкідливу програму публікуються в коментарях до відеороликів на YouTube, присвяченим шахрайським методам проходження ігор із застосуванням спеціальних додатків. Кіберзлочинці намагаються видати троянца за такі програми й інші корисні утиліти.

Зловмисне програмне забезпечення AVCrypt перед шифруванням файлів жертви намагається видалити антивірусні програми й видаляє деякі служби Windows

cmd.exe /C sc config "MBAMService" start= disabled & sc stop "MBAMService" & sc delete "MBAMService";

Першою справою AVCrypt намагається деактивувати Windows Defender і Malwarebytes. Щоб позбутися від антивірусних програм, зловмисне програмне забезпечення видаляє служби Windows, необхідні для їхньої правильної роботи: MBAMProtection, Schedule, TermService, WPDBusEnum, WinDefend і MBAMWebProtection. Потім шифрувальник перевіряє, чи зареєстрована яка-небудь антивірусна програма в Центрі забезпечення безпеки Windows (Windows Security Center), якщо це так, AVCrypt видаляє ці дані через командний рядок.

Шкідливий скрипт DiskWriter або UselessDisk заміняє завантажувальний сектор жорсткого диску власним, перезавантажує систему й вимагає викуп

Сума викупу становить 300 доларів США, які потрібно перевести на анонімний біткойн-гаманець. Зловмисне програмне забезпечення знищує або шифрує таблицю розділів диску, тому відновлення завантажувального сектора стандартними засобами операційної системи результату не приносить.

Програма діє як типовий здирник, але ряд ознак указує на те, що одержання викупу не є метою її творця. Всі вимоги містять той самий номер гаманця, автор не залишає ніяких контактів для зв'язку, а послання жертві майже повністю копіює повідомлення сумно відомого зловмисного програмного забезпечення NotPetya.

Розробка структурної схеми

Недавно ми помітили, що додаток пропускає email-адреси в небезпечному форматі. Конкретно в тому випадку, відбувалося відсилання листа з адресою без escape-послідовностей.

Перевірка адрес відбувалася, але лише за допомогою стандартного Java-валідатора javax.mail.internet.InternetAddress.validate(). На сторінці Вікіпедії присутні легітимні адреси, які здебільшого успішно проходять перевірку методами бібліотеки Java.

У зловмисників є два способи зробити ін'єкцію через email-адресу: коментарі й лапки. Java-валідатор не пропускає коментарі, але пропускає рядки, укладені в лапки. Приклад легітимної адреси з лапками:

"john.smith"@example.org

Або такий:

"john.smith<script>alert(1);<script>"@example.org

Останній приклад – канонічний тест на наявність можливості XSS-атаки.

В останньому прикладі email-адресу використовувалася як вихідну адресу, але цей випадок, як правило, не придатний для XSS-атак, оскільки поштові додатки найчастіше не мають движків на базі JavaScript або взагалі відмовляються виконувати будь-які скрипти. Іноді зловмисники все-таки знаходять лазівки, але зробити подібне досить складно. Якщо все-таки уразливість перебуває, то проблема стає набагато більше масштабної чим те, про що я розповідають у даній роботі.

Сучасні поштові клієнти допускають використання CSS, і, відповідно, є можливість додавання довільного HTML-коду й зміни частини листа, видимої користувачеві. Подібний розклад дозволяє успішно виконувати фішінгові атаки, оскільки зловмисник може сформувати шкідливі повідомлення від імені легітимних сервісів.

Мій основний застосунок для читання пошти – Mail.app (ОС OSX), другорядний – Thunderbird. У досліджуваному застосунку є строгі обмеження: адресу – не більше 50 символів, домен – не менш двох частин, друга з яких повинна складатися як мінімум із двох символів.

(Ці умови не прописані в RFC, і подібних фільтрів немає в Java-Бібліотеках). З огляду на лапки й формат домену, я можу передати максимум 43 символу:

"XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX"@x.xx

Природно, сюди ж необхідно додати що відкривається й закривається тег style:

"<style>XXXXXXXXXXXXXXXXXXXXXXXXXXX</style>"@x.xx

Але навіть незважаючи на подібні обмеження, завдяки коротким URL і директиві @import, ми можемо вставити корисне навантаження:

"<style>@import 'http://xxxxxxxxxxx'</style>"@x.xx

Префікс http:// обов'язковий так само як і лапки.

Виникає закономірне питання: чи можливо знайти короткий домен з 11 символів? Отут є 2 варіанти: зареєструвати домен на зразок «ant.nu», або скористатися сервісом ly.my. В останньому випадку ми можемо укластися в 9 символів:

"<style>@import 'http://ly.my/pva'</style>"@x.xx

Далі перезаписуємо поштове повідомлення корисним навантаженням приблизно наступного виду:

```
body {
visibility: hidden;
}
body:after {
content:'We have detected unauthorized access to your account. Please visit http://example.account-recovery.net/ to restore access, or call 555-1212.';
visibility: visible;
display: block;
position: absolute;
padding: 5px;
top: 2px;
}
```

Висновки:

1. Валідатори email-адрес не ідеальні.
2. У більшості поштових клієнтів повинна бути присутнім додаткова перевірка зовнішніх посилань і додаткові можливості на прикладі в Thunderbird, де пропонується припинення завантаження зовнішнього вмісту.

На структурній схемі (рисунок 1) зображена розроблена під час дипломного проектування система реалізації методів соціального інжинірингу через адресу e-mail.

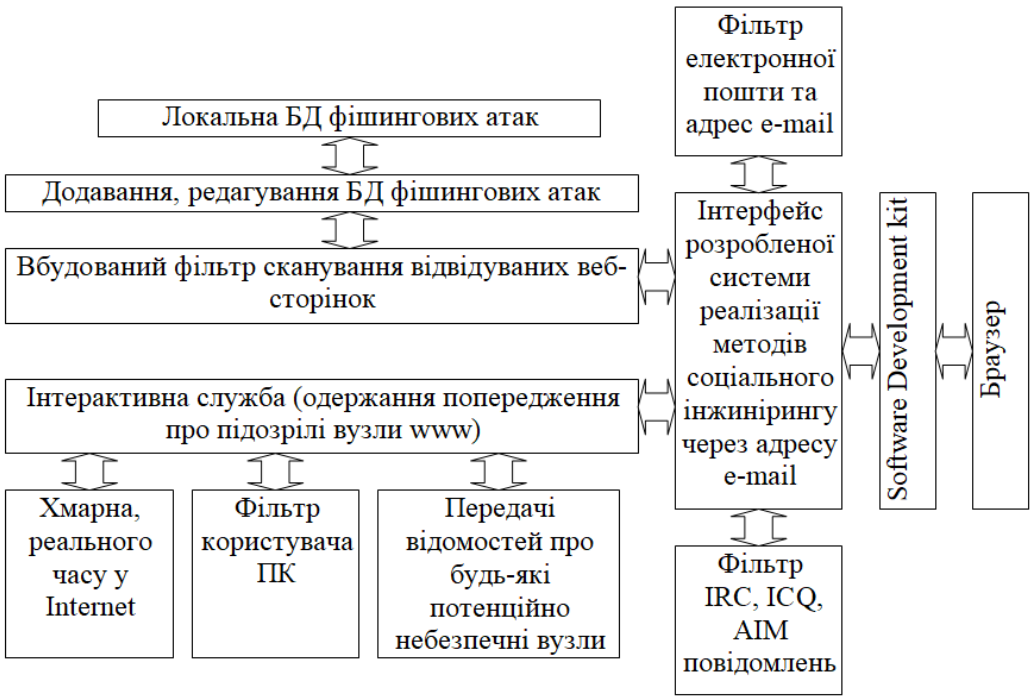


Рисунок 1 – Структурна схема системи

Розробка системи реалізації методів соціального інжинірингу через адресу e-mail повинна ґрунтуватися на потужній базі – браузері з розширеними можливостями. Так як найпоширеніший браузер Microsoft Internet Explorer поширюється із закритим вихідним кодом, а також має сховану структуру, що негативно впливає при написанні додаткових програм і плагинів на його основі й проаналізувавши існуючі на даний момент браузери, і їхні розподілені системи захисту , я зупинив свій вибір на браузері FireFox.

Він має величезну кількість переваг, головна з яких – надання великої кількості підпрограм що дозволяють одержати доступ до пошти, використанню Інтернет-пейджерів систем IRC, ICQ, AIM.

FireFox розповсюджується із частково відкритим кодом і має розширений набір засобів (Software Development Kit) для написання й розповсюдження додатків на його основі.

Як показано на рисунку 1, система реалізації методів соціального інжинірингу через адресу e-mail заснована на браузері FireFox і робить взаємодію через Software Development Kit.

Розглянемо загальні можливості розробленого програмного забезпечення зображені на схемі. Через розроблену систему реалізації методів соціального інжинірингу через адресу e-mail відбуваються наступні дії:

1. Фільтр електронної пошти – дозволяє частково убезпечити поштові повідомлення від фішингових атак розширеним керуванням і контролем даних, що надходять,. Фільтр спільно працює з антивірусними програмними продуктами й фаєрфолами (якщо такі присутні в операційній системі) не викликаючи конфліктних ситуацій і зависань тому що працює через браузер Firefox.

2. Фільтр IRC, ICQ, AIM повідомлень – При використанні внутрішньої програми спілкування через Інтернет-пейджери IRC, ICQ, AIM – розроблене програмне забезпечення реалізації методів соціального інжинірингу через адресу e-mail дозволяє контролювати процес передачі файлів і не дати зробити несанкціонований запуск шкідливої програми на ПК.

3. Інтерактивна служба (одержання попередження про підозрілі вузли “www.”) – складається із трьох підрозділів, які дозволяють інтерактивно контролювати WEB контент, який попадає на машину користувача.

3.1. Реального часу на основі IE 7.0, Opera Software (GeoTrust) у глобальній мережі – з версії браузерів IE 7.0 і Opera 8.0 з'явився новий безкоштовний Інтернет сервіс, який надає доступ до всесвітньої бази перевірки веб-вузлів. В Інтернеті існує величезна кількість посилань на сайти при переході на які, відбувається запуск шкідливого програмного забезпечення й крадіжка особистої інформації, у даних випадках антивирустні програми неспроможні тому що використовуючи помилки ОС шкідливі програми одержують статус перевірених. За допомогою цього безкоштовного сервісу й розробленого в дипломному проекті можна значною мірою усунути можливість запуску такого шкідливого коду.

Інтерактивний сервіс повертає наступні повідомлення:

– Веб-вузли, підозрювані в атаках.

– Веб-вузли, на яких фішинг-атаки вже відбувалися.

– Чорний список.

3.2 Фільтр користувача в ПК – локальний фільтр блокування доступу складений користувачем. Існують різні ситуації під час роботи ПК, фільтр користувача дозволяє скласти список ресурсів доступ на який буде заборонений при переадресаціях і.т.ін.

3.3 Передати відомості про будь-які потенційно небезпечні вузли – можливість послати в інтерактивну службу дані для перевірки на наявність на сайті фішингово-шкідливого коду.

4. Вбудований фільтр сканування відвідуваних веб-сторінок – розширені можливості переходу на сторінки, які відвідувалися, з перевіркою на можливу переадресацію, а також база шаблонів відомих шкідливих кодів з можливістю редагування.

4.1 Додавання, Редагування БД – можливість редагування й ручного додавання шаблона відомих шкідливих кодів.

4.2 Локальна БД фішингових атак – шаблонів відомих шкідливих кодів.

За допомогою даних засобів імовірність фішингової атаки через електронну пошту й Spam, фішинг-атаки з використанням web-контента, фальсифиция рекламних банерів, IRC і передача IM-повідомлень, використання троянських програм значно зменшується надаючі користувачеві надійну систему захисту.

Висновок. У статті розглянуто та проаналізовано програмне забезпечення, створене в результаті виконання роботи, призначено для системи реалізації методів соціального інжинірингу через адресу e-mail. В межах України в недостатній мірі представлені вітчизняні розробки в цій області. У роботі наведені теоретичне узагальнення й рішення наукового завдання дослідження методів реалізації методів соціального інжинірингу через адресу e-mail. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем реалізації методів соціального інжинірингу через адресу e-mail; Досліджена система реалізації методів соціального інжинірингу через адресу e-mail; На основі отриманих результатів досліджень створена програмна реалізація системи реалізації методів соціального інжинірингу через адресу e-mail. Розроблені під час виконання роботи алгоритми дозволяють успішно вирішувати завдання реалізації методів соціального інжинірингу через адресу e-mail. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки. Розроблене програмне забезпечення має простий, дружній та зручний інтерфейс користувача, що забезпечує легкість у освоєнні роботи програмного продукту, зручність у використанні, і не потребує особливих спеціальних знань. При створені програмного забезпечення було використано об’єктно-орієнтований підхід, що відповідає сучасним тенденціям у галузі розробки комерційних програмних систем. Програма реалізована на мові високого рівня Delphi 10.2, XUL. Дана мова програмування дозволяє найбільш ефективно обробляти дані. Це дозволило мінімізувати строк розробки програмного забезпечення, і, як слід, зменшити витрати на його розробку. Запропоноване програмне забезпечення ділиться на загальне програмне забезпечення, що поставляється із засобами обчислювальної техніки й спеціальне програмне забезпечення, що спеціально розроблене

для даної конкретної системи й включає програми, що реалізують її функції. Програма призначена для виконання під управлінням багатозадачної операційної системи Windows XP/Vista/7/8/10. Даються необхідні рекомендації з установки розробленого програмного забезпечення. Для підвищення рівня безпеки запропоновано застосовувати алгоритм DSA.

Список літератури

1. Смирнов А.А. Анализ и сравнительное исследование перспективных направлений развития цифровых телекоммуникационных систем и сетей / А.А.Смирнов, В.В.Босько, Е.В.Мелешко // Системи обробки інформації. – Х.: ХУ ПС, 2008. – Вип.7(74). – С.120-123.
2. Смирнов А.А. Усовершенствование метода управления очередями в многопротокольных узлах телекоммуникационной сети / А.А.Смирнов, Е.В.Мелешко // Збірник тез та доповідей другої всеукраїнської науково-практичної конференції «Системний аналіз. Інформатика. Управління». Запоріжжя. Тези доповідей. Запоріжжя: КПУ, 2011.
3. Смирнов С.А. метод безопасной маршрутизации метаданных в облачные антивирусные системы / А.К. Дидык, С.А. Смирнов // Информационные технологии в управлении, образовании, науке и промышленности: монография / Под редакцией профессора В.С. Пономаренко. – Х.: Видавець Рожко С.Г., 2016. – 566 с.
4. Смирнов С. А. Сравнительные исследования математических моделей технологии распространения компьютерных вирусов в информационно-телекоммуникационных сетях / Мохамад Абу Таам Гани, А. А. Смирнов, А. В. Коваленко, С. А. Смирнов // Системи обробки інформації: зб. наук. праць. – Х.: ХУПС, 2014. – Вип. 9(125). – 105-110.
5. Смирнов С. А. Математическая модель интеллектуального узла коммутации с обслуживанием информационных пакетов различного приоритета / Мохамад Абу Таам Гани, А. А. Смирнов, Н. С. Якименко, С. А. Смирнов // Збірник наукових праць Харківського університету Повітряних Сил. – Харків: ХУПС, 2014. – Вип. 4 (41). – С. 48-52.
6. Смирнов С. А. Исследование показателей качества функционирования интеллектуальных узлов коммутации в телекоммуникационных системах и сетях / Мохамад Абу Таам Гани, А. А. Смирнов, Н. С. Якименко, С. А. Смирнов // Наука і техніка Повітряних Сил Збройних Сил України: наук. журн. – Х.: ХУПС, 2014. – № 4(17). – С. 90-95.
7. Смирнов С. А. Усовершенствованный алгоритм управления доступом к «облачным» телекоммуникационным ресурсам / Мохамад Абу Таам Гани, А. А. Смирнов, Н. С. Якименко, С. А. Смирнов // Системи обробки інформації: зб. наук. праць. – Х.: ХУПС, 2015. –Вип. 1(126). – С. 150-153.
8. Smirnov S.A. Method of controlling access to intellectual switching nodes of telecommunication networks and systems / A.A. Smirnov, Mohamad Abou Taam, S.A. Smirnov // International Journal of Computational Engineering Research (IJCER). – **Volume 5, Issue 5. –** India. Delhi. – 2015. – P. 1-7.
9. Смирнов С. А. Анализ и исследование методов управления сетевыми ресурсами для обеспечения антивирусной защиты даннях / Мохамад Абу Таам Гани, А. А. Смирнов, С. А. Смирнов // Системи озброєння і військова техніка: наук. журн. – Х.: ХУПС, 2015. – № 3(43). – С. 100-107.
10. Смирнов С. А. Исследование эффективности метода управления доступом к облачным антивирусным телекоммуникационным ресурсам / Мохамад Абу Таам Гани, А. А. Смирнов, С. А. Смирнов // Наука і техніка Повітряних Сил Збройних Сил України: наук. журн. –Х.: ХУПС, 2015. –№ 3(20). – С. 134-141.
11. Смирнов С. А. Комплекс gert-моделей технологии облачной антивирусной защиты телекоммуникационной системы / А. А. Смирнов, А. К. Дидык, А. Н. Дреев, С. А. Смирнов // Безпека інформації: наук. – практ. журн. – К.: НАУ, 2015. – Т. 21, № 3. – С. 251-262.

УДК: 615.322:633.82

А. Шамка, магістр гр. АГ-18М-1,9
Л. Сало, канд. с.-г. наук, доцент
Центральноукраїнський національний технічний університет

ВИВЧЕННЯ ВПЛИВУ ФАКТОРІВ ЖИВЛЕННЯ НА ФОРМУВАННЯ ВРОЖАЙНОСТІ СУЦВІТЬ НАГІДОК

Лікарські рослини вирощують в Україні майже на 2 тис. га полів. Ріст попиту на біологічну сировину в країнах Європи та можливість експорту продукції викликали зростання агробізнесу вирощування лікарських культур. Експерти прогнозують, що експорт лікарських трав з України у 2023 році збільшиться до $25-30 млн. [1].

Втім, український трав'яний агробізнес переживає ряд проблем вирощування лікарських рослин, серед яких – низький рівень врожайності. Основним чинником підвищення даного показника є оптимізація живлення рослин. Мікроелементи покращують засвоєння основних елементів живлення і є впливовим фактором отримання екологічно безпечної продукції рослинництва, що є надзвичайно важливим при вирощуванні лікарської сировини [2].

Нагідки лікарські по праву відносять до десятки найбільш популярних лікарських рослин. Тому вивчення елементів оптимізації удобрення даної культури залишається доволі актуальним [3].

В зв'язку з цим протягом 2018-2019 років нами були проведені дослідження по впливу мінеральних макро- та мікродобрив на врожайність лікарської сировини нагідок лікарських. Дослідження проводили шляхом закладання польового досліду за двофакторною схемою. Фактором А слугували два фони: без добрив та з припосівним внесенням нітроамофоски у нормі $N_{16}P_{16}K_{16}$. Фактор В включав 4 варіанти – контроль без обробки та три дози використання мікродобрив Вуксал Мікромінераліс (1, 2 та 3 л/га) для обробки вегетуючих рослин у фазі гілкування-початку формування кошиків. В досліді вивчали сорт нагідок Березотоцька сонячна. Ґрунт дослідної ділянки чорнозем звичайний глибокий важкосуглинковий на лесі.

Формування врожаю рослин здійснюється за оптимальних умов фотосинтезу. Інтенсивність накопичення органічної речовини залежить від площі листкової поверхні, яка визначається біометричними параметрами рослин і значною мірою залежить від режиму їх живлення.

Середній показник площі листків коливався в межах 8,5–13,8 тис.$м^2$/га. Мінімальний показник отримали у контрольному варіанті, а максимальний – у восьмому варіанті – застосування NPK з мікродобривом Вуксал Мікроплант у нормі 3 л/га.

Очевидно, що фонове внесення мінеральних добрив впливає на збільшення площі листкової поверхні у рослин, різниця склала 1,5 тис.$м^2$/га.

Аналізуючи середні показники за фактором В, можна стверджувати, що обробка рослин мікродобривом Вуксал Мікроплант помітно збільшує площу фотосинтетичного апарату рослин нагідок. Навіть мінімальна норма підвищує даний показник на 2,0-3,5 тис.$м^2$/га. Причому, хоча більший результат отримали на удобреному фоні, на неудобреному різниця до контролю була більша.

Різниця між варіантами з використанням 2 л/га та 3 л/га незначна, як з припосівним удобренням, так і без нього.

Тому можна стверджувати, що кратне збільшення норми Вуксал Мікроплант не викликає аналогічної реакції збільшення площі листкової поверхні.

При вивченні показників формування площі фотосинтетичного апарату важливою характеристикою є листковий індекс. Листковий індекс – коефіцієнт використання посівами земельної площі, і визначається як відношення сумарної листкової поверхні до площі поля.

З рисунка помітно, що характер впливу досліджуваних факторів був аналогічним в обидва роки досліджень з тою різницею, що у 2019 році листковий індекс був більшим у всіх досліджуваних варіантах. Так, у 2018 році показники були в межах 0,76-1,33, тоді як у 2019 вони коливались від 0,94 до 1,43.

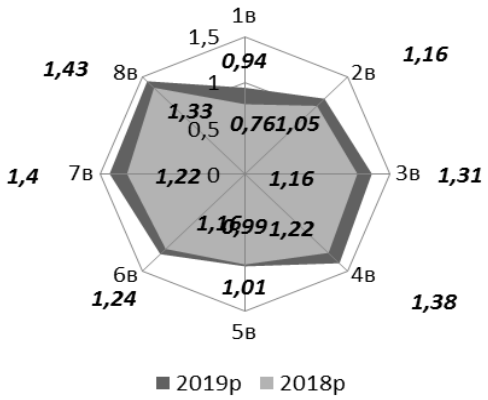


Рис.1. Листковий індекс рослин нагідок лікарських залежно від мінеральних добрив (2018-2019 рр.)

На рисунку помітно, що максимальна площина зорієнтована у четвертому, сьомому та восьмому варіантах. Це свідчить що саме за цих умов складаються найкращі умови для формування листкової поверхні. Тобто, на обох фонах це обробка Вуксал Мікроплант у нормі 3 л/га та обробка 2 л/га на фоні припосівного внесення нітроамофоски.

Врожайність нагідок складається із суми послідовних зборів. Результати досліджень сумарної врожайності кошиків по роках досліджень наведені в таблиці 1 та на рисунку 2.

Таблиця 1. Урожайність кошиків нагідок по роках досліджень, ц/га

Варіанти			Врожайність	Середня за фактором		Врожайність	Середня за фактором	
				A	B		A	B
			2018 р.			2019 р.		
1	Фон 1 без добрив	Контроль	8,2	11,6	9,4	9,7	13,4	11,0
2		Вуксал Мікроплант - 1л/га	11,2			13,6		
3		Вуксал Мікроплант - 2л/га	12,6		12,2	15,0		14,2
4		Вуксал Мікроплант - 3л/га	14,3			15,3		
5	Фон $N_{16}P_{16}K_{16}$	Контроль	10,6	13,2	13,2	12,4	15,3	15,8
6		Вуксал Мікроплант - 1л/га	13,1			14,8		
7		Вуксал Мікроплант - 2л/га	13,9		14,8	16,5		16,4
8		Вуксал Мікроплант - 3л/га	15,2			17,4		
$НІР_{05}$			*A-0,9 B-1,25 AB-1,8*			*A-1,1 B-1,5 AB-2,1*		
Частка впливу факторів			*A-9,7 B-57,1*			*A-9,7 B-57,1*		

Ми також виявили залежність динаміки добового приросту маси кошиків від досліджуваних факторів і біологічних особливостей культури нагідок. Добовий приріст максимальний на початку цвітіння, відсоток від загальної маси сформованих суцвіть складав близько 40%, надалі він помітно знижувався. У необроблених мікродобривами варіантах

період найвищої продуктивності помітно коротший, ніж при використанні підживлень, основна маса суцвіть (64%) формується за короткий період від першого до третього збирання. Найбільш тривалий період формування кошиків складається при внесенні максимальної норми Вуксал Мікроплант в досліді (3 л/га).

У 2018 році урожайність лікарської сировини нагідок на фоні з внесенням NPK відрізнялась від неудобреного фону більш високими показниками відповідно 10,6-15,2 ц/га до 8,2-14,3 ц/га. Максимальне значення було у восьмому варіанті, де рослини оброблялися Вуксал Мікроплант у нормі 3 л/га на фоні припосівного внесення нітроамофоски.

Аналізуючи вплив фактору А відзначено, що припосівне внесення NPK викликає істотне збільшення врожаю, різниця між середніми показниками становила – 1,6 ц/га при НІР – 0,9. За дії фактору В всі удобрені варіанти із застосуванням мікродобрив мали істотний вплив на підвищення врожайності суцвіть нагідок порівняно до контрольного варіанту. Збільшення складало від 2,8 до 5,4 ц/га при НІР 1,25.

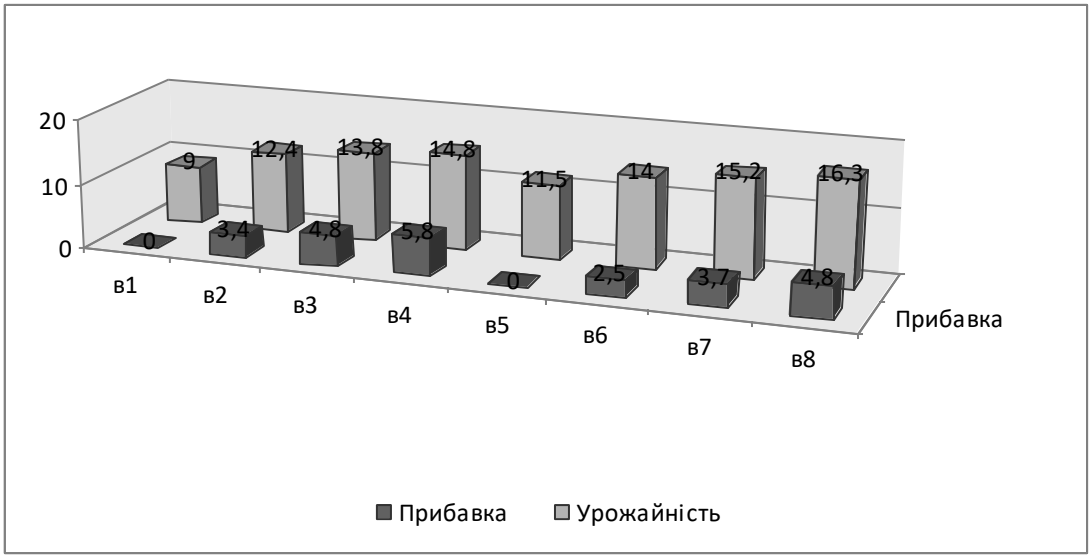


Рис. 2. Середня врожайність кошиків нагідок за 2018 – 2019 р.р.

Серед досліджуваних факторів більший вплив мав фактор В (мікродобрива). Частка його впливу становить 57,1%, тоді як від фактору А врожайність залежить лише на 9,7%. (Таблиця 1.).

В наступному 2019 році досліджень рівень врожайності сировини нагідок складав від 9,7 до 17,4 ц/га. Максимальна врожайність була при використанні Вуксал Мікроплант у нормі 3 л/га на фоні припосівного внесення нітроамофоски. Аналізуючи вплив фактору А помітно, що варіанти з припосівним внесенням нітроамофоски мали істотне збільшення врожаю, різниця між ними становила – 1,9 ц/га при НІР – 1,1. Аналіз дії фактору В показує, що всі удобрені варіанти із застосуванням мікродобрив мали істотний вплив на ріст врожайності нагідок порівняно до контрольного варіанту. Збільшення складало від 2,2 до 5,4 ц/га при НІР 1,5.

Частка впливу фактору В (мікродобрива) становить 57,4%, тоді як від фактору А врожайність залежить лише на 11,9%, отже, як і в попередньому році, фактор В був визначальним.

Усереднені результати врожайності за два роки досліджень (Рисунок 1) підтверджують отриману по роках залежність. Урожайність суцвіть нагідок коливалася від 9,0 до 16,3 ц/га.

Мінімальний показник отримали в контрольному варіанті, а максимальний – у восьмому варіанті, де використовували Вуксал Мікроплант у нормі 3 л/га на фоні припосівного внесення нітроамофоски. Помітно, що урожайність на неудобреному фоні була меншою ніж на фоні з внесенням NPK при сівбі.

Що стосується фактору В, то обробка рослин мікродобривами підвищували врожайність кошиків нагідок як в самостійному застосуванні, так і на фоні мінеральних добрив. Максимальний вплив на формування врожайності прослідковується при внесенні Вуксал Мікроплант у нормі 3 л/га на фоні припосівного внесення нітроамофоски.

Тож за результатами дворічних досліджень можна зробити наступні висновки.

Висновки: Найбільша площа листкової поверхні формується при застосуванні мікродобрива Вуксал Мікроплант у нормі 3 л/га на фоні припосівного внесення $N_{16}P_{16}K_{16}$. Добовий приріст маси кошиків нагідок максимальний на початку цвітіння, надалі він помітно знижується. У необроблених мікродобривами варіантах період найвищої продуктивності помітно коротший, ніж при використанні підживлень. Припосівне внесення добрив підвищує врожайність культури. Максимальну врожайність отримали при застосуванні Вуксал Мікроплант в нормі 3 л/га на фоні внесення нітроамофоски.

Список літератури

1. Майже на 2 тис. га українських полів вирощуються лікарські рослини [Електронний ресурс]. – 2019. – Режим доступу до ресурсу: https://superagronom.com/news/7361-mayje-na-2-tis-ga-ukrayinskih-poliv-viroschuyutsya-likarski-roslini.
2. Булигін С.Ю. Мікродобрива важливий резерв підвищення урожайності сільськогосподарських культур / С.Ю. Булигін, А.І. Фатєєв, Л.Ф. Демішев, Ю.Ю.Туровський // Вісн. аграр. науки. – 2000. – № 11. –С. 13-15.
3. Куценко Н. І. Перспективи селекційних досліджень лікарських та ефіроолійних рослин в україні / Н. І. Куценко. // Агроекологічний журнал. – 2016. – №2. – С. 85–92.

УДК 004

Д. Шашин, магістр гр. КІ-18МЗ-1,4
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ ЕКРАНІВ DIGITAL SIGNAGE ЩО ОБЕРТАЮТЬСЯ, З СИНХРОНІЗОВАНИМ ВІДЕОПОТОКОМ

У статті розроблено програмне забезпечення, яке призначено для системи екранів Digital Signage що обертаються, з синхронізованим відеопотоком. Метою розробки є дослідження та програмна реалізація системи екранів Digital Signage що обертаються, з синхронізованим відеопотоком. Об’єктом дослідження є процес екранів Digital Signage що обертаються, з синхронізованим відеопотоком. Предметом дослідження є методи екранів Digital Signage що обертаються, з синхронізованим відеопотоком. Методи дослідження базуються на методах теорії кодування відеоданих, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи екранів Digital Signage що обертаються, з синхронізованим відеопотоком. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

комп’ютерна інженерія, Digital Signage, відеопоток

Постановка проблеми. З тих пір, як рекламні агентства й роздрібні мережі почали активно впроваджувати системи Digital Signage, була проведена безліч досліджень їхньої ефективності. От що вдалося з'ясувати психологам і маркетологам:

- 60% покупок відбувається імпульсивно;
- завдяки Digital Signage імовірність покупки зростає на 20-120%;
- 77% аудиторії звертають увагу на динамічне зображення;

– при перегляді відео час очікування біжить на 35% швидше;

– 42% аудиторії воліють купувати в тих магазинах, де демонструється цифрове відео;

– 76% покупців хочуть користуватися інтерактивними системами;

– 30% споживачів вважають, що цифрові меню мотивують до здійснення покупки.

Ефективність Digital Signage більше не піддається сумніву, і при впровадженні мова йде про те, як прискорити повернення інвестицій і досягти максимальних показників ефективності. Цього можна домогтися двома способами: запропонувати більше якісний, таргетований контент або підсилити вплив за рахунок технічних інновацій.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи екранів Digital Signage що обертаються, з синхронізованим відео потоком.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи екранів Digital Signage що обертаються, з синхронізованим відеопотоком.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем екранів Digital Signage що обертаються, з синхронізованим відеопотоком.

– Дослідження системи екранів Digital Signage що обертаються, з синхронізованим відеопотоком.

– Програмна реалізація системи екранів Digital Signage що обертаються, з синхронізованим відеопотоком.

Об'єктом дослідження є процес екранів Digital Signage що обертаються, з синхронізованим відеопотоком.

Предметом дослідження є методи екранів Digital Signage що обертаються, з синхронізованим відеопотоком.

Методи дослідження базуються на методах теорії кодування відеоданих, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Розгортання системи Digital Signage – складний проект, при реалізації якого доводиться враховувати багато важливих нюансів: від вибору засобів відображення й визначення оптимальної архітектури – до розробки контентної стратегії й підготовки інформації для відтворення в системі. Нижче коротко представлені проекти й/або рекомендації провідних постачальників і інтеграторів, що займаються відповідними системами.

Завдання

На об'єкті, у торговому центрі площею 10 000 м^2 необхідно розгорнути систему Digital Signage для надання відвідувачам різної інформації й показу реклами. З обліком непростої економічної ситуації замовник зацікавлений у тім, щоб система забезпечила швидке повернення інвестицій. Відповідні розрахунки вітаються.

Засоби відображення (замовник просить рекомендувати конкретні моделі продуктів і прокоментувати вибір використовуваних технологій):

– 25 панелей (дисплеїв) с діагоналлю 40-55";

– 1 відеостіна типового розміру 2х2 або 3х3 з панелей 40-55" (розмір на розсуд постачальника);

– 1 світлодіодна панель для установки на вулиці (розмір на розсуд постачальника).

Основна функціональність (укажіть особливості й спосіб реалізації):

– подача й вивід на дисплеї в заданій (що налаштовується) послідовності інформації різного типу: відеофайли, аудіофайли, зображення, текст і таблиці, сторінки Web-сайтів і інше.;

– трансляція на дисплеї зовнішніх ТБ-програм і довідкової інформації (курси валют, прогноз погоди, інформація про пробки та ін.);

– гнучке настроювання графіка видачі інформації;

– можливість створення зон трансляції, аж до окремого дисплея: наприклад, щоб магазин або інший орендар міг транслювати власний контент на розташованій поруч панелі.

Інфраструктура

Передбачається, що відстань від серверної кімнати (де розташовуються сервери з локальним контентом і куди надходить зовнішній контент) до самого вилученого дисплея не перевищує 150 м.

– Укажіть необхідне для реалізації системи Digital Signage устаткування і його конкурентні переваги:

– передавачі/приймачі;

– контент-плеєри;

– комутатори;

– засоби формування відеостіни;

– інше.

Замовник хотів би для доставки контенту до засобів відображення використовувати наявну на об'єкті гігабітну локальну мережу Ethernet. Чи можливо це? Якщо ні, надайте інформацію про необхідність модернізації локальної мережі або побудови нової мережі для функціонування системи Digital Signage.

Додаткові побажання:

– запропонуйте рішення по інтеграції системи Digital Signage із системою аварійного оповіщення (вивід на панелі інформації про позаштатну ситуацію й показ напрямків до виходу);

– запропонуйте систему створення контенту з більшим числом шаблонів, за допомогою якої замовник зможе самотужки формувати необхідний контент.

Засоби відображення

Вибір форматів відображення інформації – одне із самих відповідальних завдань. Для подібних проектів найбільш актуальні й перспективні «великі формати»: напольні тотеми з більшими дисплеями, відеостіни, нестандартні конструкції на основі світлодіодних екранів. При виборі місць розміщення засобів відображення Digital Signage він рекомендує дотримуватися простого правила: цифрові конструкції варто встановлювати там, де ви розташували б (або де вже розташовуються) світлові короби й надруковані баннери.

Щоб грамотно вибрати дисплеї, варто враховувати безліч параметрів. До їхнього числа ставляться кути огляду, характеристики приміщення, тривалість роботи протягом доби, дистанції перегляду та ін. Ці параметри можна спробувати попередньо уточнити в замовника або одержати під час передпроектного обстеження ТЦ, результатом якого вже стануть рекомендації з вибору конкретних моделей, а також можливих місць їхньої установки.

Покладається, що при виборі дисплеїв для даного сегмента не слід гнатися за низькою ціною й купувати у звичайних магазинах електроніки стандартні телевізори, які усе ще зустрічаються в різних проектах. Необхідно використовувати професійні дисплеї, які залежно від конкретних завдань можуть бути не набагато дорожче. Уважається: при цьому ви одержите більші переваги при експлуатації систем Digital Signage на основі професійних дисплеїв, що в підсумку обернеться істотною економією

Потрібно вибирати дисплеї з діагоналями не менше 46–48″ і взагалі рекомендує не розглядати для подібних проектів панелі з діагоналями 40-42″. У більшості випадків вибір залежить від розмірів приміщення й висоти стель, але найчастіше самими підходящими виявляються дисплеї 55?. Власне кажучи, саме цей розмір і виявився самим популярним у присланні нам пропозиціях.

Архітектура системи

Вибір архітектури системи Digital Signage залежить від безлічі факторів, таких, наприклад, як розмір ТЦ і пропускна здатність наявної мережної

інфраструктури. Відзначимо ще такий фактор, як формат віщання, а точніше – кількість трансльованих каналів: чи буде на всіх екранах відтворюватися один канал, чи є кілька груп каналів або планується показувати індивідуальний канал на кожному екрані. Немаловажно й те, як розташовуються екрани – тільки один або відразу кілька екранів будуть видні відвідувачеві ТЦ.

Все різноманіття варіантів розміщення медіаплеєрів можна розділити на дві більші групи: плеєри розташовуються поруч із екранами (або із групами екранів) або централізовано, наприклад у серверній або апаратній кімнаті. Фахівці виділяють у кожній групі ще по двох варіанта.

Чотири архітектури Digital Signage:

– установка окремого плеєра на кожний екран (або на два екрани, розташованих «спиною до спини»);

– установка плеєра на групу рядом розташованих екранів (підключення екранів кабелями або за допомогою подовжувачів по кручений парі);

– установка плеєра (або плеєрів) у серверній кімнаті й комутація за допомогою подовжувачів сигналу по кручений парі або оптиці;

– установка плеєра (або плеєрів) у серверній кімнаті й доставка відеосигналу по IP (для цього біля кожного екрана повинен перебувати IP-декодер або бути убудовані можливості для програвання IPTV).

При централізованому розміщенні плеєрів вимоги до каналів зв'язку, що забезпечує підключення дисплеїв, – вище. Але, по завіренню більшості експертів, гігабітной локальної мережі буде цілком достатньо. Рекомендується організувати окрему підмережу (приміром, створити зону DMZ), і тоді всі потоки інформації, використовуваною системою Digital Signage, будуть відділені від трафіку інших застосунків. Якщо вимоги до надійності високі, і є необхідний бюджет, можна прокласти окремі кабелі й створити повністю незалежну підмережу, що дозволить контролювати всі елементи системи й не залежати від зовнішніх факторів.

Для передачі відео по звичайній локальній мережі (IP-віщання), як правило, потрібна установка спеціальних засобів для впакування (кодування) і розпакування (декодування) відео. Можливий і альтернативний варіант: передача відео за допомогою подовжувачів сигналу. Але застосування подібних подовжувачів відеосигналу обґрунтовано в поточних умовах тільки локально, коли потрібно розділити один відеосигнал на трохи однакові на невеликих відстанях. Варто також мати на увазі, що, оскільки в нашім вигаданому випадку дальність може досягати 150 м, для передачі сигналу у форматі Full HD можуть знадобитися передавачі по оптичному кабелі, що збільшує бюджет проекту.

При використанні стельових екранів найбільш типова ситуація – один канал віщання. Якщо мова йде про знову споруджуваному ТЦ або про будинок із сучасною мережною інфраструктурою, то оптимальним рішенням буде використання IP-віщання. У цьому випадку в серверній кімнаті встановлюються Digital Signage-плеєр і IP-передавач. Такий підхід звичайно простий у реалізації, у той же час він забезпечує достатню гнучкість – почати можна із трансляції одного віщального каналу, а потім додавати нові канали (установлюючи додаткові плеєри й передавачі), при цьому управляти тим, на яких екранах які канали показуються, можна віддалено. Сучасні професійні IP-декодери здатні автоматично перемикатися на програвання локального контенту. Це гарантує, що екрани не будуть чорними навіть у випадку втрати зв'язку з IP-передавачем.

Використання архітектури «один екран – один плеєр» не дуже поширено в ТЦ, тому що звичайно при цьому потрібно синхронізувати плеєри. Разом з тим відеостіни, світлодіодні конструкції й напольні тотеми звичайно обслуговуються незалежними плеєрами. У цих випадках синхронізувати контент звичайно не потрібно, а от гнучкість його подачі й керування, виходить на перший план.

Плеєри: убудовані й зовнішні

У більшості випадків медіаплеєри являють собою компактні комп'ютери (ПК або промислові) зі спеціальним ПЗ.

Окремо варто згадати запропоновані відразу декількома компаніями дисплеї Samsung з убудованим медіаплеєром (платформа System-on-Chip, SoC). На даній платформі за замовчуванням установлений безкоштовний клієнт MagicInfo-S. У плеєре вже є убудовані шаблони дизайну для швидкого створення контенту. У портфелі продуктів Samsung є й інші варіанти реалізації плеєрів: зовнішні модулі SBB або PIM, які являють собою міні-ПК. Модуль SBB кріпиться за панелі, а PIM установлюється в її спеціалізований слот.

Компанія NEC Display Solutions запропонувала плеєр, що встановлюється в слот OPS (технології Open Pluggable Specification, OPS, – спільна розробка NEC і Intel) рекомендованих моделей дисплеїв. Як вважають фахівці NEC, на відміну від рішень SoC, підхід, заснований на технології OPS, володіє рядом незаперечних переваг. Використовуючи незалежне рішення (медіаплеєр поставляється як опція додатково до дисплея), замовник одержує більше високий рівень надійності. Якщо медіаплеєр вийшов з ладу, міняти прийде тільки плеєр – це набагато дешевше, ніж заміна рішень SoC.

Система керування контентом

Система створення контенту й керування їм, мабуть, головний елемент Digital Signage. На даний момент по основних можливостях різні системи відрізняються не сильно, і з базовими завданнями впораються практично всі продукти, представлені на ринку. Для того щоб вибрати підходяще рішення, необхідно більш детально представляти майбутній процес керування створюваною системою Digital Signage, а також брати до уваги нюанси, наприклад, зручність і дружелюбність інтерфейсу керування, кількість дій, необхідних для створення плей-аркушів, наявність онлайн-статистики що програється контенту й оперативного моніторингу роботи системи.

Завдання сполучити трансляцію зовнішніх ТБ-програм і рекламно-інформаційних матеріалів, теж не унікальні, але список підтримуючу цю функцію ПЗ значно коротше. У сучасних системах дана функціональність найчастіше реалізується двома способами: перший – за допомогою зовнішнього медіаплеєра (або спеціального комп'ютера) з додатково встановленої на нього платою ТБ-тюнера або відеозахвата; другий – за допомогою медіаплеєрів, убудованих у сучасні професійні панелі, які підтримують дану функцію. Залежно від використовуваного ПЗ, ТБ-сигнал може транслюватися або на весь екран, або в певній зоні. При реалізації цієї функціональності Рекомендується для початку протестувати якість ТБ-сигналу, а також з'ясувати права на його використання.

Нашому вигаданому замовникові запропоновано ПЗ різних розроблювачів: DISA, Scala, Net Display Systems (NDS), Smartsign. Відразу кілька компаній зупинили свій вибір на продуктах Samsung і її системі керування Samsung MagicInfo, тому скажемо про неї тут кілька слів.

Вище вже згадувався клієнт MagicInfo S, установлюваний на окремо варті дисплеї з інтегрованим медіаплеєром (SoC). Серверне ПЗ MagicInfo Server дозволяє дистанційно управляти дисплеями, розкладом відтворення, регулювати настроювання, а також консолідувати всю інформацію про роботу панелей. Крім того, система забезпечує многоадресну трансляцію контенту по IP. Ще один компонент системи – MagicInfo Author – дає можливість створювати, редагувати й публікувати різні види медіаконтенту. Крім того, це ПЗ здатне завантажувати й відтворювати інформацію не тільки із сервера, але й з вилучених джерел (зовнішні ТБ-програми й довідкові інформаційні ресурси – курси валют, прогноз погоди, відомості про пробки та ін.) або з жорсткого диска плеєра, що значно знижує навантаження на робочу мережу.

Розробка структурної схеми

Запропонуємо два варіанти рішення. Обоє передбачають використання 25 дисплеїв Samsung DB55D і LED-відеостіни, а відрізняються вибором відеостіни: в одному варіанті вона створюється на основі дисплеїв Samsung 55, в іншому – на основі дисплеїв Planar Matrix 55″ с антивандальним покриттям ERO.

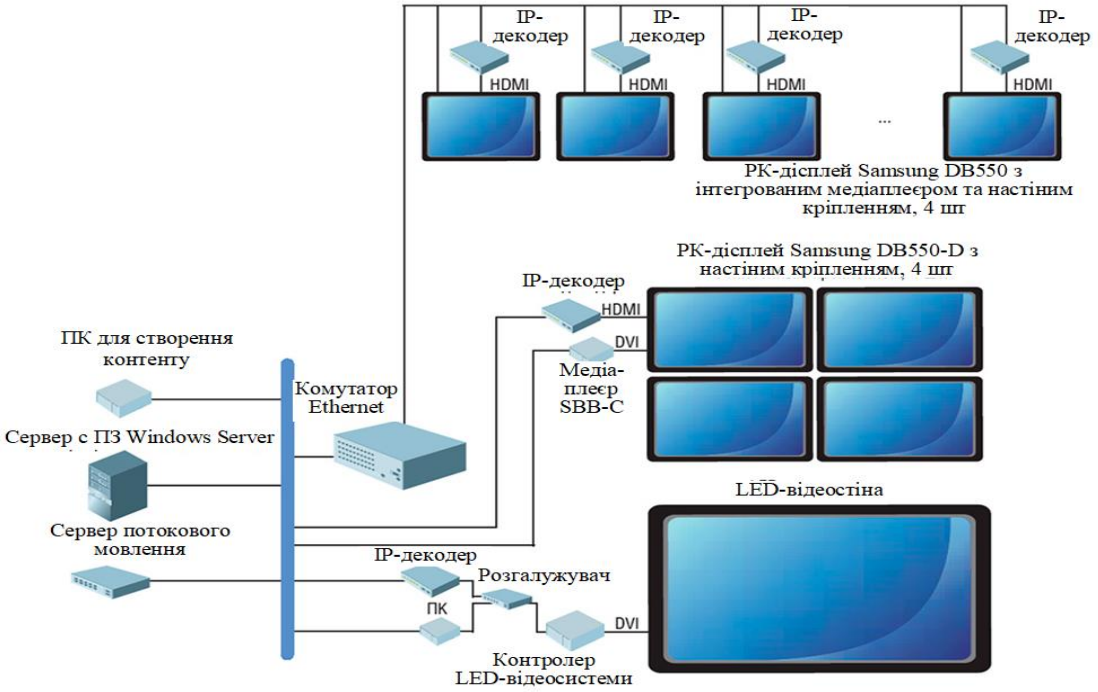


Рисунок 1 – Структурна схема системи

Для керування мережею встановлюється сервер. Він може бути розташований у довільному місці, на ньому збирається й організується новий контент.

Поточний контент зберігається й відтворюється з медіаплеєрів, зовнішніх і інтегрованих.

У нинішній час головне питання для замовника – вартість рішення. Отже, найдорожчий елемент – зовнішня LED-стіна, вона обійдеться замовникові майже в 7,5 млн гривень.

Видимо, це той самий компонент рішення, яким в умовах обмеженості бюджету можна буде пожертвувати.

Вартість 25 дисплеїв Samsung DB55D з інтегрованим медіаплеєром – 3,25 млн гривень, а відеостіни із чотирьох дисплеїв Samsung UD55C-B – близько 1,5 млн гривень.

Помітимо, що інший варіант організації відеостіни – на основі дисплеїв Planar Matrix – приблизно в п'ять разів дорожче.

25 ліцензій на плеєри Magicinfo Player збільшують витрати замовника ще приблизно на 573 тис. гривень, а необхідні для організації ТБ-віщання сервер Avercaster і 27 IP-декодерів – ще приблизно на 300 тис. гривень. Разом, вартість проекту (без зовнішньої LED-стіни) виходить близько 5,6 млн гривень.

Наскільки швидко окупляться ці вкладення? У цьому випадку окупність перебуває поза зоною відповідальності інтегратора.

Наше завдання – надати інструмент. Як саме й з якою ефективністю він буде використовуватися замовником, ми, на жаль, пророчити не можемо. Замовник повинен розуміти й усвідомлювати, що для ефективного керування подібною системою, зокрема одержання прибутку від розміщення реклами, необхідні співробітники з навичками роботи в області медіа: його позиціонування, продажі й розміщення.

Замовник може взяти таких фахівців у власний штат або скористатися послугами професійних медіаагентств.

Висновок. У статті розглянуто та проаналізовано програмне забезпечення, яке призначено для операційної системи екранів Digital Signage що обертаються, з синхронізованим відеопотоком. В межах України в недостатній мірі представлені вітчизняні розробки в цій області. У роботі наведені теоретичне узагальнення й рішення наукового завдання дослідження методів екранів Digital Signage що обертаються, з синхронізованим

відеопотоком. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем екранів Digital Signage що обертаються, з синхронізованим відео потоком; Досліджена система екранів Digital Signage що обертаються, з синхронізованим відео потоком; На основі отриманих результатів досліджень створена програмна реалізація системи екранів Digital Signage що обертаються, з синхронізованим відеопотоком. Розроблені під час виконання роботи алгоритми дозволяють успішно вирішувати завдання екранів Digital Signage що обертаються, з синхронізованим відеопотоком. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки. Розроблене програмне забезпечення має простий, дружній та зручний інтерфейс користувача, що забезпечує легкість у освоєнні роботи програмного продукту, зручність у використанні, і не потребує особливих спеціальних знань. При створені програмного забезпечення було використано об'єктно-орієнтований підхід, що відповідає сучасним тенденціям у галузі розробки комерційних програмних систем. Програма реалізована на мові високого рівня Delphi 10.2. Дана мова програмування дозволяє найбільш ефективно обробляти дані. Це дозволило мінімізувати строк розробки програмного забезпечення, і, як слід, зменшити витрати на його розробку. Запропоноване програмне забезпечення ділиться на загальне програмне забезпечення, що поставляється із засобами обчислювальної техніки й спеціальне програмне забезпечення, що спеціально розроблене для даної конкретної системи й включає програми, що реалізують її функції. Для підвищення рівня безпеки запропоновано застосовувати алгоритм AES.

Список літератури

1. Дреев А.Н. Использование неравномерного распределения единичных битов для дополнительного сжатия SPIHT кода / А.Н. Дреев, А.А. Смирнов// Информационные системы в управлении, образовании, промышленности: монография. Под редакцией профессора В.С. Пономаренко. – Х.: Вид-во ТОВ «Щедра садиба плюс», 2014. – 498 с.
2. Дрєєв О.М. Дослідження впливу шляху розгортки на ступінь ентропійного стиснення цифрового зображення / О.М. Дрєєв, О.В. Слюсар // Збірник наукових праць Кіровоградського національного технічного університету. Техніка в сільськогосподарському виробництві, галузеве машинобудування, автоматизація. Випуск 21. – Кіровоград: КНТУ. – 2008 – С. 115-118
3. Дрєєв О.М. Метод розвантаження телекомунікаційного сервера за рахунок кешування зображень / О.М. Дрєєв // Збірник наукових праць Кіровоградського національного технічного університету. Техніка в сільськогосподарському виробництві, галузеве машинобудування, автоматизація. Випуск 25. Частина І. – Кіровоград: КНТУ. – 2012 – С. 419-424
4. Дрєєв О.М. Метод прогнозування завантаженості серверу телекомунікаційної мережі / О.М. Дрєєв, О.А. Смірнов, Є.В. Мелешко, О.В. Коваленко // Системи обробки інформації. Випуск 3(101) Том 2. – Х.: ХУПС. – 2012. – С. 181-188
5. Дрєєв О.М. Оцінка якості стиснення зображень на основі дискретного перетворення Хартлі / О.В. Коваленко, О.П. Доренський, О.М. Дрєєв // Системи озброєння і військова техніка. Науковий журнал 2(34) – Х.: ХУПС – 2013. С. 99-102.
6. Дрєєв О.М. Дослідження впливу ступеня стиснення зображень на оперативність їх доставки у телекомунікаційній системі / О.А. Смірнов, О.М. Дрєєв, О.П. Доренський // Збірник наукових праць "Системи обробки інформації". – Випуск 8(115). – Х.: ХУПС – 2013. – С. 234-239.
7. Дреев А.Н. Сравнение битовых плотностей при использовании различных методов кодирования информации / А.Н. Дреев, А.А. Смирнов // Системи обробки інформації, 2014, випуск 2(118), том 2 – Харків: ХУПС – 2014. С 64-66.
8. Дрєєв О.М. Моделювання впливу інтенсивності трафіку на оперативність доставляння інформації / О.М. Дрєєв // Науково-виробничій журнал "Зв'язок". – Київ: ДУТ, 2014. – № 2 (108) С. 24-29.
9. Дреев А.Н. Повышение вероятности доставки сообщений в телекоммуникационных системах и сетях для обеспечения информационной безопасности / А.Н. Дреев, А.А. Смирнов //«Безпека інформації» Том 21, №1 2015 р. – Київ: НАУ – 2015. – С. 22-28.
10. Dreyev A.N. Block Mathematical Coding Method of Images Compressed by a SPIHT Algorithm / A.N. Dreyev, A.A. Smirnov // International Journal of Computational Engineering Research (IJCER). – Volume 03, Issue 5. USA, Indiana, Riley: Science and Engineering Publishing Company. – May 2013 – P.34-39. ISSN: 2250-3005

УДК 004

С. Шимко, магістр гр. КІ-18М-1,4
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ АГРЕГАТОРА ДАНИХ ІНТЕРНЕТ-ПОРТАЛІВ

У статті розроблено програмне забезпечення, яке призначено для агрегатора даних інтернет-порталів. Метою розробки є дослідження та програмна реалізація агрегатора даних інтернет-порталів. Об'єктом дослідження є процес агрегації даних інтернет-порталів. Предметом дослідження є методи агрегації даних інтернет-порталів. Методи дослідження базуються на методах Big Data, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація агрегатора даних інтернет-порталів. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.
комп'ютерна інженерія, агрегатор даних, інтернет-портал

Постановка проблеми. Агрегатор даних – під цим терміном розуміють програму або сервіс, яка збирає інформацію в Інтернеті з новинних каналів, сайтів, форумів і блогів.

Новим явищем віртуального ефіру є портали, де максимально повно представлені відомості з певної тематики, які користувач може знайти сьогодні в Інтернеті.

Для отримання інформації з інтернет порталів використовуються RSS стрічки. RSS – це родина XML-форматів, що використовується для публікації та постачання інформації, що часто змінюється, наприклад, нових записів в блозі, заголовків новин, анонсів статей, зображень, аудіо і відео матеріалів (в стандартизованому форматі). Документ в стандарті RSS (який також інколи називають «стрічкою», «веб-стрічкою» або «каналом») складається з повного або часткового тексту і метаданих (дата і авторство).

Як правило за допомогою RSS дається короткий опис нової інформації, що з'явилася на сайті, і посилання на її повну версію.

Багато сучасних браузерів, поштових клієнтів і програм миттєвого обміну повідомленнями вміють працювати з RSS-стрічками. Крім того, існують спеціалізовані програми (агрегатори), що збирають і обробляють інформацію RSS-каналів. Також дуже популярні веб-агрегатори, що являють собою сайти для збирання та відображення RSS-каналів.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні агрегатора даних інтернет-порталів.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація агрегатора даних інтернет-порталів.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем агрегації даних інтернет-порталів.
– Дослідження агрегатора даних інтернет-порталів.
– Програмна реалізація агрегатора даних інтернет-порталів.

Об'єктом дослідження є процес агрегації даних інтернет-порталів.

Предметом дослідження є методи агрегації даних інтернет-порталів.

Методи дослідження базуються на методах Big Data, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Система Android надає різнобічну платформу застосунків, на основі якої можна створювати інноваційні програми та ігри для мобільних пристроїв в середовищі мови Java.

Застосунки для Android будуються з окремих компонентів, які можна викликати

незалежно один від одного. Наприклад, окрема операція надає один екран для користувача інтерфейсу, а служба незалежно виконує роботу у фоновому режимі.

За допомогою об'єкта Intent з одного компонента можна запустити інший компонент. Можна навіть запустити компонент з іншої програми, скажімо, операцію з картографічного додатка, щоб показати адресу. Ця модель формує кілька точок входу для однієї програми, і при цьому користувач може вибрати будь-який застосунок для виконання за замовчуванням тієї або іншої дії, яке можуть викликати інші застосунки.

Android надає адаптивну платформу застосунків, яка дозволяє забезпечувати унікальні ресурси для різних конфігурацій пристроїв. Наприклад, можна створити різні файли XML макета для екранів різних розмірів, а система буде визначати, який макет використовувати, з урахуванням розміру екрану даного пристрою.

Якщо будь-яким функцій програми потрібен певний обладнання, наприклад камера, можна запитувати його наявність в пристрої під час виконання. При необхідності також можна оголошувати функції, які потрібні додатком, з тим щоб такі магазини застосунків, як Google Play, не дозволяли встановлювати застосунки на пристроях, в яких цієї функції немає.

Android призначений для роботи на безлічі різних типів пристроїв, від телефонів до планшета та телевізорів. Діапазон пристроїв забезпечує величезну потенційну аудиторію для додатка. Щоб застосунок був успішним на всіх цих пристроях, він повинен терпіти деякі варіанти функцій і забезпечити гнучкий користувальницький інтерфейс, який адаптується до різних конфігурацій екрана.

Щоб полегшити зусилля для досягнення цієї мети, Android забезпечує динамічну структуру застосунків, в якій можна надавати ресурси застосунків для конфігурації в статичних файлах (наприклад, різні макети XML для різних розмірів екрана). Тоді Android завантажує відповідні ресурси на основі поточної конфігурації пристрою. Тому з деякою передбачливістю до дизайну додатка та деякими додатковими ресурсами можна опублікувати єдиний пакет програм (APK), який забезпечує оптимізований користувацький досвід на різних пристроях.

Однак, за потреби, можна вказати вимоги до функцій додатка та контролювати, які типи пристроїв можуть встановлювати застосунок у магазині Google Play.

Оскільки Android – це проект з відкритим кодом, будь-який виробник обладнання може створити пристрій, на якому запущена операційна система Android. Тим не менш, пристрій "Android-сумісний", лише якщо він може правильно запускати застосунки, написані для середовища виконання Android. Точні дані про середовище виконання Android визначаються програмою сумісності Android, і кожен пристрій повинен пройти тестовий пакет сумісності (CTS), щоб він вважався сумісним.

Розробнику застосунків не потрібно турбуватися, чи сумісний пристрій з Android, тому що лише пристрої, сумісні з ОС Android, включають Google Play Store. Тому користувачі, які встановлюють застосунок у магазині Google Play, використовують сумісний з Android пристрій.

Однак потрібно враховувати, чи сумісний застосунок із кожною конфігурацією пристрою. Оскільки Android працює в широкому діапазоні налаштувань пристрою, деякі функції недоступні на всіх пристроях. Наприклад, деякі пристрої можуть не включати датчик компаса. Якщо для основної функціональності додатка потрібно використовувати датчик компаса, тоді застосунок сумісний лише з пристроями, що містять датчик компаса.

Щоб мати змогу керувати наявністю додатка на основі функцій пристрою, Android визначає ідентифікатори функцій для будь-якої функції програмного забезпечення, яка може бути недоступною на всіх пристроях. Наприклад, ідентифікатор функції для датчика компаса – FEATURE_SENSOR_COMPASS, а ідентифікатор для віджетів додатка – FEATURE_APP_WIDGETS.

У разі потреби можна заборонити користувачам встановлювати застосунок, якщо їхні пристрої не надають певну функцію, оголосивши його елементом <uses-feature> у файлі маніфесту вашого додатка.

Наприклад, якщо застосунок не має сенсу на пристрої, який не має сенсора компаса, можна оголосити датчик компаса, якщо це потрібно, за допомогою тегу маніфесту.

Google Play порівнює функції, які потрібні застосунку, до функцій, доступних на кожному пристрої користувача, щоб визначити, чи є застосунок сумісним з кожним пристроєм. Якщо пристрій не надає всіх функцій, потрібних для додатка, користувач не може встановити застосунок.

Проте якщо основна функціональність додатка не вимагає функції пристрою, слід встановити необхідний атрибут "false" та перевірити наявність функції пристрою під час виконання.

Різні пристрої можуть запускати різні версії платформи Android, такі як Android 4.0 або Android 4.4. Кожна наступна версія платформи часто додає нові API, недоступні в попередній версії. Щоб вказати, який набір API доступний, кожна версія платформи визначає рівень API. Наприклад, Android 1.0 – це API-рівень 1, а Android 4.4 – 19 рівні API.

Рівень API дозволяє оголосити мінімальну версію сумісності вашого додатка, використовуючи тег маніфесту <uses-sdk> та його атрибут minSdkVersion. Наприклад, у Android 4.0 (API-рівень 14) додано API-провайдер календаря. Якщо застосунок не може працювати без цих API, необхідно оголосити API-рівень 14 як мінімальну підтримувану версію додатка.

Атрибут minSdkVersion оголошує мінімальну версію, з якою ваш застосунок сумісний, а атрибут targetSdkVersion оголошує найвищу версію, на якій оптимізовано застосунок.

Однак, атрибути в елементі <uses-sdk> перевизначаються відповідними властивостями у файлі build.gradle. Отже, при використанні Android Studio, необхідно вказати там значення minSdkVersion і targetSdkVersion

Обов'язково необхідно експортувати з коду ресурси програми, такі як зображення і рядки, для подальшої їх незалежної обробки. Слід також забезпечити альтернативні ресурси для певних конфігурацій пристроїв, групуючи їх в каталогах ресурсів зі спеціальними іменами. У режимі виконання Android використовує відповідні ресурси з урахуванням поточної конфігурації. Наприклад, можна надавати інший макет призначеного для користувача інтерфейсу в залежності від розміру екрана або різні рядки в залежності від налаштування мови.

Після виконання експорту ресурсів програми можна звертатися до них за допомогою ідентифікаторів ресурсів, які генеруються в класі R вашого проекту.

Для того щоб застосунок підтримував кілька конфігурацій пристроїв, дуже важливо завжди надавати ресурси за замовчуванням для кожного типу ресурсів, використовуваних додатком.

Наприклад, якщо застосунок підтримує кілька мов, завжди необхідно включити каталог values / (в якому збережені рядки) без кваліфікатора мови і регіону. Якщо замість цього помістити всі файли рядків в каталоги з кваліфікаторів мови і регіону, застосунок закриється з помилкою при запуску на пристрої, на якому встановлена мова, відсутня в ваших рядках. Але як тільки ви надали ресурси values / за замовчуванням, застосунок буде працювати правильно (навіть якщо користувач не розуміє цієї мови, це краще, ніж завершення з помилкою).

Таким же чином, якщо надавати різні ресурси макета в залежності від орієнтації екрану, слід вказати одну орієнтацію в якості орієнтації за замовчуванням. Наприклад, замість надання ресурсів макета в каталозі layout-land / для альбомної орієнтації і в каталозі layout-port / для портретів, залишити один варіант за замовчуванням: наприклад, layout / для альбомної і layout-port / для портретів.

В Android 5.0 реалізована концепція Material Design. Розширений набір інструментів в інтерфейсі дозволяє с легкістю використовувати нові можливості в додатках.

Новий 3D-режим дозволяє додати глибину (вісь z), щоб підняти об'єкти над площиною і створити реалістичні тіні навіть при русі.

Вбудовані переходи дій забезпечують безперервний рух, як в анімації. Тема Material додає в дії переходи, в тому числі можливість використовувати загальні візуальні елементи в різних діях.

Для кнопок, прапорців та інших елементів управління в застосунку можна створити пульсуючу анімацію.

Також можна визначати векторні області малювання в XML і по-різному їх анімувати. Векторні області масштабуються без втрати дозволу, тому вони ідеально підходять для одноколірних значків в додатках.

Новий системний потік обробки RenderThread забезпечує плавність анімації навіть при затримках в основному потоці інтерфейсу.

Android 5.0 відрізняється більш швидкими та ефективними обчисленнями з плавним інтерфейсом.

Android працює виключно на базі нової середовища виконання ART, створеної спеціально для підтримки попередньої компіляції (AOT), динамічної компіляції (JIT) і інтерпретується коду. Це середовище підтримується архітектурою ARM, x86 і MIPS. Крім того, вона повністю сумісна з 64-розрядними системами.

ART покращує ефективність застосунків і підвищує швидкість їх роботи. Оптимізована очищення пам'яті скорочує кількість і тривалість пауз між подіями, так що програма не пропускає кадри. Крім того, ART динамічно коригує використання пам'яті, щоб основні процеси протікали більш ефективно.

Android 5.0 підтримує 64-розрядні архітектури, які використовуються в NVIDIA Tegra K1 для Nexus 9. Оптимізація розширює простір адрес і підвищує ефективність певних обчислень. Програми, написані на мові Java, автоматично діють як 64-розрядні. Ніяких модифікацій не потрібно. Якщо в застосунку використовується власний код, NDK буде підтримувати нові ABI для ARM v8, x86-64 і MIPS-64.

В Android 5.0 також поліпшена синхронізація аудіо і відео. Канали аудіо і відео передають більш точні часові мітки. Завдяки цьому поліпшується якість роботи ігрових і відеозастосунків.

Нові API спеціальних можливостей дозволяють отримувати докладні відомості про вікна на екрані, з якими можуть взаємодіяти користувачі. Також можна задати стандарти або певні дії для елементів інтерфейсу.

API для редакторів способів введення забезпечують швидке переключення між доступними способами.

Майже кожен застосунок має надавати альтернативні ресурси, щоб підтримувати певні конфігурації пристроїв. Наприклад, необхідно включити альтернативні графічні ресурси для екранів з різною щільністю растру і альтернативні ресурси для різних мов. У режимі виконання Android визначає конфігурацію пристрою і завантажує відповідні ресурси для застосунків.

Кваліфікатор hdpi вказує, що ресурси в цьому каталозі призначені для пристроїв, оснащених екраном високої щільності. Зображення в кожному з цих каталогів для графічних об'єктів мають розмір для певної щільності екрану, але імена файлів повністю збігаються. Таким чином, ідентифікатор ресурсу, який вказує на зображення icon.png або background.png, завжди однаковий, але Android вибирає версію кожного ресурсу, яка оптимально відповідає поточному пристрою, порівнюючи інформацію про конфігурацію пристрою з кваліфікатором в імені каталогу ресурсів.

При виборі ресурсів на основі кваліфікаторів розміру екрана система буде використовувати ресурси призначені для екрану, меншого ніж поточний екран, якщо немає більш підходящих ресурсів (наприклад, на екранах великого розміру при необхідності будуть використовуватися ресурси, призначені для екранів нормального розміру). Однак, якщо єдині доступні ресурси перевершують розмір поточного екрану, система не буде використовувати ці ресурси, і застосунок аварійно завершиться, якщо немає інших ресурсів, відповідних конфігурації пристрою (наприклад, якщо всі ресурси макета відзначені

кваліфікатором xlarge, але пристрій оснащений екраном нормального розміру).

Весь набір функцій ОС Android доступний за допомогою API, написаних на мові Java. Ці API являють собою будівельні блоки, необхідні для створення застосунків для Android, шляхом спрощення повторного використання основних, модульних компонентів системи та служб, до яких належать наступні:

– багата та розширювана система перегляду, яку можна використовувати для створення інтерфейсу додатка, включаючи списки, сітки, текстові поля, кнопки та навіть вставлений веб-браузер;

– менеджер ресурсів, що забезпечує доступ до ресурсів без кодів, таких як локалізовані рядки, графічні файли та макети;

– менеджер сповіщень, який дозволяє всім програмам відображати власні сповіщення в рядку стану;

– менеджер дій, який керує життєвим циклом застосунків і забезпечує загальний стек навигації назад;

– постачальники вмісту, які дозволяють додаткам отримувати доступ до даних з інших програм, таких як програма "Контакти", або для обміну власними даними.

Розробники мають повний доступ до тих самих базових API, які використовують системні застосунки Android.

Апаратний абстрактний рівень (HAL) забезпечує стандартні інтерфейси, які виявляють можливості апаратного забезпечення апаратного забезпечення на рівні Java API. HAL складається з декількох бібліотечних модулів, кожен з яких реалізує інтерфейс для певного типу апаратного компонента, такого як камера або модуль Bluetooth. Коли API-структура здійснює виклик для доступу до апаратного забезпечення пристрою, система Android завантажує модуль бібліотеки для цього апаратного компонента.

Для пристроїв з ОС Android версії 5.0 (API-рівень 21) або новішої версії кожна програма працює в своєму власному процесі та має власний приклад роботи Android Runtime (ART). АРТ написаний для запуску декількох віртуальних машин на пристроях з малою пам'яттю, виконуючи файли DEX, формат байт-коду, розроблений спеціально для Android, оптимізований для мінімального відстані пам'яті. Побудовані інструментальні ланцюжки, такі як Jack, складають джерела Java у байт-код DEX, який може працювати на платформі Android.

Переваги використання ART:

– швидший запуск і виконання застосунків;

– швидке перемикання між застосунками;

– більше вільної оперативної пам'яті.

Недоліки використання ART:

– збільшується час установки програми;

– збільшується займане місце у внутрішній пам'яті пристрою

Розробка структурної схеми

Розглянемо структурну схему системи, що представлено на рисунку 1.

На цій схемі ми бачимо, що програма зв’язується з парсером xml документів та адаптером, які формують отриману інформацію.

Дані за допомогою адаптеру передаються RecyclerView, з якого інформація виводиться на відео карту і відповідно на екран.

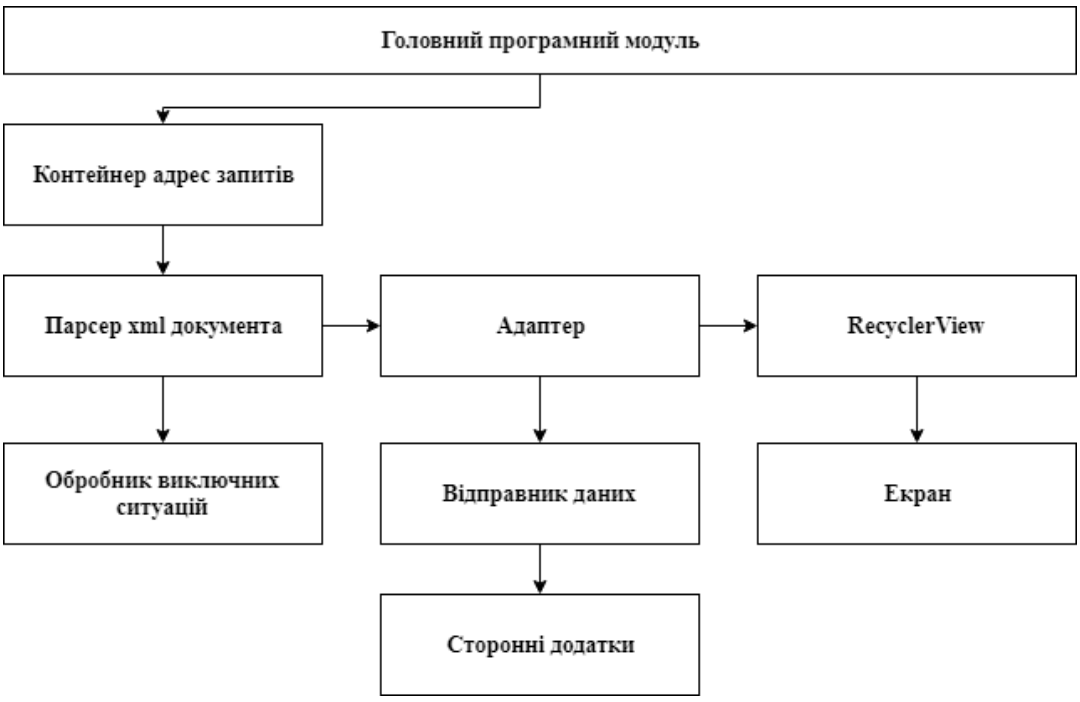


Рисунок 1 – Структурна схема системи

Висновок. У статті розглянуто та проаналізовано програмне забезпечення, яке призначено для агрегатора даних інтернет-порталів. В межах України в недостатній мірі представлені вітчизняні розробки в цій області. У роботі наведені теоретичне узагальнення й рішення наукового завдання дослідження методів агрегації даних інтернет-порталів. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем агрегації даних інтернет-порталів; Досліджена система агрегації даних інтернет-порталів; На основі отриманих результатів досліджень створена програмна реалізація агрегатора даних інтернет-порталів. Розроблені під час виконання роботи алгоритми дозволяють успішно вирішувати завдання агрегації даних інтернет-порталів. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки. Розроблене програмне забезпечення має простий, дружній та зручний інтерфейс користувача, що забезпечує легкість у освоєнні роботи програмного продукту, зручність у використанні, і не потребує особливих спеціальних знань. При створені програмного забезпечення було використано об’єктно-орієнтований підхід, що відповідає сучасним тенденціям у галузі розробки комерційних програмних систем. Програма реалізована на мові високого рівня Java. Дана мова програмування дозволяє найбільш ефективно обробляти дані. Це дозволило мінімізувати строк розробки програмного забезпечення, і, як слід, зменшити витрати на його розробку. Запропоноване програмне забезпечення ділиться на загальне програмне забезпечення, що поставляється із засобами обчислювальної техніки й спеціальне програмне забезпечення, що спеціально розроблене для даної конкретної системи й включає програми, що реалізують її функції. Програма призначена для виконання під управлінням багатозадачної операційної системи Android. Даються необхідні рекомендації з установки розробленого програмного забезпечення. Для підвищення рівня безпеки запропоновано застосовувати алгоритм Blowfish.

Список літератури

1. Мелешко Е.В. Математическая модель подсистемы управления и обслуживания в многопротокольном узле связи / Е.В.Мелешко // Збірник наукових праць Харківського університету повітряних сил.– Х.: ХУПС. – 2010. – Вип. 4 (26). – С. 124-128.

2. Мелешко Е.В. Методы идентификации трафика и динамического управления очередями в многопротокольных узлах связи и оценка их эффективности / Е.В.Мелешко // Системи обробки інформації. – Х.: ХУПС. – 2010. – Вип. 8 (89). – С. 68-74.
3. Мелешко Е.В. Усовершенствование математической модели подсистемы управления трафиком в узле телекоммуникационной сети / Е.В.Мелешко // Збірник тез та доповідей третьої науково-технічної конференції студентів та аспірантів «Захист інформації з обмеженим доступом та автоматизація її обробки (RISAP-2011)». Тези доповідей. Київ: НАУ, 2011. – 6 с.
4. Назаров А.Н. АТМ: Технология высокоскоростных сетей / А.Н. Назаров, М.В. Симонов. – М.: Эко-Трендз, 1997. – 232 с.
5. Назаров А.Н. Модели и методы расчета структурно-сетевых параметров АТМ сетей / Алексей Николаевич Назаров. – М.: Горячая линия – Телеком, 2002. – 256 с.
6. Новиков Ю.В. Локальные сети: архитектура, алгоритмы, проектирование / Ю.В. Новиков, С.В. Кондратенко – М.: ЭКОМ, 2000. – 312 с.
7. Одом Ш. Коммутаторы CISCO / Ш. Одом, Х. Ноттингем – М.:"Кудиц-Образ", 2003. – 528 с.
8. Олифер В.Г. Компьютерные сети. Принципы, технологии, протоколы: учебник для вузов / В.Г. Олифер, Н.А. Олифер. –2-е изд. – СПб.: Питер, 2007. – 958 с.
9. Пантелеев А.В. Т.А. Методы оптимизации в примерах и задачах / А.В. Пантелеев, Т.А. Летова. – М.: Высшая школа, 2002. – 544 с.
10. Руководство по технологиям объединенных сетей. 4-е изд. / пер.с англ. и ред. А.Н. Крикуна – М.: Изд. дом «Вильямс», 2005. – 1040 с.

УДК 633.152:631

Д. Шкляренко, магістр гр. АГ-18М-1,9
Л. Сало, канд. с.-г. наук, доц.
Центральноукраїнський національний технічний університет

ВИВЧЕННЯ ХАРАКТЕРУ ФОРМУВАННЯ ВРОЖАЙНОСТІ ГІБРИДІВ КУКУРУДЗИ В УМОВАХ ФРАНЦІЇ (ЗА РЕЗУЛЬТАТАМИ ЗАКОРДОННОГО СТАЖУВАННЯ)

Вступ. Найважливішим чинником сучасної технології вирощування й отримання високих врожаїв зерна кукурудзи є використання для сівби високоякісного гібридного насіння. В цьому контексті визначальним критерієм одержання високих врожаїв зерна кукурудзи при дотриманні і чіткому та своєчасному виконанні регламенту агротехнології є добір гібридів кукурудзи різних груп стиглості з високим потенціалом врожайності та підвищеною адаптивністю до несприятливих абіотичних факторів певної зони агровиробництва [1, 2].

Досвід розвинених країн є доречним для добору найкращих гібридів для вирощування в Україні. Сьогодні Франція є найголовнішим експортером насіння кукурудзи в світі. У Франції вирощується близько 2100 тис. гібридів кукурудзи, які призначені як для французького ринку, так і для ринку Західної і Східної Європи. Щорічно у Франції виробляють 14 млн. посівних одиниць, з яких 8% експортується в інші країни за межами ЄС, в тому числі в Україну [3].

Завдяки міжнародним програмам стажувань для студентів, які ефективно функціонують в ЦНТУ, Шкляренко Д.С. протягом 2017-2018 років проходив стажування в компанії “Euralis Semens”, де ознайомився з методами їх роботи, вивчав технології вирощування гібридів кукурудзи та приймав участь у дослідженнях компанії по вивченню характеристик гібридів кукурудзи та особливостей формування їх врожайності.

Мета досліджень: встановити оптимальні гібриди кукурудзи з максимальною врожайністю зерна для подальшого вирощування їх в умовах Кіровоградського регіону.

Методика досліджень: дослідження формування врожайності зерна гібридів кукурудзи французької селекції в умовах одного з науково-селекційних центрів компанії Євраліс Семенс (Euralis Semences) на південному заході Франції поблизу м. Блуа.

Ґрунти, представлені в умовах проведення досліджень - карбонатні та бурі лісові типи.

Дослідження проводили шляхом закладання польового досліду. Досліджували гібриди кукурудзи ЕС Астероїд (контроль), ЕС Сіріус, ЕС Кроссман, ЕС Конкорд, ЕС Креатив, ЕС Фарадей, ЕС Москіто, ЕС Сенсор, ЕС Мілорд і ЕС Метод

Результати досліджень. Результати визначення врожайності зерна гібридів кукурудзи відображені в таблиці 1.

Як показали спостереження, врожайність зерна кукурудзи у 2017 році коливалась від 151,6 до 88,9 ц/га. Максимальний показник був у гібриду ЕС Сенсор, це вище за контроль на 29,9 ц/га або майже на 25%. Достовірна прибавка врожайності була також у гібридів ЕС Метод, ЕС Москіто, ЕС Конкорд і ЕС Креатив.

Таблиця 1. Рівень врожайності зерна гібридів кукурудзи у роки досліджень

Варіанти		2017 р.		2018 р.		Зниження врожайності	
		Врожайність	Різниця до контролю	Врожайність	Різниця до контролю		
№	Назва гібриду		ц/га		ц/га	ц/га	%
1	ЕС Астероїд (контроль)	121,7	-	101,9	-	19,8	16,3
2	ЕС Сіріус	115,2	-6,5	86,7	-15,2	28,5	24,7
3	ЕС Кросман	88,9	-32,8	80,2	-21,7	8,7	9,8
4	ЕС Конкорд	137,2	15,5	120,1	18,2	17,1	12,5
5	ЕС Креатив	136,4	14,7	109,4	7,5	27,0	19,9
6	ЕС Фарадей	95,8	-25,9	87,7	-14,2	8,1	8,5
7	ЕС Москіто	144,2	22,5	118,5	16,6	25,7	17,8
8	ЕС Сенсор	151,6	29,9	131,2	29,3	20,4	13,5
9	ЕС Мілорд	129,4	7,7	117,6	15,7	11,8	9,1
10	ЕС Метод	149,3	27,6	130,8	28,9	18,5	12,4
$НІР_{05}$		*13,6*		*12,7*			

Врожайність гібриду ЕС Мілорд була вищою за контроль на 7,7 ц/га, але при НІР 13,6 така прибавка вважається недоведеною.

Низький рівень врожайності був відмічений у гібридів ЕС Сіріус, ЕС Кроссман та ЕС Фарадей. У двох останніх гібридів зниження показника перевищувало 20% відносно контролю.

У 2018 році в зв'язку з менш сприятливими умовами погоди під час вегетації кукурудзи рівень врожайності був помітно меншим. Порівняно з попереднім роком досліджень зниження становило від 8,1 до 28,5 ц/га.

Найбільш врожайними серед гібридів були ЕС Сенсор і ЕС Метод, відповідно 131,2 та 130,8 ц/га.

Достовірну прибавку створили також гібриди ЕС Москіто і ЕС Конкорд. Гібрид ЕС Мілорд виявився досить пластичним до погодних умов і, на відміну від попереднього 2017 року, в даному році сформував достовірну прибавку.

А от гібрид ЕС Креатив був нестійким до несприятливих факторів вегетаційного періоду і в 2018 році його прибавка до контролю була неістотна - 7,5 ц/га при НІР 12,7. Традиційно низьким рівнем врожайності характеризувались гібриди ЕС Сіріус, ЕС Кроссман та ЕС Фарадей.

В середньому за 2 роки досліджень (Рис.1.) стабільно високою врожайністю характеризувались гібриди ЕС Сенсор (141,4 ц/га) та ЕС Метод (140,0 ц/га).

Врожайність, вищу за контрольний гібрид ЕС Астероїд, показали ЕС Москіто, ЕС Конкорд, ЕС Мілорд і ЕС Креатив. Гібриди ЕС Сіріус, ЕС Кроссман та ЕС Фарадей мали показники менші за контроль.

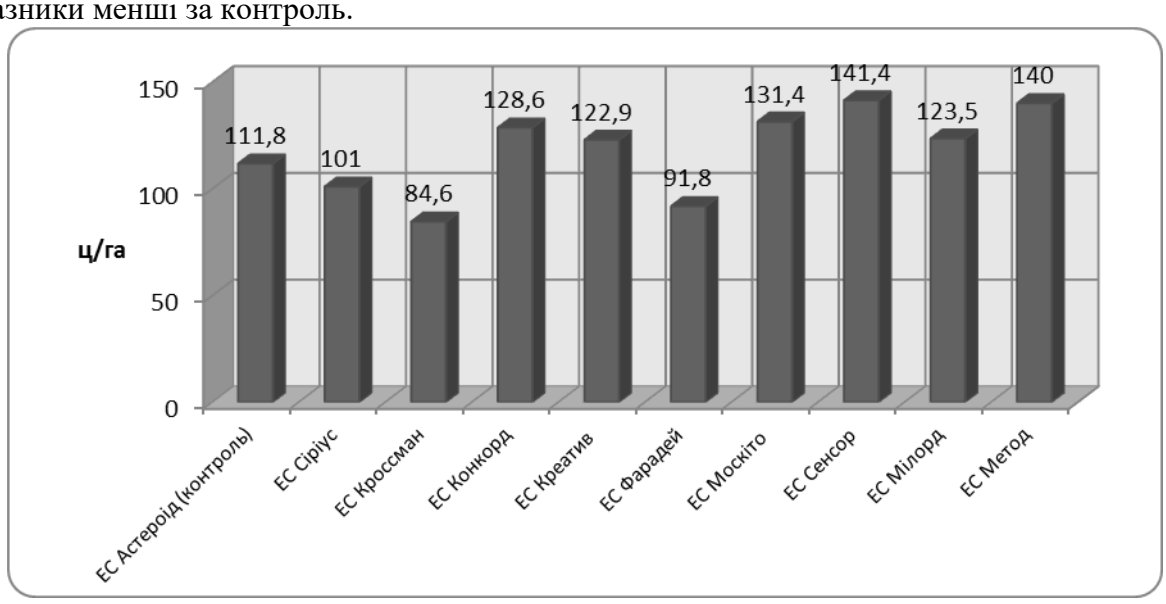


Рис.1. Середня за 2 роки врожайність зерна гібридів кукурудзи, ц/га

Тож, як висновок, можна виділити гібриди ЕС Сенсор та ЕС Метод за їх досить високу врожайність як в сприятливий рік, так і в рік коли кліматичні умови були посушливими, в середньому рівень їх врожайності був більшим за контроль на 29,6 та 28,2 ц/га.

Найменш чутливими були гібриди ЕС Кроссман та ЕС Фарадей, їх зниження склало 8,7 та 8,1 ц/га, але це пов’язано, очевидно з найменшим рівнем врожайності в досліді.

Показники структури врожаю є важливими в контексті відображення чинників формування врожайності культури. Серед досліджуваних показників слід відмітити масу 1000 зернівок та кількість сформованих зерен у качані кукурудзи (Рис.2 і 3).

Як показали наші спостереження, максимальна маса 1000 зерен була у гібридів з найвищим ФАО, це ЕС Мілорд і ЕС Метод. Відповідно 348,5 та 352,0 г. Перевищення показників контрольного гібриду було на рівні 18,0-21,5 г.

Досить вагомим зерном виділялися також гібриди УС Креатив та ЕС Сенсор -341,5-343,0 г. Це було вище за показники контрольного гібриду на 11,0-12,5 г.

На однаковому рівні були також гібриди ЕС Конкорд та ЕС Фарадей, від 320,0 до 324,5 г.

Найменші показники маси 1000 зернівок в середньому за два роки сформував гібрид ЕС Сіріус, його рівень не досягав 300 г і склав 293,5.

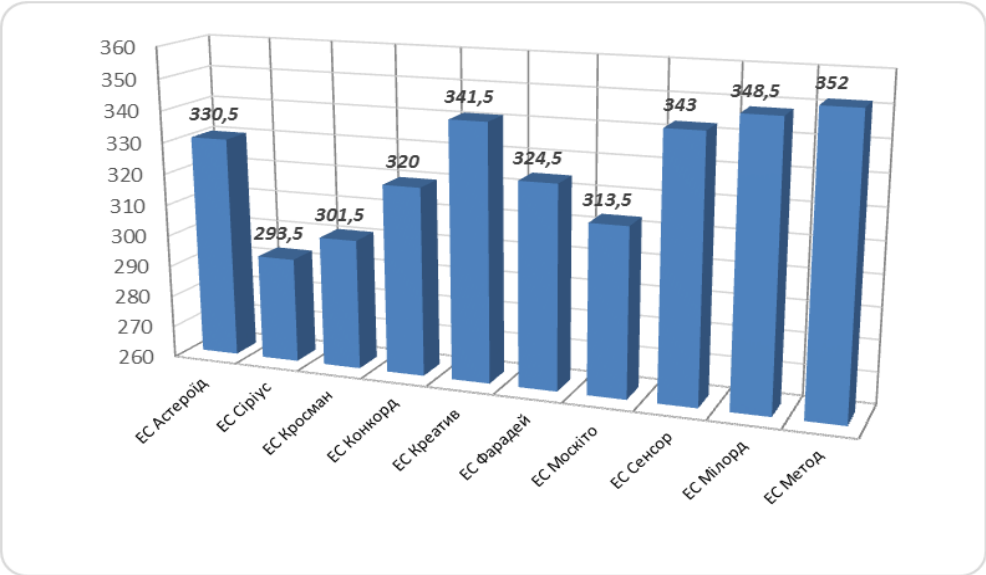


Рис.3.5. Середня за 2 роки маса 1000 зерен кукурудзи, г

На основі даного аналізу показників маси 1000 зернівок можна зробити висновок, що даний показник не залежить від групи стиглості і мало залежить від умов погоди. Основна характеристика – це біологічні особливості гібриду.

Середня кількість зерен в качані залежить як від кількості зерен в ряду, так і від кількості рядів. Як показав аналіз середніх за два роки даних на рисунку 3, кількість зерен в качанах контрольного гібриду становила 483,1 штук. Найменша кількість зерен в качані, як і найменша кількість зерен в ряду, сформувалась у гібриду ЕС Кроссман – лише 400,4 штук. Це менше за показники контрольного варіанту гібриду ЕС Астероїд на 82,7 зернівки.

Також близькими показниками 490,6 та 487,5 штук характеризувались гібриди ЕС Сіріус та ЕС Фарадей. Дані гібриди характеризувались також схожими показниками середньої кількості зерен в ряду. Дані показники були вищими за контроль лише на 7,5-4,4 штуки. Гібрид ЕС Мілорд явно покращив свої показники і був четвертим від найвищого рівня.

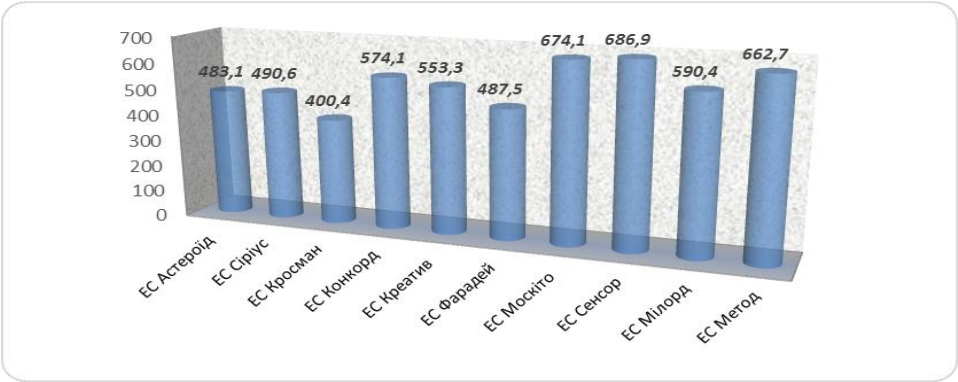


Рис.3. Середня за 2 роки кількість зерен у качані кукурудзи, шт.

А от гібрид ЕС Конкорд мав невисокі показники кількості зерен в качані, на відміну від кількості зерен в ряду. Це говорить про те, що качани у даного гібриду сформувались довгі, але з незначною кількістю рядів. Крім того, це пов’язано з біологією гібридів даної групи.

Те ж саме можна сказати про гібрид ЕС Креатив, який явно поступався даними показниками, відносно попередніх.

І, нарешті, три гібриди мали найбільше зерен у качані. Це ЕС Москіто, ЕС Сенсор та ЕС Метод, відповідно 674,1, 686,9 та 662,7 штук. Це майже на 30 % більше за показники контрольного гібриду ЕС Астероїд.

Тобто, можна стверджувати, що дані гібриди характеризувались найбільшими качанами.

Висновки: 1.Найбільш високоврожайними і найменш чутливими до умов погоди є гібриди ЕС Сенсор та ЕС Метод, які мали в обидва роки достовірну прибавку врожайності. 2.За кількісними характеристиками структури врожаю зерна кукурудзи кращим був гібрид ЕС Сенсор. 3.Максимальна маса 1000 зерен була у гібридів ЕС Мілорд і ЕС Метод. Даний показник не залежить від групи стиглості і мало залежить від умов погоди. Основна характеристика – це біологічні особливості гібриду. 4.Максимальна кількість зерна з качана була отримана у гібриду ЕС Сенсор.

Список літератури

1. Стратегічні напрями розвитку сільського господарства України на період до 2020 року / за ред. Ю.О. Лупенка, В.Я. Месель-Веселяка. – К.: ННЦ "ІАЕ", 2012. – 182 с.
2. Глушко Т.В. Вплив зрошення та мінеральних добрив на урожайність гібридів кукурудзи в умовах Південного Степу України / Т.В. Глушко // Зрошуване землеробство: зб. наук. праць. - Херсон: Айлант, 2012. - Вип. 57. - С.116-118.
3. Насіння кукурудзи в Україні родом із Франції [Електронний ресурс] – Режим доступу до ресурсу: http://milkua.info/uk/post/nasinna-kukurudzi-v-ukraini-rodom-iz-francii.

УДК 004

М. Янков, магістр гр. КІ-18М-1,4
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ ВКЗ ПОБУДОВАНОЇ НА БАЗІ ТЕРМІНАЛІВ YEALINK VC200

У статті розроблено програмне забезпечення, яке призначено для системи ВКЗ побудованої на базі терміналів Yealink VC200. Метою розробки є дослідження та програмна реалізація системи ВКЗ побудованої на базі терміналів Yealink VC200. Об'єктом дослідження є процес ВКЗ побудованої на базі терміналів Yealink VC200. Предметом дослідження є методи ВКЗ побудованої на базі терміналів Yealink VC200. Методи дослідження базуються на методах теорії кодування відеоданих, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи ВКЗ побудованої на базі терміналів Yealink VC200. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.
комп'ютерна інженерія, відео-конфернц-зв'язок, Yealink VC200

Постановка проблеми. Майже в кожної компанії виникає питання про оптимізацію бізнес-процесу, за допомогою сучасних технологій. Відеоконференцзв'язок не виключення; він дозволяє оптимізувати часові й грошові витрати підприємства й оперативно вирішувати питання з партнерами.

Що таке відеоконференцзв'язок, узагальнено зрозуміло з назви, але необхідно усвідомлювати, ВКЗ – це більше, ніж просто камери, комп'ютер і ПЗ – це встаткування й технології, які в сукупності дозволяють перевести віддалене спілкування на високий, якісний рівень, найчастіше досягаючи ефекту присутності.

Система професійної відеоконференцзв'язку містить у собі наступні елементи:

1.Якісна відеокамера з високою розв'язною здатністю. Під час розмови за допомогою популярного відеочату, найчастіше ви бачите картинку низької якості, з нерегульованою освітленістю. Професійна відеокамера з регулюванням світлочутливості й передачі кольору,

відтворює якісну, деталізовану картинку вашого співрозмовника. У підсумку, ви не відволікаєтеся від спілкування й сприймаєте співрозмовника так, нібито він перебуває на відстані витягнутої руки.

2.Конференц-системи (мікрофони). Конференц-системи мають високу чутливість, для забезпечення якісної мови під час переговорів, у відмінності від мікрофона на телефоні або комп'ютері. Більш докладно про мікрофони.

3.Акустичні системи. Звукове встаткування встановлюється винятково після інженерних акустичних розрахунків приміщення. У конференц-залах і переговірних кімнатах використовують різні види встаткування: стельова акустика, настінна, фронтальна. При використанні останнього виду акустики, буде виникати додатковий ефект присутності віддаленого учасника.

4.Акустичні дані приміщення. Цей пункт прямо пов'язаний з перерахованими вище; без гідної акустики приміщення, не можна домогтися звукового ефекту присутності. В основному редагується й формується за допомогою інтер’єрних матеріалів, під час ремонту.

5. Відеоустаткування. Маються на увазі системи відеовідображення співрозмовників (екрани, монітори, панелі). Передача візуального контенту найважливіше під час відеоконференції, якість устаткування грає тут найважливішу роль.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-16] було виявлено певні прогалини у забезпеченні системи ВКЗ побудованої на базі терміналів Yealink VC200.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи ВКЗ побудованої на базі терміналів Yealink VC200.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

- Огляд існуючих систем ВКЗ побудованої на базі терміналів Yealink VC200.
- Дослідження системи ВКЗ побудованої на базі терміналів Yealink VC200.
- Програмна реалізація системи ВКЗ побудованої на базі терміналів Yealink VC200.

Об’єктом дослідження є процес ВКЗ побудованої на базі терміналів Yealink VC200.

Предметом дослідження є методи ВКЗ побудованої на базі терміналів Yealink VC200.

Методи дослідження базуються на методах теорії кодування відеоданих, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Завдяки конструкції все в одному й бездротовій передачі відео, звуку й контенту VC200 значно спрощує розгортання й використання ВКЗ

Термінал відео-конференц-зв'язку Yealink VC200 призначений для оснащення невеликих переговірних кімнат. VC200 має конструкцію «усе в одному» – кодек з убудованою відеокамерою й мікрофонною панеллю. Він сумісний з рішеннями інших вендорів за протоколами SIP і H.323, а також із хмарними сервісами Zoom і BlueJeans. Відеоконференцію можна записувати на USB-накопичувач. Для передачі контенту на вибір пропонуються провідний (Yealink VCH50) або бездротової (Yealink WPP20) адаптери.

Керована відеокамера з функцією електронного (ePTZ) руху (нахил, поворот, зум) забезпечує чіткість зображення до 4K (4096×3072 пікселів). Мікрофонна панель із 6 мікрофонів дозволяє сформувати широкоугольну зону захвата голосу дальністю до 5 м, кутом до 150° і фокусуванням на мовець. Широкий кут захвата відеокамери (103°) і убудованої мікрофонної панелі (150°) дозволяють всім присутнім бути видимими й чутними віддаленими співрозмовниками й повноцінно брати участь у відеоконференції навіть у невеликому приміщенні.

Протокол H.265/HEVC реалізований на спеціалізованому процесорі, він ефективно стискає й обробляє відеозображення, забезпечуючи усталену роботу на нестабільних каналах зв'язку. Передача гладкого відео із чіткістю 1080p можливо при пропускній здатності каналу від 512 кбіт/с і захищена від втрат до 30% відеопакетів.

Бездротові технології передачі контенту, звуку й відео значно полегшують розгортання й використання встаткування. Крім того, базова комплектація передбачає 1 рік сервісу Yealink AMS (програма технічної підтримки).

Рисунок 1 – VC200 сполучимо з рішеннями інших вендорів за протоколами SIP і H.323, а також із хмарними сервісами Zoom і BlueJeans

VC200 поставляється у двох базових комплектаціях: із пристроєм бездротової передачі контенту WPP20 або ж без нього. Адаптер WPP20 підключається до ноутбука або персонального комп'ютера по USB і дозволяє ділитися контентом з екрана з усіма учасниками відеоконференції, не роблячи ніяких додаткових дій. При цьому, на відміну від інших терміналів Yealink, WiFi-модуль уже убудований в VC200, і для підключення адаптера не потрібно додатковий переходник.

Термінал відеоконференцзв’язку для невеликих переговірних кімнат. Керована відеокамера з функцією електронного (ePTZ) руху: нахил, поворот, зум. Чіткість відеозахвата до 4K (4096×3072 пікселів). Конструкція "усе в одному": кодек з убудованою відеокамерою й мікрофонним масивом з 6 мікрофонів, що формують широкоугольну зону захвата голосу дальністю до 5 метрів, кутом до 150° і спрямованістю на мовець. Сполучимо з рішеннями інших вендорів за протоколами SIP і H.323, а також із хмарними сервісами Zoom і BlueJeans. Підтримка запису відеоконференцій на USB-накопичувач. На вибір пропонуються адаптери для провідний Yealink VCH50 або бездротової Yealink WPP20 передачі контенту.

Широкий кут захвата відеокамери 103° і убудованої мікрофонної панелі 150° дозволяє всім присутнім, перебуваючи близько до екрана в невеликому приміщенні, бути видимим і чутними віддаленим співрозмовникам і повноцінно брати участь у відеоконференції.

H.265/HEVC протокол, реалізований на спеціалізованому процесорі, ефективно стискає й обробляє відеозображення, захищаючи від нестабільностей у каналах зв'язку. Передача відео чіткістю 1080p забезпечується в смузі пропущення від 512 кбіт/с і захищена від втрат до 30% відеопакетів.

Бездротові технології передачі контенту, звуку й відео значно полегшують розгортання й користування встаткуванням.

Характеристики

Системні компоненти:

- Моноблок VC200.
- Пульт ДУ VCR11.
- PoE-інжектор.

Камера:

- Камера 4K Ultra HD.
- Відеодозвіл Full HD (1920x1080 30 кадр/с).

– Zoom 4x (цифровий) ePTZ.
– Поле огляду по горизонталі 103°.

Розрішення відео:
– 1080p (1920x1080).
– 720p (1280x720).
– W448p (768x448).
– WQVGA (400x240).
– 4CIF (704x576).
– CIF (352x268).

Відеопротоколи й взаємодія з мережею:
– H.265/HEVC, H.264 High Profile, H.264, H.263.
– Динамічне адаптивне налаштування смуги пропущення.
– Пряма корекція помилок (FEC), захист від втрат до 30% відеопакетів.
– Автоматичний пріоритет забезпечення якості контенту й голосу.

Мікрофони:
– Убудований масив з 6 мікрофонів.
– Захват на відстані до 5 метрів.
– Кут захвата 150°.

Протоколи обробки звуку:
– Підтримка Opus (8-48 кгц).
– Підтримка G.722.1C (14 кГц).
– Підтримка G.722.1 (7 кГц).
– Підтримка G.711 (3.4 кГц).
– Придушення луни (AEC).
– Автоматичне регулювання чутливості мікрофона (AGC).
– Технологія захисту від фонового шуму (Yealink Noise Proof Technology).
– Генератор комфортного шуму (CNG).
– PLC, AJB, De-Rerb.

Операційна система:
– Android 7.1.

Функції:
– Підтримка відео 1080p30 + контент 1080p30.
– Підтримувані розкладки:
– Картинка в картинці
– Зображення учасника на весь екран.
– Запис аудіо й відео, відтворення.
– Запис знімків (скріншотів).
– DND, статистика викликів.
– Автовідповідь, відключення мікрофона й очікування виклику.
– Пароль віртуальної кімнати.
– Віртуальна клавіатура.
– Локальна книга: 500 контактів.
– LDAP.
– Історія викликів: всі/пропущені/прийняті/набрані.
– Організація 5-сторонньої аудіоконференції.

Підтримка комунікаційних протоколів:
– H.323 (1 аккаунт), SIP (1 аккаунт).
– H.239, BFCP.
– FECC: H.224/H.281, Sony VISCA і PELCO D/P.

– Протоколи H.323: H.245, H.225, H.235, H.241.

Сумісність із хмарними платформами:

– Yealink Cloud Management Service.
– Yealink Meeting Server.
– StarLeaf/UC OpenCloud, підтримка коду QCP.
– Mind/Pexip/Zoom/BlueJeans.

Мережа й безпека:

– Убудована підтримка Wi-Fi (2.4/5 ГГц).
– Убудована підтримка Bluetooth.
– TCP/IP (IPv4/IPv6), DHCP і статичний режим роботи з мережею.
– HTTP/HTTPS веб-сервер.
– RS232/HTTP API для інтеграції із системами керуваннями.
– TLS, AES-шифрування.
– SRTP.
– QoS: 802.1p/Q, Diff-serv.
– IEEE 802.1X, LLDP-MED, VLAN.
– Захист від атак.
– Мережна діагностика: Ping і Trace Route.
– Синхронізація часу й дати по SNTP.
– Убудований сертифікат.

NAT і міжмережевий екран:

– Конфігурування NAT (ручне й автоматичне).
– ICE/TURN/STUN.
– Інтелектуальне проходження NAT.
– OpenVPN.
– Підтримка H.460.

Керування:

– Налаштування через веб-інтерфейс/пульт ДУ/Autoprovision.
– Відновлення ПЗ, скидання налаштувань.
– Експорт і імпорт конфігураційних файлів.
– Експорт system log і PCAP Trace.

Інтерфейси:

– 1 x HDMI-вихід.
– 1 x RJ45 для конференц-телефону CP960 або комутаційного блоку VCH50.
– 1 x RJ45 Ethernet-порт 10/100 Мбит/с.
– Підтримка PoE (IEEE 802.3af).
– 2 x USB 2.0.
– 1 x Line-out (3.5 мм).
– Слот для замка Kensington.
– Кнопка скидання налаштувань.

Фізичні характеристики:

– Споживання: режим очікування <6.5 Вт, у робочому стані 7 Вт, макс. 8 Вт.

Розмір (Ш*Г*В):

– Кодек: 300*70*87 мм
– Пульт ДУ: 190*55*24 мм
– Робоча вологість: 10~95%.
– Робоча температура: 0~40^{o}C.

Комплектація

– Моноблок VC200 – 1 шт.

- PoE-інжектор YLPOE30 – 1 шт.
- Пульт ДУ VCR11 – 1 шт.
- AAA батарейки – 2 шт.
- HDMI-кабель (1.8 м) – 1 шт.
- Ethernet-кабель (3 м) – 1 шт.
- Гвинт – 1шт.
- Кабельні стяжки – 5 шт.
- Посібник користувача – 1 шт.
- Сервіс Yealink AMS – 1 рік.

Розробка структурної схеми

H.265 або **HEVC** (англ. High Efficiency Video Coding – високоефективне кодування відеозображень) – формат відеостиску із застосуванням більше ефективних алгоритмів у порівнянні з H.264/MPEG-4 AVC [1]. Рекомендація МККТТ H.265, а також стандарт ISO/IEC 23008-2 MPEG-H Частина 2, – спільна розробка експертної групи по відеокодуванню МККТТ (ITU-T Video Coding Experts Group – VCEG) і експертної групи по зображенню, що рухається, MPEG [2]. Рекомендація стандарту розроблена у зв'язку зі зростаючою потребою в більше високому ступені стиску зображень, що рухаються, для самих різних додатків, таких як потокова передача в інтернеті, передача даних, відеоконференцзв'язок, цифрові запам'ятовувальні пристрої й телевізійне віщання [3].

Підтримуються формати кадру до 8K (UHDTV) з дозволом 8192×4320 пікселів [4].

В 2004 році VCEG приступилася до дослідження розвитку технологій, які дозволили б створити новий стандарт стиску відео (або домогтися істотного поліпшення стандарту H.264/MPEG-4 AVC). У жовтні 2004 року зроблений огляд різних способів можливого вдосконалення H.264/MPEG-4 AVC [5].

Споконвічно передбачалося, що H.265 буде повністю новим стандартом, а не розширенням H.264 начебто HVC (High-performance Video Coding). У рамках проекту були привласнені попередні імена H.265 і H.NGVC (англ. Next-generation Video Coding – наступне покоління відеокодування), також існувала значна частина роботи VCEG до її еволюції в HEVC, спільний проект із MPEG в 2010 році. У квітні 2009 року проект одержав назву NGVC; у липні 2009 відбулася нарада MPEG і VCEG, на якому обговорювалася подальша спільна робота з NGVC і HVC.

Попередні вимоги до NGVC складаються в зменшенні бітрейта на 50 % при схожій суб'єктивній оцінці якості зображення й порівнянної з H.264 High profile обчислювальною складністю. Залежно від налаштувань передбачається варіювання обчислювальної складності від 1/2 до 3 у порівнянні з H.264 High profile, при цьому в першому випадку NGVC повинен забезпечувати на 25 % менший бітрейт [6].

ISO / IEC Moving Picture Experts Group (MPEG) почали аналогічний проект в 2007 році, попередньо названий Високопродуктивне відеокодування (High-performance Video Coding). У липні 2007 року було ухвалене рішення як мета проекту досягти зниження бітрейта на 50 % [7]. До липня 2009 року результати експерименту показали середнє зниження швидкості потоку приблизно на 20 % у порівнянні з AVC High Profile, ці результати спонукали MPEG почати стандартизацію в співробітництві з VCEG.

Для розробки стандарту MPEG і VCEG створили Об'єднану команду по відеокодуванню Joint Collaborative Team on Video Coding (JCT-VC) (ITU-T Rec H.264|ISO/IEC 14496-10) [8]. Перше засідання Об'єднаної команди по відеокодуванню (JCT-VC) відбулося у квітні 2010 року. Було представлено 27 повноцінних проектів. Оцінки показали, що деякі пропозиції можуть досягти такої ж якості зображення, як AVC, лише з половинним бітрейтом у багатьох випробуваннях, при 2— 10-кратному збільшенні обчислювальної складності, і в деяких проектах була досягнута гарна суб'єктивна якість і гарні результати швидкості передачі даних з більше низькою обчислювальною складністю, чим при референсном кодуванні AVC з високим профілем. На цій нараді була прийнята

назва для спільного проекту – високоефективне відеокодування High Efficiency Video Coding (HEVC) [9].

Комітет Проекту HEVC був затверджений у лютому 2012 року. У червні 2012 року MPEG LA оголосила про початок процесу прийняття спільних ліцензій на патенти HEVC. Проект міжнародного стандарту був затверджений у липні 2012 року на нараді, що відбулася в Стокгольмі. Fröjdh, голова шведської делегації MPEG, уважає, що комерційні продукти, які підтримують HEVC, можуть бути випущені в 2013 році [10].

29 лютого 2012 року на виставці Mobile World Congress компанія Qualcomm показала HEVC-декодер, що працює на планшеті під керуванням ОС Android із двоядерному процесором Qualcomm Snapdragon S4 із частотою 1,5 ГГц. Показувалися дві версії відеозапису з однаковим змістом, закодованими H.264/MPEG-4 AVC і HEVC. На цьому показі HEVC показав майже 50%-е зниження швидкості передачі в порівнянні з H.264/MPEG-4 AVC [11].

31 серпня 2012 Allegro DVT оголосила про випуск двох HEVC-віщальних кодерів: кодер AL1200 HD-SDI і IP-транскодер AL2200 [12]. Allegro DVT заявила, що апаратних декодерів HEVC не слід очікувати до 2014 року, але HEVC зможе застосовуватися й раніше в додатках із програмним декодуванням. На виставці IBC 2012 Allegro DVT показала HEVC-Системи потокового IP-віщання на основі IP-транскодера AL2200.

Ericsson у вересні 2012 року на виставці International Broadcasting Convention (IBC) представила перший у світі HEVC-кодер, Ericsson SVP 5500, що призначений для кодування відео в реальному часі для трансляції ефірного ТВ у мережах рухливого зв'язку [13].

У квітні 2013 року проект прийнятий як стандарт MCE-T [3].

На початок 2017 на апаратному рівні реалізована часткова підтримка стандарту HEVC всіма великими виробниками процесорів.

Як вимоги до стандарту запропоновано багато нових можливостей:

- Двовимірний нероздільний адаптивний інтерполяційний фільтр (AIF).
- Роздільний AIF.
- Спрямований AIF.
- Компенсація руху з точністю до 1/ 8-пікселя (Qpel).
- Адаптивне пророкування помилок кодування (APEC) у просторовій і частотній областях.
- Адаптивний вибір матриці квантування (AQMS).
- Заснована на порівнянні схема вибору й кодування вектора руху.
- Режимозалежне зміна налаштування внутрікадрового кодування.

Передбачається, що ці прийоми принесуть найбільшу користь при багатопроходному кодуванні [14].

Ефективність кодування

Розробка більшості стандартів відеокодування призначена, у першу чергу, для досягнення найбільшої ефективності кодування. Ефективність кодування визначається здатністю закодувати відео з мінімально можливим бітрейтом при збереженні певного рівня якості відео. Існує два стандартних способи виміру ефективності кодування відео, один із яких полягає у використанні об'єктивної метрики, такий як пікового відношення сигнал-шум (PSNR), а другий складається у використанні суб'єктивної оцінки якості відео. Суб'єктивна оцінка якості зображення є найбільш важливим параметром для оцінки кодування відео, тому що глядачі сприймають якість відео саме суб'єктивно.

Замість макроблоків, які застосовувалися в H.264, в HEVC використовуються блоки з деревоподібною структурою кодування. Виграш кодера HEVC – у застосуванні блоків більшого розміру. Це було показано в тестах PSNR з моделлю кодера HM-8.0, де рівнялися результати кодування з різними розмірами блоків. У результаті тестів було показано, що в порівнянні з кодуванням блоків розміром 64x64 пікселів бітрейт збільшується на 2,2 %, коли використовуються блоки розміром 32x32 і збільшується на 11,0 %, коли використовується

розмір блоків 16x16. У тестах кодування відео з дозволом 2560x1600 пікселів при використанні блоків з розміром 32x32 пікселів бітрейт збільшується на 5,7 %, а при використанні блоків розміром 16x16 пікселів – на 28,2 %, у порівнянні з відео, де використані блоки розміром 64x64, при однаковому піковому відношенні сигнал-шум. Тести показали, що застосування блоків більшого розміру більш ефективно при кодуванні відео з високою розв'язною здатністю. Тести також показали, що для декодування відео, закодованого з розмірами блоків 16x16, потрібно на 60 % більше часі, чим при використанні блоків 64x64. Тобто, застосування блоків більших розмірів підвищує ефективність кодування при одночасному скороченні часу декодування [15].

Було проведене порівняння ефективності кодування основного профілю H.265 з кодеками H.264/MPEG-4 AVC High Profile (HP), MPEG-4 Advanced Simple Profile (ASP), H.263 High Profile Latency (HLP) і H .262/MPEG-2 Main Profile (MP). Були закодовані відео розважальних програм і дев'ять тестових відеопослідовностей із дванадцятьома різними бітрейтами з використанням тестової моделі HEVC HM-8.0, п'ять із них були з HD-розрішенням, а чотири минулі з дозволом WVGA (800 × 480). Зменшення бітрейта визначалося на основі PSNR [15].

Структура кодера HEVC

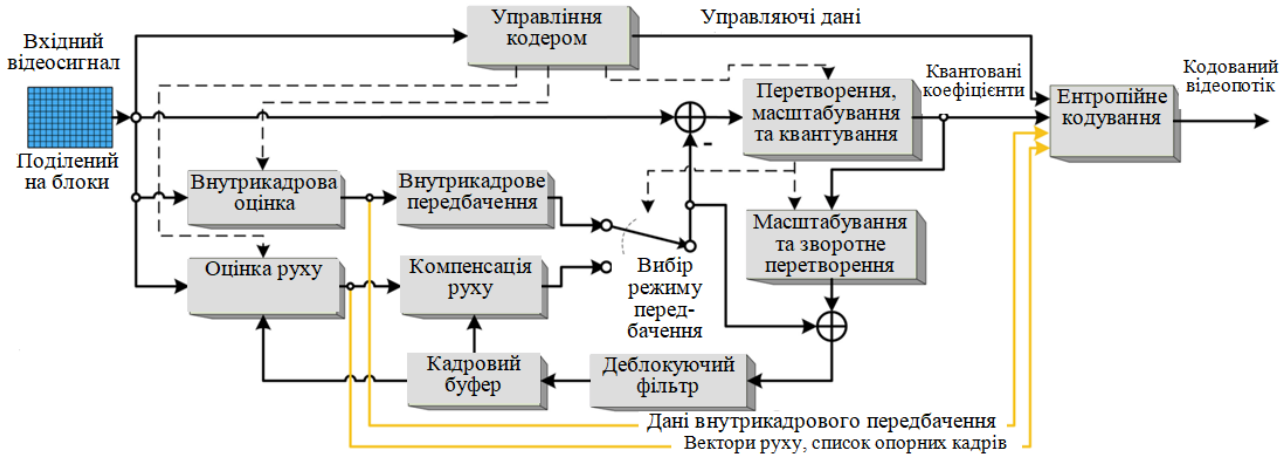


Рисунок 2 – Структурна схема системи

При кодуванні відео в HEVC застосовується такий же «гібридний» підхід, що й у всіх сучасних кодеках, починаючи з H.261. Він полягає в застосуванні усередині- і міжкадрового (Intra-/Inter-) пророкування й двовимірного кодування з перетворенням.

У кодері HEVC кожний відеокадр ділиться на блоки. Перший кадр відеопослідовності кодується з використанням тільки внутрікадрового пророкування, тобто застосовується просторове пророкування очікуваного рівня відліку усередині кадру по сусіднім відлікам, при цьому відсутня залежність від інших кадрів. Для більшості блоків всіх інших кадрів послідовності, як правило, використовується режим міжкадрового часового пророкування. У режимі міжкадрового пророкування на підставі даних про величину відліків опорного кадру й вектора рухи оцінюються поточні відліки кожного блоку. Кодер і декодер створюють ідентичні міжкадрові пророкування шляхом застосування алгоритму компенсації руху за допомогою векторів руху й даних обраного режиму, які передаються як додаткова інформація.

Різницевий сигнал пророкування, що являє собою різницю між опорним блоком кадру і його пророкуванням, піддається лінійному просторовому перетворенню. Потім коефіцієнти перетворення масштабуються, квантуються, застосовується ентропійне кодування, і потім передаються разом з інформацією пророкування.

Кодер у точності повторює цикл обробки декодером так, що в обох випадках будуть генеруватися ідентичні пророкування наступних даних. Таким чином, перетворені

квантовані коефіцієнти піддаються зворотному масштабуванню й потім зворотному перетворенню, щоб повторити декодоване значення різницевого сигналу. Різниця потім додається до пророкування, і отриманий результат фільтрується для згладжування артефактів, отриманих розподілом на блоки й при квантуванні. Остаточне подання кадру (ідентичне кадру на виході декодера) зберігається в буфері декодованих кадрів, що буде використовуватися для прогнозування наступних кадрів. У підсумку, порядок кодування й декодування обробки кадрів часто відрізняється від порядку, у якому вони надходять із джерела.

Передбачається, що відеоматеріал на вході кодера HEVC має прогресивне розгорнення. В HEVC не представлено явних функцій кодування черезрядкового розгорнення, тому що черезрядкове розгорнення не використовується в сучасних дисплеях і мають все менше поширення. Проте, в HEVC були представлені метадані, що дозволяють указати кодеру, що було закодовано відео із черезрядковим розгорненням в одному із двох режимів: у вигляді окремих зображень, як два поля (парні або непарні рядки кадру) або весь кадр цілком. Цей ефективний метод забезпечує кодування відеосигналу із черезрядковим розгорненням, минаючи необхідність навантажувати декодери підтримкою спеціального процесу декодування.

Профілі

Проект містить у собі три профілі: Основний (Main), Основний 10 (Main 10) і Основний профіль нерухливих зображень (Main Still Picture) [16].

Профіль – це певний набір засобів кодування й алгоритмів, які можуть бути використані для створення відеопотоку, що відповідає цьому профілю [15]. Кодер при формуванні відеопотоку визначає, які компоненти можна використовувати для профілю, у той час як декодер повинен підтримувати всі функції для даного профілю.

Main (Основний профіль)

Для основного профілю визначені наступні обмеження:

– Глибина кольору – 8 біт на канал (16,78 млн можливих кольорів),

– Колірна субдискретизація – 4:2:0,

– Розмір буфера декодера обмежується 6 кадрами максимального розміру яскравістної компоненти для цього рівня.

Main 10 (Основний профіль 10)

Main 10 – профіль для кодування відео із глибиною кольору 10 біт на канал [16].

Main Still Picture (Основний профіль нерухливих зображень)

Основний профіль нерухливих зображень дозволяє кодувати окреме зображення при дотриманні деяких обмежень, що відповідають Основному профілю [16].

Рівні

Проект HEVC визначає два шари, Основний (Main) і Високий (High), і 13 рівнів [16]. **Рівень** (Level) являє собою набір обмежень для потоку даних, пов'язаних з обчислювальними можливостями декодера й завантаженням пам'яті. Рівень установлюється, виходячи з максимальної частоти дискретизації, максимального розміру кадру, максимальної швидкості потоку, мінімального ступеня стиску й можливостей кадрового буфера декодера й кодера. Поняття **шар** (англ. Tier – ярус) було уведено для додатків, які розрізняються тільки максимальною швидкістю потоку і ємністю кадрового буфера кодера. Основний шар був розроблений для більшості додатків, а Високий рівень призначений для додатків з підвищеними вимогами. Декодер, що відповідає певному шару й рівню, повинен декодувати всі потоки, закодовані з параметрами цього шару й рівня й усіх більше низьких шарів і рівнів. Для рівнів нижче четвертого допускається тільки Основний шар [1] [16].

Висновок. У статті розглянуто та проаналізовано програмне забезпечення, яке призначено для системи ВКЗ побудованої на базі терміналів Yealink VC200. В межах України в недостатній мірі представлені вітчизняні розробки в цій області. У роботі наведені теоретичне узагальнення й рішення наукового завдання дослідження методів ВКЗ побудованої на базі терміналів Yealink VC200. Рішення даного завдання полягало у

вирішенні наступних задач: Був проведений огляд існуючих систем ВКЗ побудованої на базі терміналів Yealink VC200; Досліджена система ВКЗ побудованої на базі терміналів Yealink VC200. На основі отриманих результатів досліджень створена програмна реалізація системи ВКЗ побудованої на базі терміналів Yealink VC200. Розроблені під час виконання роботи алгоритми дозволяють успішно вирішувати завдання ВКЗ побудованої на базі терміналів Yealink VC200.

Список літератури

1. Айфичер Э. Цифровая обработка сигналов. Практический подход / Э. Айфичер – М.: «Вильямс», 2004. – 992 с.
2. Амиантов И.Н. Избранные вопросы статистической теории связи / Амиантов И.Н. – М.: Советское радио. – 1971. – 416 с.
3. Артеменко М.Е., Касымов Р.Р. Прогнозирование временных рядов для задач управления с использованием аппарата нейронных сетей и вейвлет анализа / М.Е. Артеменко, Р.Р. Касымов // Холодильна техніка і технологія. – 2010. – №3. – С. 74-76.
4. Артеменко М.Е, Касымов Р.Р. Использование вейвлетов для повышения качества прогноза телекоммуникационного трафика/ М.Е. Артеменко, Р.Р. Касымов // Зв'язок. – 2010. – №3.- С. 57-60.
5. Баранник В.В. Обоснование базовой технологии компрессии изображений с заданным качеством визуализации / В.В. Бараник, И.Е. Рогоза, А.А. Краснорукий // Інформаційно-керуючі системи на залізничному транспорті. – 2013. – Вип. 1. – С. 17-23.
6. Баранник В.В. Теоретичні основи та методи стиску зображень в телекомунікаційних системах на підставі біноміально-поліадичного представлення: Автореф. дис. д.т.н.: 05.12.02 / В.В. Баранник //. – Харків, Українська державна академія залізничного транспорту 2006. – 36 с.
7. Бараннік В.В. Метод стиснення НН-квадратури вейвлет-перетвореного зображення на основі поліадичного кодування/ В.В. Бараннік, А.В. Ширяєв, П.Н. Гуржий // Наукоємні технології, 2011. № 1-2 (9-10) – С. 69-72.
8. Богданова Н.В. Метод та способи підвищення ефективності управління телекомунікаційними мережами: Автореф. дис. кандидата техн. наук: 05.12.02/ Н.В. Богданова // Державний університет інформаційно-комунікаційних технологій. – К. 2008. – 20 с.
9. Бомба А.Я. Застосування арифметичного кодування у растровому графічному форматі PNG / А.Я. Бомба, О.В. Шпортько // Вісник Нац. ун-ту водного господарства та природокористування: серія «Технічні науки». – Вип. 2(50). – 2010. – С. 246-247.
10. Ватолин Д.С. Алгоритмы сжатия изображений: метд. пособие / Д.С. Ватолин – М.: МГУ им. В.М. Ломоносова, 1999. – 76 с.
11. Ватолин Д. Методы сжатия данных. Устройство архиваторов, сжатие изображений и видео / Д. Ватолин, А. Ратушняк, М. Смирнов, В. Юркин. – М.: ДИАЛОГ-МИФИ, 2003. – 384 с.
12. Вегешна Ш. Качество обслуживания в сетях IP / Ш. Вегешна – Пер. с англ.. – М.: Издательский дом «Вильямс», 2003. – 386 с.
13. Вентцель Е.С. Теория вероятностей: учеб. для вузов / Е.С. Вентцель. – М.: Высш. шк., 1999. – 576 с.
14. Вишневский В.М. Теоретические основы проектирования компьютерных сетей / В.М. Вишневский – М.: Техносфера, 2003. – 512 с.
15. Галкин В.А. Телекоммуникации и сети / В.А. Галкин, Ю.А. Григорьев. – М.: МГТУ имени Н.Э. Баумана, 2003. – 608 с.
16. Гмурман В.Е. Теория вероятностей и математическая статистика / В.Е. Гмурман. – М.: Высшая школа, 2003. – 479 с.

УДК 004

В. Яремєнко, магістр гр. КІ-18М-1,4
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ЦОД

У статті розроблено програмне забезпечення, яке призначено для системи забезпечення безпеки ЦОД. Метою розробки є дослідження та програмна реалізація системи забезпечення безпеки ЦОД. Об'єктом дослідження є процес забезпечення безпеки ЦОД. Предметом дослідження є методи забезпечення безпеки ЦОД. Методи дослідження базуються на методах захисту інформації, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи забезпечення безпеки ЦОД. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.
комп'ютерна інженерія, захист інформації, ЦОД

Постановка проблеми. . Безпека виходить на перший план при проектуванні центрів обробки даних. Ці місця зосередження інформаційних ресурсів стають головною мішенню хакерських атак, які можуть мати самі серйозні наслідки. Так, кількість простоїв центрів обробки даних (ЦОД) через інциденти в області безпеки зросло з 2% в 2017 році до 22% в 2018-м. Навіть якщо атака спрямована проти всього лише одного з орендарів ЦОДу, постраждати можуть і всі інші, як у випадку масштабних DDoS-атак.

Збільшення числа погроз і обсягу трафіку змушує власників центрів обробки даних застосовувати різні рішення для їхнього захисту, що, у свою чергу, приводить до бурхливого росту відповідного ринку. Так, по даним Markets and Markets, загальні продажі продуктів безпеки для ЦОДів повинні скласти в 2018 році 6,3 млрд доларів, а до 2021 року очікується дворазове збільшення – до 12,9 млрд доларів, тобто збільшення більше 15% щорічно. Схожі цифри приводять і інші аналітичні агентства – наприклад, Transparency Market Research прогнозує щорічний приріст в 12,6%.

У широкому змісті забезпечення безпеки ЦОДу можна розділити на фізичний і логічний захист. Незважаючи на всю важливість першого, головні зусилля зосереджені на другому. Так, згідно Transparency Market Research, ще в 2017 році на логічні компоненти витрачалося 85% всіх засобів, що направляються на усунення ризику погроз для ЦОДів. При цьому через повсюдний перехід до хмарних обчислень і необхідності прискорення розробки застосунків принципи захисту доводиться переглядати.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи забезпечення безпеки ЦОД.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи забезпечення безпеки ЦОД.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

- Огляд існуючих систем забезпечення безпеки ЦОД.
- Дослідження системи забезпечення безпеки ЦОД.
- Програмна реалізація системи забезпечення безпеки ЦОД.

Об'єктом дослідження є процес забезпечення безпеки ЦОД.

Предметом дослідження є методи забезпечення безпеки ЦОД.

Методи дослідження базуються на методах захисту інформації, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. В останні кілька років розподілені атаки типу «відмова в обслуговуванні» (Distributed Denial Of Service, DDoS) еволюціонували з відносно простих (flood) атак у досить комплексні й багатоступінчасті атаки. Разом із традиційними атаками високого рівня, які направляють масовані обсяги трафіку з метою перевантаження сервера, бізнес також зштовхнувся зі спрямованими атаками. Вони використовують щодо невеликий обсяг трафіку, націлений на додатки, які обробляють величезні обсяги даних. Причому ці атаки не виявляються традиційними рішеннями захисту від DDoS.

Рішення DDoS Secure для забезпечення безпеки ЦОД забезпечує функції повністю автоматизованого DDoS-захисту для інтернет-сервісів, з використанням поведінкового підходу до виявлення й відбиття атак DDoS. Рішення забезпечує захист від атак високого рівня, а також просунутих атак типу «low-and-slow» на рівні застосунків. Шляхом кореляції вхідних ризиків і відповідної реакції, DDoS Secure для забезпечення безпеки ЦОД здатно виявляти «невидимі» атаки, які розроблені для обходу сигнатурних захисних систем. Докладно про це рішення під катом

Спочатку про DDoS

Перша розподілена атака типу DDoS відбулася в 2000 р. і була націлена на сайти Amazon, eBay і інші площадки e-commerce. Як інструмент використовували ботнет з безлічі ПК, які генерували величезне число запитів і завантажили сервери, що обслуговують портали e-commerce, настільки сильно, що ті вже не могли обробляти запити користувачів. Загальний збиток від атак оцінюється приблизно в $1,7 млрд.

З тих пор DDoS-атаки дуже сильно еволюціонували: від примітивного інструмента, що використовує атаки з більшим обсягом трафіку для перевантаження веб-серверів, до складних комплексних атак рівня застосунків, розроблених для прицільного удару по стратегічним бізнес-ресурсам. В 2012 р. відбулася серія таких атак проти банківської індустрії, з метою здійснення фінансового шахрайства. Сектори утворення й електронної комерції теж стали мішенню кіберзлочинців.

Інтернет і соціальні мережі зробили з інформації зброя, що може бути використане проти користувачів. Це означає, що кіберзлочинці як і раніше мають доступ до безлічі дешевих ботнетів і безкоштовних програмних засобів типу Low Orbit Ion Cannon (LOIC), які легкі в застосуванні й можуть вивести з ладу інфраструктуру застосунків більшості компаній.

Вартість однієї години DDoS-атаки приблизно становила всього $5, тиждень безперервної DDoS-атаки – приблизно $260, а місяць – усього $900.

Способи й мотиви застосування DDoS також еволюціонували. Цей тип атак стали частіше використовувати групи «хактивистів» типу Anonymous для соціальних протестів і організованої злочинної діяльності, наносячи фінансовий збиток атаками по заданим веб-сайтах і веб-сервисам. Крім того, DDoS-атаки відіграють більшу роль у витончених гібридних атаках на організації, для яких Інтернет грає критично важливу роль. Гібридні атаки мають на увазі використання техніки DDoS для того, щоб спантеличити команди фахівців IT і ІБ і ефективно відволікти їхня увага від більше уразливих місць у захисті.

Не тільки тактика, але й мотиви DDoS-атак стали трохи іншими за останні пару років, починаючи з «хактивизма» і закінчуючи фінансовим експлойтами й шахрайством, а також політично мотивованими атаками й атаками соціального протесту. Деякі експерти навіть заявили, що DDoS-атаки «зібрані під парасолькою цивільної непокори».

2013 р. показав, що DDoS-атаки досягли нового рівня й привели до ще більшого числа згадувань у ЗМІ. У той час, як багато компаній продовжують думати, що їх веб-сайти й інфраструктура застосунків адекватно захищені проти кібератак, інші вже приготувалися до захисту проти більше складної структури DDoS-атак. Відповідно до незалежного дослідження, 64% IT-фахівців (щомають більше 10 років досвіду) заявили, що потужність кібератак на підйомі, при цьому тільки 25% заявили, що мають можливість прийняти відповідні контрзаходи. Усього 22% ИТ-Менеджерів, що приймає рішення, уже впровадили захист від DDoS.

Ескалація DDoS-атак рівня застосунків

DDoS-атаки рівня застосунків є сьогодні однієї з найпоширеніших і руйнівних форм кіберзагроз. Прості DDoS атаки з більшим обсягом трафіку усе ще заподіюють проблеми, однак їх легко виявити. При правильній організації оборони ризики цих атак зведені до нуля. Новий тип DDoS рівня застосунків під кодовою назвою «low-and-slow», проте, набагато складніше виявити й відбити, що являє собою реальну загрозу для бізнесу.

2012 р. показав різкий стрибок DDoS-атак типу Layer 7. Ці атаки протікають малопомітно, оскільки свій трафік вони видають за легітимний. Атаки Layer 7 або рівня застосунків, скоріше, орієнтуються на уразливості в самому коді застосунків, чим на застосування «лобової» атаки, для досягнення необхідних результатів. Ціль більшості атак рівня застосунків – це добре відоме ПО, що використовує HTTP, HTTPS, DNS, and VoIP (Session Initiation Protocol або SIP). Як і flood атаки, атаки L7 вимагають дуже мало витрат з боку кіберзлочинців. Цілком можливо паралізувати великі веб-сайти з одного ноутбука, відсилаючи від 40 до 60 однакових запитів у секунду (скорочено PPS, або пакетів із секунду). У той же час в flood атаках відсилається від декількох сотень або тисяч PPS до мільйонів. Зовнішня легальність – це те, що робить атаки L7 розповсюдженими й надзвичайно важкими для виявлення й блокування.

Атаки рівня застосунків можуть бути не виявлені системою захисту, тому що користуються слабкою стороною технології виявлення, що використовує принцип мережного потоку й методику граничних величин. RUDY (U-Dead-Yet) і Slow Loris – це два типи атак рівня застосунків, які націлені на HTTP-протокол. Зловмисники намагаються запустити безліч запитів, які важко обслужити, вичерпуючи ресурси додатка й швидко паралізуючи веб-сайт.

Якийсь час назад хакери почали використовувати атаку DNS-посилення (відбиття). Її суть полягає в тому, що хакер надсилає короткий запит уразливому DNS-серверу, що відповідає на нього вже значно більшим за розміром пакетом. Якщо використовувати в якості вихідного IP-адреси при відправленні запиту адреса комп'ютера жертви (ip spoofing), то уразливий DNS-сервер буде посилати у великій кількості непотрібні пакети комп'ютеру-жертві, поки повністю не паралізує його роботу.

DNS-сервери є привабливим видобутком, тому що вони звичайно дуже великі, працюють на широкополосному інтернет-каналі, і не можуть бути так просто занесені в «чорний» список.

Хакери використовують DNS шляхом підміни цільової адреси й відправлення невеликих запитів на DNS-сервер, що відповідає на ці помилкові запити в 10~1000 разів більшим обсягом трафіку, тим самим бомбардуючи жертву масованою хвилею трафіку. Узяті окремо, ці запити до DNS є легітимними, так само як і відповідні дані; проте, за рахунок камуфляжу зловмисник може залишатися анонімним і управляти привселюдно доступними DNS для відбиття атак і посилення їхньої потужності.

Застосовуючи такі методи атак в 2013 р., невелика група злочинців змогла згенерувати найбільшу DDoS-атаку в історії, досягши безперервного потоку трафіку на рівні 300 Гбіт/с. Хакери атакували spamhaus.com, організацію, що публікує «чорні» списки спамерів в Інтернеті.

Альтернативна форма DNS-атак може привести в результаті до пробоїв у захисті, як недавно відбулося в Каліфорнійському університеті в Сакраменто, коли було украдено порядку 1800 записів. Хакери змогли зламати університетський DNS-сервер. Але ризику піддаються не тільки університети. Ігрова, фінансова, роздрібна онлайн-індустрії є також уразливими для таких атак.

Відволікаюча DDoS-атака, що є набагато більше підступним типом мультивекторних атак, використовує масштабний DDoS як тактичний прийом відволікання уваги IT-персоналу, у той час як кіберзлочинці здійснюють розкрадання даних або фінансових засобів. Банки й фінансові організації найбільше часто піддаються цьому типу атак. Публічний приклад – кібератака, що відбулася в Bank of the West4 у грудні 2012 р. Знаючи,

що команда IT-фахівців буде на канікулах, хакери правильно вибрали час і контекст мети. Спершу банк піддали DDoS-атакам, і, поки службовці банку й IT-персонал намагалися зупинити потужний потік трафіку на їхні сервери й удержати стабільність роботи онлайн-сервісів, кіберзлочинці успішно викрали $900 000.

Недавня відволікаюча DDoS-атака на онлайн-валюту Bitcoin6 ілюструє сутність, що трансформується постійно, DDoS. У цьому випадку, кіберзлочинці використовували DDoS-атаки як «димову завісу» для реалізації атаки на DNS-записі Bitcoin. Хакери змогли створити іншу IP-адресу в актуальному DNS-записі для онлайнового чат-форуму Bitcoin. Шляхом вставки цих шкідливих машинних адрес у звичайний повсякденний DNS-Механізм, хакери прозоро перенаправляли трафік користувачів на сервер, що належить зловмисникам. Як тільки користувач входив у свій обліковий запис на зламаній машині, хакери записував його облікове ім'я й пароль, які пізніше могли бути використані для спустошення гаманця цього користувача.

Атака для злодійства паролів проти користувачів Bitcoin могла бути виявлена, однак цьому перешкодила «димова завіса», створена за допомогою DDoS-атаки, що порушувала доступність, у той час як запису DNS-адрес змінювалися.

Атаки рівня застосунків всі частіше направляються проти онлайн-банкінгу інтернет-магазинів. Ці атаки часто ховають у шифрованому (HTTPS/SSL) трафіку й вони залишаються невидимими для традиційних рішень. Як приклад, така атака може бути запущена шляхом функції «add to cart» на веб-сервері, генеруючи більше трафіку, чим зможуть обробити додатка, перевантажуючи сайт і генеруючи повідомлення про помилку для кінцевих користувачів, які намагаються робити онлайн-покупки. Ці атаки не виявляються, поки не стане занадто пізно, оскільки вони використовують легальні канали трафіку для проникнення на веб-сервери й додатки.

«Атаки нульового дня» є мегатрендами DDoS, вони націлені на новітні виявлені уразливості у веб-додатках, а не на лавинний потік даних. Величезне число веб-застосунків сьогодні запускається на мобільних пристроях (згадаємо тренд BYOD), що піддає компанії великому ризику DDoS-атак «нульового дня».

Вплив на бізнес

У цей час переважна більшість професіоналів в області ИТ і інформаційної безпеки інформовані про ризики для бізнесу, які несуть кібератаки. У той же час, вони не підготовлені відповідним чином. Відповідно до дослідження Ponemon Institute, проведеному в лютому минулого року7, 60 % IT-фахівців відповіли в анкеті, що DDoS-атаки є найбільш серйозним типом атак, які випробовують компанії. Збиток, заподіяний DDoS-атакою, може вплинути на бізнес, незалежно від його розміру.

Оскільки компанії збільшують свою присутність в Інтернеті й, таким чином, подовжують «лінію фронту», на якій може бути проведена атака, час простоїв веб-серверів або застосунків через DDoS-атаки є реальною погрозою. Бізнеси покладаються на безперервну доступність їх веб-серверів і застосунків, тому кілька годин простою можуть привести до катастрофи. Вони повинні забезпечувати роботу веб-сервісів без усяких перебоїв у режимі 24x7x365. Стабільність роботи застосунків – це критична вимога для цих бизнесів.

Простої не тільки приведуть до збитків і відлякування замовників, вони також негативно впливають на цінність бренда й репутацію. В індустрії фінансових сервісів кіберзлочинці використовують крадіжку конфіденційних даних і фінансове шахрайство. У секторі утворення й охорони здоров'я основний інтерес полягає в доступі до студентської інформації, електронним медичним записам і розкраданню важливих конфіденційних даних, що може привести до великих судових позовів і жахливих наслідків для людей, до яких украдена інформація. Збої в роботі сайтів із продажу авіаквитків і онлайн-магазинах веде до зниження прибутку й втраті репутації. За DDoS-атакою можуть піти фінансові втрати, які важко відновити.

Статистика DDoS-атак рівня застосунків насторожує. Gartner оцінює, що 70% всіх погроз націлені на рівень веб-застосунків. Дослідження Ponemon Institute виявило, що середній щорічний збиток від DDoS-атаки оцінюється в $3,5 млн. Інше недавнє дослідження Forrester оцінює середні фінансові витрати в $2,1 млн для кожних 4 годин простою й $27 млн для 24 годин простою, викликаних DDoS-атаками. Forrester указує, що частота атак у всіх галузях приблизно дорівнює 1 разу на місяць, у той час як у фінансовому секторі це трапляється 1 раз у тиждень. Якщо виходити із привселюдно доступних оцінок збитку, надаваних організаціями, які підверглись атакам, то фінансові компанії зазнали шкоди в середньому біля $17 млн на кожний інцидент в 2012 р. И, хоча найчастіше атакують фінансові організації, дослідження Forrester показало, що урядові заклади, у середньому, піддаються більше тривалим атакам. Це відбувається з тієї причини, що фінансові організації, як правило, використовують більше якісний захист від кібератак.

Незважаючи на цю тривожну статистику, менш чим 25% компаній впровадили рішення для захисту від DDoS**.**

Потреба у виділеному локальному DDoS-рішенні

Відбиття лавинних атак на рівнях 3 і 4 традиційно виконується в хмарі за допомогою рішення, що інспектує зворотний трафік. Ці атаки, що вимагають широкого каналу, досить легко виявляються й відбиваються сервісом-провайдером. Насправді, замовники можуть навіть не помітити яких-небудь проблем. Є, однак, багато середовищ, де, в основному з міркувань безпеки, дані просто не можуть покинути приватні мережі. Крім того, атаки рівня застосунків типу «low and slow» не можуть бути відбиті в хмарі, тому що ці атаки звичайно не споживають багато трафіку й заховані в легітимному трафіку.

Відбиття цих атак вимагає окремого локального рішення в корпоративному ЦОДі. Виділене DDoS-рішення потрібно по безлічі причин:

– Система захисту периметра, що включає файрвол, NG-файрвол і окремі системи запобігання вторгнень недостатньо добре підходять для захисту проти DDoS-атак, оскільки добре технічно підготовлені атаки можуть швидко переповнити таблицю статусів з'єднань і паралізувати файрвол або IPS, піддаючи целую мережа ризику.

– Файрволи й IPS-системи можуть самі по собі стати метою для атаки «на відмову», вимагаючи захисту.

– Файрволи й IPS-системи не можуть протистояти більше витонченим атакам рівня застосунків, оскільки ці рішення створені для того, щоб пропускати саме ті протоколи, які використовуються під час цих атак; кожний хакер знає, що файрвол звичайно пропускає HTTP- і HTTPS-трафік, адже більшість систем вимагає такого доступу для відповідного зв'язку з веб-сервісом.

Обмеження традиційних рішень для відбиття DDoS-атак

Традиційні рішення для виявлення DDoS-атак обмежені по своїх можливостях, вони здатні управляти тільки мережною телеметрією, такий як мережний потік (netflow), що не несе атрибутів рівня застосунків і залишає більший пролом при виявленні сучасних атак рівня застосунків. Крім того, всі ці рішення забезпечують сигнатурне детектування й відбиття атак у режимі «on premises», що не є ефективним проти невідомих атак нульового дня. Далі, такі рішення оцінюють тільки вхідний трафік на основі сигнатурної бази погроз, залишаючи уразливості в безпеці для проходу шкідливого трафіку. Один із прикладів – атака DNS-посилення.

Крім того, традиційні рішення не здатні розрізняти легітимний і згенерований машинний (шкідливий) трафік. Таким чином, система повинна бути зконфігурована вручну для визначення високого/середнього/низького граничних величин, на яких трафік повинен бути блокований. Подібний підхід веде до компромісу між низьким порогом помилкового позитивного спрацьовування й агресивним захистом.

Якщо поріг виставлений занадто високо, це створює проблему помилкового позитивного спрацьовування, що приводить до блокування більших обсягів легального трафіку. Якщо поріг занижений, то потенційно шкідливий трафік буде дозволений, що

приведе до злому. Недостача інструментів захисту на рівні Layer 7 і нездатність реалізувати моніторінг захищених ресурсів роблять традиційні DDoS-рішення неефективними проти сучасних атак, які здійснюються поза границею сигнатурного периметра. Статичний поріг не відповідає вимогам захисту. Є також адміністративна проблема, пов'язана з підтримкою набору сигнатур і ручного налаштування порога.

Коротенько, забезпечення повного спектра засобів захисту проти сучасних DDoS-атак вимагає окремого рішення з малим часом очікування, розташованого локально на периметрі ЦОДу. Таке рішення оцінює продуктивність кожного додатка, від layer 7 до мережних ресурсів, необхідних для гарантії їхньої доступності, здійснюючи моніторінг як вхідного так і вихідного трафіку. Це найбільш ефективний підхід для запобігання відомих і невідомих атак, що розрізняють легітимний і шкідливий трафік, і мінімізуючий помилкові позитивні спрацьовування. У цьому випадку навіть не потрібна ручне налаштування сигнального порога, що був завжди необхідний, але ж він створює постійне операційне навантаження, і завжди запізнюється в порівнянні з реальними змінами в шаблоні трафіку. Цей інноваційний евристичний підхід більш докладно описаний нижче.

На противагу традиційним рішенням, DDoS Secure для забезпечення безпеки ЦОД використовує несигнатурні технології для виявлення й відбиття атак рівня застосунків. Програма інспектує весь вхідний і вихідний трафік на периметрі ЦОДу, а також здійснює моніторінг продуктивності застосунків з кожним вхідним клієнтським запитом. Перед використанням граничного методу або налаштування для відбиття атак, DDoS Secure для забезпечення безпеки ЦОД використовує спеціальний алгоритм, CHARM, для кількісної оцінки ризиків у режимі реального часу, пов'язаної із двостороннім трафіком. Продукт аналізує ресурси цільового додатка, коли останнє прибуває під атакою. Якщо додаток атакують, він піднімає поріг CHARM, необхідний для доступу до застосунків, блокуючи найбільш ризиковий трафік. Шляхом кореляції вхідних ризиків і вихідної реакції, DDoS Secure для забезпечення безпеки ЦОД здатний виявляти невидимі атаки, які типово обходять традиційні сигнатурні рішення захисту від DDoS.

Інноваційна архітектура DDoS Secure для забезпечення безпеки ЦОД використовує процес «зворотного зв'язка» для аналізу повного циклу вхідних пакетів і відповіді, що був відправлений назад запитуючій стороні.

DDoS Secure для забезпечення безпеки ЦОД є що самонавчається й не вимагає налаштуванання або визначення граничної величини. Він здійснює моніторінг того, як додаток реагує й аналізує кожний напад. Цей інноваційний евристичний підхід дозволяє технологіям визначати, як повинен виглядати нормальний трафік і нормальна реакція з боку додатка. Коли відбувається нова атака, DDoS Secure для забезпечення безпеки ЦОД обновляє алгоритм для включення характеристик нової атаки, створюючи високоінтелектуальну систему оборони від DDoS, що включає динамічні відновлення. У випадку атаки DNS-посилення, DDoS Secure для забезпечення безпеки ЦОД застосовує інтелектуальний підхід у відношенні DNS-ресурсу з метою відбити атаку ще до того, як вона паралізує DNS-сервер. Спеціальні фільтри DDoS Secure для забезпечення безпеки ЦОД відсівають періодично повторювані запити DNS-системи для однієї й тої ж інформації, тим самим запобігаючи атаці DNS-посилення й захищаючи мети зловмисників від злобливих запитів, що впливають на їхню доступність.

По суті, система розрізняє реальний користувальницький трафік і трафік, згенерований машиною. Цей підхід гарантує пропуск легітимного трафіку й блокування атак ще до того, як вони заподіють шкоду. Це критично важливо протягом періоду, коли сервери перебувають під високим навантаженням, наприклад, під час різдвяних свят, коли будь-які перебої в доступі до сервера через помилкове позитивне спрацьовування можуть привести до падіння прибутку. Багато хто кіберзлочинці сьогодні комбінують ці нові ускладнені DDoS-атаки із традиційні «лавинними» атаками; у той же час, DDoS Secure для забезпечення безпеки ЦОД здатний виявляти й запобігати обидва типи атак.

DDoS Secure для забезпечення безпеки ЦОД можна встановити у вигляді фізичного пристрою розміром 1U, або віртуальної машини. Оскільки рішення корелює вхідну й вихідну інформацію для оцінки ризиків, а не використовує визначену граничну величину, помилкові позитивні спрацьовування обмежені, що робить керування простим і легенею в розгортанні. Крім того, інтеграція BGP дозволяє рішенню працювати із хмарним захисним рішенням для боротьби з масштабними «лавинними» атаками.

Розробка структурної схеми

DDoS-атаки залучають, мабуть, найбільша увага через їхні широкомасштабні наслідки. Так, недавня атака на сервери компанії Dyn, що контролює значну частину інфраструктури DNS, привела до неприступності безлічі відомих сайтів у США і Європі. Це була сама велика атака з використанням заражених пристроїв, які зараз прийнято відносити до Інтернету речей (у цьому випадку цифрових камер і DVD-плеєрів). Потужність атаки з використанням мережі 100 тис. ботів Mirai склала, за деякими оцінками, 1,2 Тбіт/с, що вдвічі більше, ніж коли-або раніше.

Як відзначається в недавньому звіті Nexusguard (служби захисту від DDoS), число атак в II кварталі 2018 року в порівнянні з аналогічним періодом 2015 року зменшилося майже на 40%, зате їхня інтенсивність значно зросла. Щоб захиститися від масованих атак, одних мір безпеки на рівні ЦОДу недостатньо. Тим часом дотепер є замовники, упевнені у тому, що вони можуть уберегтися від DDoS-атаки за допомогою міжмережних екранів і систем запобігання вторгнень. Як свідчить статистика, понад половину організацій, у яких були встановлені цей пристрої, зіштовхнулися зі збоями мережі в результаті атак DDoS. Крім використання спеціалізованих засобів, необхідно організувати ешелоновану оборону.

У ході DDoS-атаки ресурси ЦОДу піддаються «бомбардуванню» шляхом напрямку до них безлічі специфічних запитів і в остаточному підсумку перестають справлятися з навантаженням. Усього можна виділити три більших класи атак: масовані атаки на переповнення інтернет-каналу; атаки на пристрої з контролем стану, такі як балансувальники навантаження, міжмережні екрани, сервери застосунків; атаки на рівні застосунків, невеликі по потужності, але не менш ефективні – як правило, вони націлені на конкретні уразливості. DDoS-атаки легко організувати, а вартість відповідних пропозицій починається від 5 доларів у годину.

Концепція ешелонованої оборони для захисту від DDoS припускає установку двох спеціалізованих компонентів – у ЦОДі й в оператора. Перший дозволяє блокувати всі типи атак, однак, коли масштаб атаки на канал стає порівнянним з наявною пропускною здатністю, він звертається по допомогу до компонента, установленому в оператора. Тому дуже важливо, щоб ці компоненти «уміли» взаємодіяти один з одним.

Коли атака на канал досягає визначеної потужності, компонент у ЦОДі повідомляє оператора про необхідність очищення трафіку, що направляється на певний префікс. Крім того, в ідеалі таке двоскладне рішення повинне синхронізувати чорні й білі списки, а також профілі захисту. Орієнтуючись на чорні списки, оператор може здійснювати попередню фільтрацію трафіку, знижуючи навантаження на систему захисту ЦОДу. Таким чином, клієнтові (операторові ЦОДу) не потрібно звертатися до провайдеру із проханням про вживання термінових заходів для блокування атаки – захист включається автоматично, а час простою зводиться до мінімуму.

По оцінках закордонних експертів, загальна величина втрат від злому системи безпеки становить у середньому близько 4 млн доларів. Багато атак починаються з того, що зловмисник одержує доступ, у тому числі за допомогою соціальної інженерії, до робочого місця, однієї ВМ, а з її вже ініціюються атаки.

У новій, віртуальній реальності ті рішення, які використовувалися десятиліттями для захисту фізичних середовищ, перестають працювати. Подібні інциденти, у всякому разі помітна їхня частина, зв'язані саме з тим, що багато компаній продовжують використовувати старі засоби керування й захисту для середовищ віртуалізації, які засновані на агентському підході. При цьому на кожну одиницю, що захищається (ВМ) установлюється агент, що не

завжди виправдано, тим більше що його можна відключити. До того ж при безпосередньому захисті кінцевих крапок споживається велика кількість обмежених ресурсів, через що істотно знижуються продуктивність і ефективність ЦОДу.

Стара модель була сфальцьована на захисті кінцевих крапок, але тепер багато навантажень переміщаються на сервери й у хмари. Тим часом відомі виробники продовжують відтворювати у віртуальному середовищі архітектуру інформаційної безпеки, споконвічно розроблену для фізичного середовища. Це приводить до того, що нові уразливості на рівні гіпервізору й ОС виявляються незахищеними. Так, наприклад, атаки на рівні віртуальної мережі або з однієї ВМ на іншу не визначаються апаратними засобами, що контролюють фізичне середовище.

Усередині віртуального середовища треба використовувати нові способи захисту. При використанні технології віртуалізації, кращим рішенням є застосування засобів захисту від впливу шкідливого коду на рівні гіпервізору без установки агентського ПО на віртуальні машини. Однак такий підхід можливий, тільки якщо розроблювач має доступ на рівень віртуального комутатора, усередині якого й проходять всі пакети, які потім доставляються у ВМ.

Для захисту й керування віртуальними середовищами на базі Microsoft Hyper-V, мається доступ до віртуального комутатора Hyper-V, на рівні якого й реалізується захист.

Такий підхід дозволяє заощадити до 30% ресурсів сервера, а антивірусне сканування виконується в 70 разів швидше. У числі інших переваг безагентського підходу називається усунення залежності від дій персоналу й клієнтів, оскільки систему захисту не можна відключити на рівні ВМ. Крім того, загальна трудомісткість забезпечення безпеки в результаті знижується, оскільки тепер не потрібно піклуватися про кожну ВМ. Політикові можна налаштувати на хості або в центрі керування, а потім дуже швидко масштабувати її в рамках ЦОДу, адже віртуальне середовище надзвичайно динамічне – ВМ постійно створюються, переносяться й ліквідуються.

Завдяки інтеграції Cloud Security Plugin в System Center, провайдери можуть надати своїм клієнтам не тільки засобу керування інфраструктурою, але й інструменти контролю за безпекою. Будь-який клієнт зможе самостійно забезпечувати й контролювати безпеку своїх рішень. Якщо ви користуєтеся ресурсами декількох ЦОДів (наприклад, власного й приналежного хостінг-провайдеру), політики безпеки синхронізуються, так що при міграції у випадку аварії або перерозподілу навантаження з одного центра в іншій будуть зберігатися всі налаштуванання корпоративної безпеки.

Якщо на початковому етапі в хмару переносилися ємні, але не самі коштовні ресурси, то тепер, коли на порядку денному встало питання про перенос критичних ресурсів, каменем спотикання виявляється питання забезпечення ІБ. Коли клієнт передає свої ключові бізнес-сервіси в хмару, вона хоче бути впевнений у підтримці такої політики безпеки, що задовольняє його вимогам.

Безпека – це мережа

Резонансні зломи системи безпеки з очевидністю продемонстрували, що традиційний захист периметра, який фокусується на трафіку «північ – південь» (міжмережні екрани, системи виявлення й запобігання, що захищають від атак ззовні), не здатна відгородити від неприємностей центр обробки даних, де між серверами переважає трафік «схід – захід», що не виходить за його межі. За деякими оцінками, на останній доводиться три чверті всього обсягу трафіку ЦОДу.

Діючим рішенням проблеми розмежування трафіку усередині центра обробки даних є мікросегментація: поділ на численні захищені зони. Завдяки сучасним віртуалізованим рішенням практично кожна віртуальна машина може бути постачена власним міжмережним екраном, що дозволяє створити мережу з нульовим рівнем довіри усередині ЦОДу. Однак, як ми вже відзначали в попередньому розділі, набагато більше ефективним рішенням виявляється реалізація засобів безпеки на рівні гіпервізору – мова йде про убудований у цей гіпервізор віртуальному комутаторі.

Поява такого пристрою сталася відповіддю на потребу в забезпеченні оперативного розгортання й динамічної міграції віртуальних машин і застосунків. Наприклад, при розгортанні нового додатка після запуску ВМ потрібно було вручну задати VLAN, зконфігурувать маршрутизацію у фізичній мережі, налаштувати політики MCE. Всі ці операції забирали час, і до того ж вони виявлялися унікальними для кожної апаратної платформи, на якій побудований ЦОД. Інакше кажучи, додатка й ВМ були прив'язані до конкретної фізичної мережі. Необхідно було усунути цю прив'язку, тобто віртуалізировать мережа. Тепер у кожної платформи віртуалізації є свій комутатор, що є для неї «рідним». Наприклад, для гіпервізору ESXi такий віртуальний розподілений комутатор – Distributed Virtual Switch, для KVM у масштабах ЦОДу таким можна вважати Open Virtual Switch і т.д.

Поверх віртуального комутатора на програмному рівні реалізуються базові мережні функції: комутація, маршрутизація, брандмауер і балансування навантаження. Кожний фізичний сервер з гіпервізором стає не просто обчислювальною платформою, на якій можна виділити ресурси віртуальним машинам, але ще й багатогігабітним комутатором і маршрутизатором (старий слоган «мережа – це комп'ютер» одержує новий зміст). Щоб ці функції працювали, потрібна базова IP-з'вязність між серверами. На фізичній мережі більше не потрібно витрачати час на налаштування VLAN – досить один раз налаштувати транспортну мережу. Для передачі трафіку через фізичну мережу використовується інкапсуляція VxLAN.

Використання віртуальних комутаторів дозволяє автоматизувати рутинні операції по налаштуванню мережі, прискорити аварійне відновлення й, звичайно, підвищити ефективність захисту. Коли функції безпеки й фільтрації трафіку виконуються на рівні віртуальної платформи, на рівні гіпервізору, додатка можна захистити незалежно від нижчележачої фізичної архітектури. Напевно багато хто чули про мікросегментацію або про модель нульової довіри. Побудувати таку модель на платформі мережний віртуалізації дуже просто, для цього не буде потрібно розгортати безліч MCE.

Якщо відійти від питань безпеки й глянути ледве ширше, то віртуалізація мережі відкриває шлях до реалізації повністю програмно обумовлених центрів обробки даних.

На захист застосунків

У своєму прогнозі на 2019 рік серед 10 ключових технологічних тенденцій Gartner називає адаптивну архітектуру захисту. Правда, у порівнянні із прогнозом на поточний 2018-й, вона тепер перебуває не на сьомому місці, а на десятому, що пояснюється скоріше ефектом втрати новизни, чим зниженням актуальності. Як відзначається в коментарі, «багаторівневий захист і аналіз поводження користувачів і об'єктів стануть обов'язковими вимогами для кожного підприємства».

Адаптивний захист припускає вбудовування мір безпеки в усі бізнес-процеси – реалізація їх постфактум означає створення проблем самому собі. Відповідно, фахівці з безпеки повинні тісно взаємодіяти з архітекторами рішень і розроблювачами застосунків для включення мер безпеки ще на етапі проектування рішень і розробки застосунків. Останні всі частіше стають об'єктом цілеспрямованих атак.

Усе навчилися непогано захищати свою мережу, тому атаки поступово переносяться на прикладний рівень. На жаль, вони не детектуються за допомогою традиційних засобів, нездатних визначити, де запрограмована функція, а де переглянута помилка, – тобто немає аномалій, по яких можна вирішити, що йде атака.

При розгортанні хмарних сервісів більша увага приділялася можливостям, але не ризикам. Тепер же настала настав час фіксувати успіхи й думати про погрози, які починають захльостувати сервіси, побудовані без обліку такої небезпеки». Вибудуваний захист, орієнтований на монолітні додатки, безумовно, дозволяє нівелювати частина з них, тому що старі атаки нікуди не ділися. Однак нападу піддається не тільки сервіс у цілому (що виражається в спробах заблокувати канал або реалізувати якісь інші відомі атаки), але й окремі додатки в ньому.

Ця ситуація збільшується тим, що провайдери не мають контролю за надаваними додатками, які до того ж часто обновляються. Адже хмара – неважливо IaaS, PaaS або SaaS – це, по суті, деякий набір застосунків, створюваних іншими людьми. Не знаючи, як улаштовані конкретні додатки, відбивати нові атаки проти них, при організації яких використовується специфіка їхнього написання й проектування, стає усе сутужніше.

Зловмисники використовують помилки й уразливості в тих додатках, які пишуться швидко відповідно до гнучкої методології розробки (agile). Швидкість виводу на ринок нових функцій виявляється важливіше забезпечення їхньої безпеки, до того ж старі методи захисту просто не встигають за швидкістю розробки. Так, тест на проникнення (pentest) займає кілька тижнів, і до моменту його завершення можна бути впевненим лише у тому, що позаминула версія сайту була безпечною.

Розробка прискорюється, практично «іде з коліс» – зміни відбуваються кожні два тижні, а такі перевірки, як тест на проникнення, виконуються раз у півроку. У сформованій ситуації є лише один вихід – інтеграція систем захисту із самим об'єктом. Однак поки подібна можливість реалізована тільки в найбільших сервісах рівня Amazon, де окремої служби безпеки немає: є відповідальні за безпеку в команді розроблювачів і представники тої ж команди, наприклад, у підрозділі, що забезпечує доступність.

Таким чином, підхід до захисту застосунків кардинально міняється. Я думаю, що до 20-м років парадигми розробки й захисти застосунків повністю обновляться. Вони зіллються й будуть розвиватися разом. Ця тенденція явно простежується. Зараз ми перебуваємо на проміжному етапі, що характеризується реалізацією адаптивної безпеки, коли засіб захисту не тільки вивчає той або інш захищатися объект, що, але й підбудовується під нього, а також підбудовує об'єкт під свої вимоги. Однак поки тут більше питань, ніж відповідей.

Як захистити ЦОД

Атаки стають багатошаровими, багатоетапн і багаторівневими, вони здійснюються з різних сторін, з розвідкою, з відволіканням, із прикриттям. Зараз уже немає чистої DDoS- або чистої хакерської атаки. Тому ті, хто проектує засоби захисту, повинні розбиратися у видах атак. Тільки в рамках ЦОДу серйозного хостінг-провайдеру можна зібрати компетенції й устаткування такого рівня, що зможе протистояти атакам DDoS і іншим видам найбільш важких і руйнівних для бізнесу й репутації компанії дій.

Провайдери хмарних послуг перебувають в основній групі ризику – саме проти них спрямована основна частка атак DDoS. Однак навіть провайдеру неможливо реалізувати відразу всі міри захисту, тому їхнє впровадження відбувалося поетапно. Побудований в 2017 році центр обробки даних відповідає базовим вимогам до фізичного захисту ЦОДу рівня Tier III: відділений периметр навколо приміщень ЦОДу, цілодобова фізична охорона, комбінований контроль доступу з використанням RFID і біометрії, а також віддалене відеоспостереження з веденням архіву записів. Однак фізичний захист являє собою лише невелику частину мер по забезпеченню безпеки.

Насамперед класифікували наявні дані за критеріями їхньої критичності й доступності й звели все в таблицю, що дозволяє наочно бачити, для чого потрібно забезпечити пріоритетний захист. «Склавши таку таблицю, ви вже більш-менш розумієте, якими системами потрібно займатися в першу чергу. Крім цього, для ЦОДу в цілому були визначені основні джерела погроз, до яких віднесені DDoS-атаки, хакери, нелояльні співробітники й клієнти хостінгу.

На наступний рік після введення ЦОДу в експлуатацію були реалізовані заходи щодо забезпечення відповідності вимогам PCI DSS. Сертифікація по PCI DSS потрібна для тих клієнтів, хто проводить фінансові транзакції. Цей складний процес припускає реалізацію цілої програми, що складає з більш ніж 250 пунктів. Для захисту мережного периметра було розгорнуте рішення AlientVault. Платформа AlienVault Security Management (USM) дозволяє контролювати п'ять основних функцій безпеки з єдиної консолі: інвентаризацію активів, оцінку уразливостей, моніторінг поводження, виявлення вторгнення й кореляцію подій безпеки (SIEM).

Для захисту від DDoS-атак було впроваджене рішення RADware, однак для компанії воно виявилося надлишковим, тому на його базі було організоване надання послуг для банків. Реальний попит на них з'явився тільки після того, як банки піддалися атакам. Коли банки стали одержувати «листи щастя» від хакерів із пропозицією заплатити гроші, наступного дня майже всі вони приходили до нас і містили договори, і ми успішно усунули всі погрози.

Нарешті, цього року була реалізована система RAPID 7, що дозволяє проводити тестування уразливостей в ОС і сервісах, виявляти помилки в конфігурації, перевіряти відповідність політикам безпеки. Вона ж дозволяє імітувати злом, оцінити рівень готовності системи до роботи й скласти звіт з рекомендаціями про внесення необхідних поліпшень. Здавалося б, можна один раз виконати сканування й на цьому заспокоїтися. Насправді після будь-якої зміни в ОС і установки будь-якої латки сканування необхідно проводити знову. Так що замовникам виявляється вигідніше підписатися на послугу.

Вічне протистояння між нападом і захистом виходить на новий рівень. Атаки швидко роботизируються, а боти вже мають ознаки штучного інтелекту: вони діють автономно, самі знаходять додатки з уразливостями, які вони вміють розкривати, і починають діяти по певній програмі. Такі концепції, як адаптивна архітектура захисту, припускають перехід від пасивних мір до активної протидії в прагненні переграти кіберзлочинців на їхнє поле. Як виражаються в Gartner, захист повинна стати «рухливий і адаптивної».

Однак виключити на 100% імовірність успішної атаки незручно жодне технічний засіб, якщо існує обмін даними з якоюсь зовнішньою системою й інформація передається зовні. Для відомості збитку до мінімуму одним з рішень можуть бути прийняття моделі мінімальної довіри в ЦОДі, розмежування й обмеження прав адміністраторів, мікросегментація мережі.

Більш-менш великі компанії прагнуть побудувати свої ЦОДи й забезпечити їхній захист власними силами – така критична функція, як безпека, делегується досить неохоче. Як відомо, однієї із самих більших погроз для будь-який ІС є той, хто неї експлуатує. Однак, як указують провайдери послуг ЦОДів, хмарні ресурси більше абстраговані від конкретного персоналу, чим корпоративні. До того ж провайдери цілеспрямовано накопичують необхідні компетенції для організації професійної й тому ефективного захисту.

Забезпечувати безпека самому або довіритися провайдерам послуг ІБ – кожний вибирає залежно від своїх пріоритетів і можливостей, але погнатися в гонці кібервооружений за зловмисниками стає усе складніше. І погоня виявляється зовсім безнадійною справою, якщо намагатися обійтися лише застарілими методами периметрального захисту.

Захист від DDoS

Угадати всі можливі сценарії DoS атак з метою порушення забезпечення безпеки ЦОД – завдання не тривіальна. Проте, сучасні засоби захисту мережі мають у своєму составі засобу зм'якшення й запобігання найпоширеніших типів DoS-атак з метою порушення забезпечення безпеки ЦОД.

Сценарій захисту від DDoS повинен ураховувати наступне:

– Достатня потужність серверної ферми.

– Забезпечення розвантаження серверів застосунків засобами балансування навантаження, кешування й прискорення відпрацьовування запитів.

– Забезпечення достатньої потужності мережної інфраструктури й інфраструктури мережної безпеки.

– Застосування спеціалізованих пристроїв захисту від DDoS.

– Застосування глобального оповіщення про джерела й типи атак з метою порушення забезпечення безпеки ЦОД.

На схемі відображено три основні групи об'єктів:

– Користувачі

– Засобу захисту

– Цільові сервера

Користувачі

Всіх користувачів умовно можна розділити на чотири групи:

– Легітимні користувачі. Доступ цієї категорії користувачів повинен бути забезпечений.

– Користувачі, що виявили раптовий інтерес. У результаті соціальних процесів (вибори, публічні події, слухи про неприступність ресурсів) усе більше користувачів виявляють цікавість до атак з метою порушення забезпечення безпеки ЦОД надаються ресурсам, що, тим самим створюючи додаткове навантаження. Це збільшує плин DDoS. Проте, ці користувачі також повинні одержати доступ.

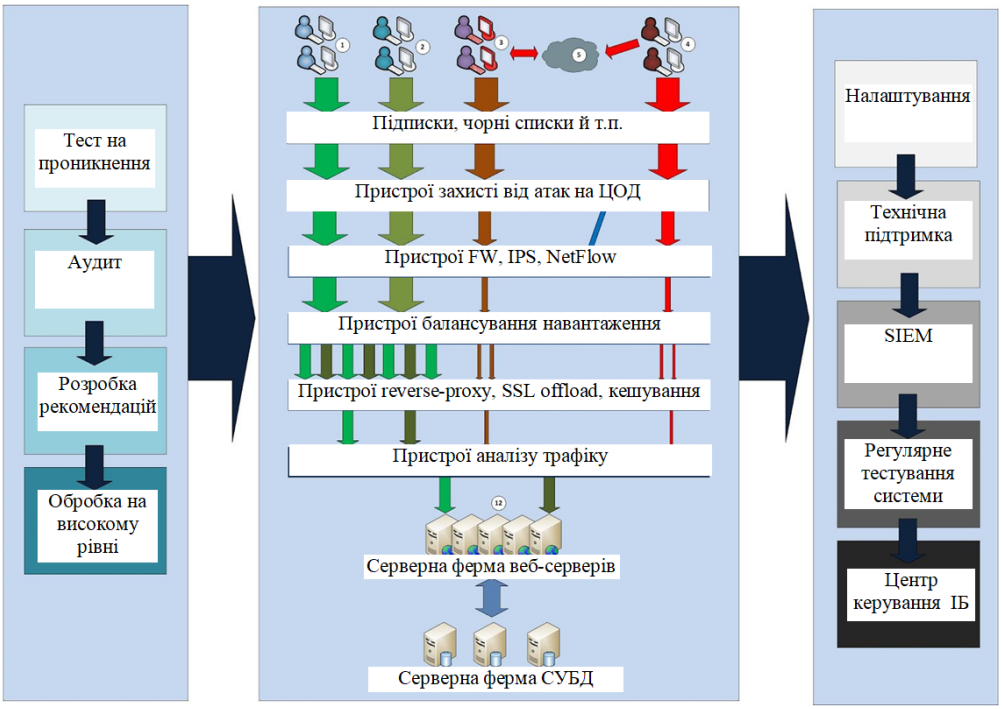


Рисунок 1 – Структурна схема системи

– На етапі планування архітектури необхідно передбачити очікуваний максимум звернень користувачів. Для цього необхідно передбачити достатню потужність серверної ферми й розвантаження серверів застосунків від відпрацьовування однакових запитів. Як правило, ця категорія користувачів обмежується переглядом стартової станиці або кінцевого числа сторінок, які можуть бути поміщені в кеш для прискорення відповідей без залучення значних обчислювальних потужностей на цільовому сервері застосунків.

– Користувачі, які беруть участь у бот-мережах. Найбільш легкий спосіб організації контрольованої DDoS атак з метою порушення забезпечення безпеки ЦОДи – використання розподіленого обчислювального ресурсу ботів-мереж. Більшість DDoS атак з метою порушення забезпечення безпеки ЦОД націлені на одержання прибутку, тому контролюємість процесу проведення й зупинки атак з метою порушення забезпечення безпеки ЦОДи дуже важлива. Найчастіше користувач навіть не знає, що його ПК є частиною бот-нета.

– Провідні розроблювачі рішень інформаційної безпеки відслідковують активність бот-мереж і командних центрів бот-мереж по усьому світі. Глобальні репутаційні списки дозволяють визначити потенційні джерела DDoS атак з метою порушення забезпечення безпеки ЦОДи й проактивно їх блокувати.

– Трафік, що виходить від таких користувачів має типову структуру, що вказує на роботу скрипта або робота. Так наприклад, важко представити, щоб легітимний користувач

зайшов на ЦОДу, що атакується 1000 разів у секунду й продовжував робити це в плині декількох годин.

– Спеціалізовані засоби захисту від DDoS можуть визначати й блокувати такий трафік. Класичні засоби мережного захисту (IPS, L7-Firewall) можуть визначити такий трафік і заблокувати, але мають обмеження у функціональних можливостях блокування DDoS. Складні типи атак з метою порушення забезпечення безпеки ЦОД можуть бути спрямовані на пристрої мережного захисту, тим самим організовуючи DDoS внаслідок вичерпання обчислювальних ресурсів засобів мережного захисту.

– Зловмисники. До цієї категорії користувачів ставляться як звичайні хулігани, що приймають добровільну участь в атак з метою порушення забезпечення безпеки ЦОДах, так і організатори атак з метою порушення забезпечення безпеки ЦОД, які можуть використовувати бот-мережі або спеціалізовані інструменти проведення складних атак з метою порушення забезпечення безпеки ЦОД.

Засоби захисту

Система захисту від DDoS повинна припускати ешелонованість, ураховувати весь спектр можливих DDoS атак з метою порушення забезпечення безпеки ЦОД, а також імовірність їхнього виникнення.

Для забезпечення високої ефективності відбиття DDoS атак з метою порушення забезпечення безпеки ЦОД необхідно передбачити спеціалізовані засоби захисту на всіх рівнях проходження трафіку до цільових серверів, що припускає:

– Визначення глобальної репутації джерела трафіку.

– Фільтрація трафіку спеціалізованими пристроями захисту від DDoS.

– Забезпечення достатньої продуктивності мережного встаткування й пристроїв мережного захисту, сигналізацію про характер трафіку на спеціалізовані засоби захисту від DDoS (наприклад, використовуючи технологію Netflow).

– Забезпечення розподілу навантаження між серверами застосунків, що виключає піки навантаження на одиничний сервер і дозволяє легко розширювати обчислювальні ресурси системи в цілому.

– Прискорення обробки запитів користувачів. В ідеалі, сервера застосунків повинні обробляти тільки унікальні запити, не виконувати ресурсномісткі операції (наприклад, шифрування SSL повинне забезпечується на спеціалізованих пристроях, розміщених перед серверною фермою).

– Фільтрація специфічних для веб-серверів атак з метою порушення забезпечення безпеки ЦОД. Вузькоспеціалізовані засоби можуть відбити більш складні типи веб-орієнтованих атак з метою порушення забезпечення безпеки ЦОД.

Цільові сервера

На цільових серверах необхідно забезпечити достатні обчислювальні потужності для обробки запитів користувачів у годину передбачуваного максимального навантаження. Веб-сайт повинен бути реалізований таким чином, щоб виключити (або мінімізувати) ресурсномісткі операції. Висока швидкість обробки типових запитів може значно зменшити негативний ефект від DDoS атак з метою порушення забезпечення безпеки ЦОДи.

При розробці сайту (порталу) необхідно визначити вимоги до безпеки. Нерідко DDoS реалізується використовуючи уразливості програмного забезпечення ЦОДу, який атакується.

Реалізація багаторівневої архітектури (винесення серверів баз даних) дозволяє значно розвантажити сервера за стосунків.

Планування системи захисту від DDoS атак з метою порушення забезпечення безпеки ЦОД

Система захист від DDoS буде забезпечувати максимальну ефективність блокування DDoS тільки у випадку правильного планування.

– Планування системи захисту від DDoS необхідно проводити використовуючи дані аналізу мережної інфраструктури, систем захисту, рівня безпеки серверів застосунків.

– Необхідно передбачити інструменти візуалізації подій інформаційної безпеки для своєчасної реакції на атак з метою порушення забезпечення безпеки ЦОДи.

– Необхідно передбачити навчання фахівців, що експлуатують систему.

– Необхідно передбачити регулярні перевірки коректності налаштуванань устаткування й дій обслуговуючого персоналу згідно розробленого плану реагування на DDoS.

Висновок. У статті розглянуто та проаналізовано програмне забезпечення, яке призначено для операційної системи забезпечення безпеки ЦОД. В межах України в недостатній мірі представлені вітчизняні розробки в цій області. У роботі наведені теоретичне узагальнення й рішення наукового завдання дослідження методів забезпечення безпеки ЦОД. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем забезпечення безпеки ЦОД; Досліджена система забезпечення безпеки ЦОД; На основі отриманих результатів досліджень створена програмна реалізація системи забезпечення безпеки ЦОД. Розроблені під час виконання роботи алгоритми дозволяють успішно вирішувати завдання забезпечення безпеки ЦОД. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки. Розроблене програмне забезпечення має простий, дружній та зручний інтерфейс користувача, що забезпечує легкість у освоєнні роботи програмного продукту, зручність у використанні, і не потребує особливих спеціальних знань. При створені програмного забезпечення було використано об’єктно-орієнтований підхід, що відповідає сучасним тенденціям у галузі розробки комерційних програмних систем. Програма реалізована на мові високого рівня Embarcadero Delphi 10.2. Дана мова програмування дозволяє найбільш ефективно обробляти дані. Це дозволило мінімізувати строк розробки програмного забезпечення, і, як слід, зменшити витрати на його розробку. Запропоноване програмне забезпечення ділиться на загальне програмне забезпечення, що поставляється із засобами обчислювальної техніки й спеціальне програмне забезпечення, що спеціально розроблене для даної конкретної системи й включає програми, що реалізують її функції.

Список літератури

1. Смирнов С. А. метод безопасной маршрутизации метаданных в облачные антивирусные системы / А. К. Дидык, С. А. Смирнов // Информационные технологии в управлении, образовании, науке и промышленности: монография / Под ред. профессора В. С. Пономаренко. –Х.: Видавець Рожко С.Г., 2016. – 566 с.
2. Смирнов С. А. Сравнительные исследования математических моделей технологии распространения компьютерных вирусов в информационно-телекоммуникационных сетях / Мохамад Абу Таам Гани, А. А. Смирнов, А. В. Коваленко, С. А. Смирнов // Системи обробки інформації: зб. наук. праць. – Х.: ХУПС, 2014. – Вип. 9(125). – 105-110.
3. Смирнов С. А. Математическая модель интеллектуального узла коммутации с обслуживанием информационных пакетов различного приоритета / Мохамад Абу Таам Гани, А. А. Смирнов, Н. С. Якименко, С. А. Смирнов // Збірник наукових праць Харківського університету Повітряних Сил. – Харків: ХУПС, 2014. – Вип. 4 (41). – С. 48-52.
4. Смирнов С. А. Исследование показателей качества функционирования интеллектуальных узлов коммутации в телекоммуникационных системах и сетях / Мохамад Абу Таам Гани, А. А. Смирнов, Н. С. Якименко, С. А. Смирнов // Наука і техніка Повітряних Сил Збройних Сил України: наук. журн. – Х.: ХУПС, 2014. – № 4(17). – С. 90-95.
5. Смирнов С. А. Усовершенствованный алгоритм управления доступом к «облачным» телекоммуникационным ресурсам / Мохамад Абу Таам Гани, А. А. Смирнов, Н. С. Якименко, С. А. Смирнов // Системи обробки інформації: зб. наук. праць. – Х.: ХУПС, 2015. – Вип. 1(126). – С. 150-153.
6. Smirnov S. A. Method of controlling access to intellectual switching nodes of telecommunication networks and systems / A. A. Smirnov, Mohamad Abou Taam, S. A. Smirnov // International Journal of Computational Engineering Research (IJCER). – India, Delhi, 2015. – Vol. 5, Issue 5. – P. 1-7.

7. Смирнов С. А. Анализ и исследование методов управления сетевыми ресурсами для обеспечения антивирусной защиты даннях / Мохамад Абу Таам Гани, А. А. Смирнов, С. А. Смирнов // Системи озброєння і військова техніка: наук. журн. – Х.: ХУПС, 2015. – № 3(43). – С. 100-107.
8. Смирнов С. А. Исследование эффективности метода управления доступом к облачным антивирусным телекоммуникационным ресурсам / Мохамад Абу Таам Гани, А. А. Смирнов, С. А. Смирнов // Наука і техніка Повітряних Сил Збройних Сил України: наук. журн. – Х.: ХУПС, 2015. –№ 3(20). – С. 134-141.
9. Смирнов С. А. Комплекс gert-моделей технологии облачной антивирусной защиты телекоммуникационной системы / А. А. Смирнов, А. К. Дидык, А. Н. Дреев, С. А. Смирнов // Безпека інформації: наук.-практ. журн. – К.: НАУ, 2015. – Т. 21, № 3. – С. 251-262.
10. Смирнов С. А. Метод безопасной маршрутизации метаданных в облачные антивирусные системы / А. А. Смирнов, А. К. Дидык, С. А. Смирнов // Системи озброєння і військова техніка: наук. журн. – Х.: ХУПС, 2016. –№ 2 (46). – С. 146-149.

УДК 336.143

Л. Ярина, магістр гр. ФС-18М(1,9)
Центральноукраїнський національний технічний університет

ОСОБЛИВОСТІ ФІНАНСОВОГО ЗАБЕЗПЕЧЕННЯ ОСВІТИ НА МІСЦЕВОМУ РІВНІ

У статті розглянуто особливості фінансового забезпечення освіти на місцевому рівні. Досліджено основні джерела фінансування закладів освіти для виконання покладених на них функцій та досягнення поставлених цілей. Запропоновано заходи щодо удосконаленняя розподілу обсягу освітньої субвенції.
фінансування, освіта, державний бюджет, місцеві бюджети

В умовах формування нової економіки, яку не безпідставно називають економікою знань, освіта забезпечує всебічний гармонійний розвиток особистості та її соціалізацію, стає одним із факторів економічного піднесення, позитивної соціальної динаміки, підвищення рівня якості життя. Інтелектуальна компонента людського та трудового потенціалу суспільства як базис нової економіки закладається на всіх рівнях освіти, проте провідна роль у накопиченні людського капіталу належить середній, фаховій передвищій та вищій освіті. На цих рівнях освіти відбувається не лише цілісний розвиток особистості та формування необхідних життєвих навичок, а й набуття професійних і загальних компетентностей, необхідних для діяльності людини за певною спеціальністю чи в певній галузі знань. Здійснення соціально-економічних перетворень у суспільстві суттєво впливають на всі сфери діяльності, докорінним чином змінюють принципи фінансування освітянської діяльності, пріоритети в роботі закладів освіти, їх правовідносини як з окремим громадянином, так і з державою в цілому. Тому фінансове забезпечення освіти є одним із головних факторів, що зумовлюють успішність реформування.

Питання проблем фінансового забезпечення розвитку освіти теоретично розробляли вітчизняні учені В. Андрущенко, Т. Боголіб, О. Бойко, Я. Бучковська, І. Каленюк, А. Касич, В. Федосов та інші. Однак, незважаючи на широкий спектр досліджень із зазначеної тематики фінансове забезпечення освіти на місцевому рівні потребує подальшого дослідження.

Метою статті є висвітлення особливостей фінансового забезпечення освіти на місцевому рівні.

Термін «фінансування» економічною наукою інтерпретується у декількох аспектах. У широкому змісті під фінансуванням розуміють будь-яке надходження із різноманітних джерел грошових коштів. У цьому випадку його обсяги залежать від результатів фінансової та господарської діяльності закладу.

У вузькому розумінні фінансування функціонує як процес забезпечення реалізації визначених цілей і завдань за допомогою грошових коштів, тобто розподіл доходів спрямовується на конкретні витрати. Для реалізації статутних цілей закладами вищої освіти повинні бути передбачені витрати на оплату праці науково-педагогічних працівників та інших співробітників закладу, придбання або оренду основних засобів (необоротних активів), забезпечення необхідними оборотними коштами і нематеріальними активами, функціонування інфраструктури (бібліотек, гуртожитків, пунктів харчування, спортивних та оздоровчих об'єктів тощо), проведення податкових, соціальних та інших виплат.

У сучасній економічній літературі поняття «фінансування» використовується дуже широко і нерідко у різних значеннях, тому єдиної думки щодо його визначення та змісту не існує. Так, проф. Каленюк І. С. стверджує, що фінансування освіти — певна система відносин по формуванню, розподілу та використанню різних фінансових ресурсів в освітній сфері. На її думку, під фінансуванням слід розуміти різноманітні фонди фінансових ресурсів, що утворюються завдяки взаємодії різних ланок управління вищої освіти і забезпечують функціонування закладів освіти [2].

Відповідно до статті 78 Закону України «Про освіту» держава забезпечує асигнування на освіту в розмірі не менше ніж 7 відсотків валового внутрішнього продукту за рахунок коштів державного, місцевих бюджетів та інших джерел фінансування, не заборонених законодавством [4].

Основним документом, який регулює нормативно-правове забезпечення фінансування освіти на місцевому рівні є Бюджетний кодекс України. Згідно Бюджетного кодексу України відбувається фінансування освіти за рахунок бюджетів міст, бюджетів обласного значення, районних бюджетів, бюджетів об’єднаних територіальних громад, що створюються згідно із законом та перспективним планом формування територій громад, а саме на [1] :

а) дошкільну освіту;

б) загальну середню освіту:

– початкові школи, гімназії, ліцеї (у тому числі з дошкільними підрозділами (відділеннями, групами);

– міжшкільні ресурсні центри;

– спеціалізовані мистецькі школи (школи-інтернати), школи-інтернати (ліцеї-інтернати) спортивного профілю, військові (військово-морські) ліцеї, ліцеї з посиленою військово-фізичною підготовкою, наукові ліцеї, наукові ліцеї-інтернати, гімназії та ліцеї, у складі яких є інтернати з частковим або повним утриманням учнів;

– дитячі будинки, навчально-реабілітаційні центри (якщо не менше 70 відсотків кількості учнів дитячих будинків, навчально-реабілітаційних центрів припадає на територію відповідного міста, району чи об’єднаної територіальної громади), інклюзивно-ресурсні центри;

в) фахову передвищу освіту (на оплату послуг з підготовки фахівців на умовах регіонального замовлення у закладах фахової передвищої освіти комунальної власності, засновником яких є міська, районна, сільська або селищна рада);

г) інші державні освітні програми;

ґ) вищу освіту (на оплату послуг з підготовки фахівців, наукових та науково-педагогічних кадрів на умовах регіонального замовлення у закладах вищої освіти комунальної власності, засновником яких є міська, районна, сільська або селищна рада);

ґ) післядипломну освіту (на оплату послуг з підвищення кваліфікації та перепідготовки кадрів на умовах регіонального замовлення);

д) позашкільну освіту;

е) професійну (професійно-технічну) освіту з бюджетів міст обласного значення - обласних центрів та бюджетів об’єднаних територіальних громад, у складі яких є місто обласного значення - обласний центр (на оплату послуг з підготовки кадрів на умовах регіонального замовлення у закладах професійної (професійно-технічної) освіти та інших

закладах освіти державної та/або комунальної власності, які розташовані на території зазначених міст).

За рахунок власних коштів місцевих бюджетів фінансуються переважно дошкільна та загальна середня освіта. Джерелами фінансування закладу дошкільної освіти незалежно від форми власності можуть бути кошти: засновника (засновників); державного та місцевих бюджетів; батьків або осіб, які їх замінюють; добровільні пожертвування та цільові внески фізичних і юридичних осіб; інші кошти, не заборонені законодавством [5].

Фінансування закладів загальної середньої освіти здійснюється з державного та місцевих бюджетів та інших джерел, не заборонених законодавством. Іншими джерелами фінансування закладів загальної середньої освіти можуть бути: доходи від надання платних освітніх та інших послуг; благодійна допомога відповідно до законодавства про благодійну діяльність та благодійні організації; гранти. Фінансування здобуття повної загальної середньої освіти за рахунок коштів державного бюджету в комунальних закладах освіти здійснюється шляхом надання освітньої субвенції та інших трансфертів з державного бюджету місцевим бюджетам. Кошти інших трансфертів з державного бюджету місцевим бюджетам на загальну середню освіту можуть спрямовуватися на підвищення кваліфікації педагогічних працівників, забезпечення учнів та педагогічних працівників підручниками (посібниками), навчальним обладнанням, засобами навчання та на інші цілі, визначені законодавством [6]. Починаючи з 2017 року, освітня субвенція спрямовується винятково на оплату праці з нарахуваннями педагогічним працівникам. Вона розподіляється між місцевими бюджетами на основі формули, в основу якої закладено дані про кількість здобувачів освіти на певній території та розрахункова наповнюваність класів, що визначається нормативно. Формульний підхід стимулює органи місцевого самоврядування до оптимізації мережі малокомплектних шкіл, оскільки за фактичної наповнюваності класів, що є меншою за розрахункову, місцева влада має додавати кошти на видатки з оплати праці із місцевого бюджету. Обсяг коштів освітньої субвенції зріс з 44,8 млрд. грн. у 2016 році до 69,6 млрд. грн. у 2019 році. Із 2018 року Урядом запроваджено субвенцію з державного бюджету місцевим бюджетам на забезпечення якісної, сучасної та доступної загальної середньої освіти «Нова українська школа», яка включає видатки споживання (підвищення кваліфікації вчителів) та видатки розвитку (закупівлю дидактичних матеріалів, музичних інструментів, сучасних меблів, комп'ютерного обладнання, відповідного мультимедійного контенту для початкових класів). Загальний обсяг субвенції з державного бюджету місцевим бюджетам на забезпечення якісної, сучасної та доступної загальної середньої освіти «Нова українська школа» у 2018 році склав 1 083 млн. грн., у 2019 році плановий обсяг субвенції становить 1 215 млн. грн. У 2019 році започатковано нову субвенцію з державного бюджету місцевим бюджетам на реалізацію заходів, спрямованих на підвищення якості освіти – 1,5 млрд. грн. [3].

Таким чином, актуальними питаннями удосконалення формули розподілу обсягу освітньої субвенції є [3] :

– урахування реального контингенту учнів станом на 1 вересня року, що передує плановому бюджетному періоду (замість року, що передує поточному бюджетному періоду);

– урахування годин індивідуального навчання;

– передбачення видатків на заміну тимчасово відсутніх працівників;

– урахування реальної потреби на оплату праці вихователів груп подовженого дня та фахівців дистанційної освіти.

Список літератури

1. Бюджетний кодекс України: Закон України від 8 липня 2010 року № 2456-VI. URL: http://zakon.rada.gov.ua/laws/show/2456-17
2. Каленюк І. С. Економіка освіти: навч. посіб. Київ: Знання, 2003. 316 с.
3. Освітня реформа: результати та перспективи. Інформаційно – аналітичний збірник. Київ, 2019. URL: https://mon.gov.ua/storage/app/media/Serpneva%20conferentcia/2019/Presentacii/Institut-zbirnik.pdf

4. Про освіту: Закон України від 05.09.2017 р. № 2145-VIII URL: http://zakon.rada.gov.ua/laws/show/2145-19
5. Про дошкільну освіту: Закон України від 11.07.2001 № 2628-III. URL: http://zakon.rada.gov.ua/laws/show/2628-14
6. Про повну загальну середню освіту: Закон України від 16.01.2020 № 463-IX. URL: http://zakon.rada.gov.ua/laws/show/463-20

УДК 336.717

В. Прокоф'єва, магістр гр. ФС-18М(1,9)
Центральноукраїнський національний технічний університет

ТЕОРЕТИЧНІ ПІДХОДИ ДО ВИЗНАЧЕННЯ СУТНОСТІ ТА СКЛАДУ ФІНАНСОВОГО ПОТЕНЦІАЛУ БАНКУ

У статті було розглянуто підходи до визначення сутності фінансового потенціалу банку та визначено його характерні риси. На основі сформованої матриці характерних рис поняття встановлено, що більшість трактувань не базується на системному підході та не враховує якості системи управління і умови діяльності, що дало можливість сформулювати уточнене комплексне поняття фінансового потенціалу банку. Проаналізовано і визначено склад фінансового потенціалу банку за функціональною спрямованістю, за ступенем реалізації, за періодом реалізації – фінансовий потенціал залучення, фінансовий потенціал розміщення та фінансовий потенціал відтворення фінансових ресурсів

фінансовий потенціал, банк, фінансові ресурси, оцінювання, реалізація фінансового потенціалу, залучення, розміщення

Постановка проблеми. Сьогодні банківська система України перебуває в процесі реформування. У ситуації реформування банківської системи країни відбувається не лише зменшення кількості банківських установ, а також відкриваються можливості їх розширення і розвитку. До того ж, з огляду на обмеженість капіталу та підвищені ризики, важливим являється достовірне і раціональне оцінювання фінансового потенціалу банку як орієнтира задля подальшої діяльності, оскільки якраз від нього залежить якість ухвалення управлінських рішень та стабільність здійснення фінансової діяльності.

Аналіз останніх досліджень і публікацій. Потенціал та його окремі види в економіці досліджували В. Г. Боронос, О. В. Васюренко, В. М. Гриньова, Н. Б. Демчишак, Р. С. Квасницька, С. М. Козьменко, С. С. Шумська. Питанням аналізу та оцінювання потенціалу банків і банківської системи присвячені дослідження А. О. Єпіфанова, О. О. Комліченко, С. В. Лєонова, О. В. Портної, Ж. І. Торяник, О. В. Шиндер. Проблеми фінансового потенціалу банку досліджувались у роботах В. Я. Вовк, А. М. Герасимовича, І. С. Кирилейзи, О. М. Колодізєва, Я. М. Кривич. Дослідження потенціалу, зокрема потенціалу банку, серед зарубіжних вчених представлені в роботах A. N. Berger, J. A. Bikker, J. C. Paradi, D. A. Grigorian

Проте незважаючи на велику кількість наукових робіт із питань дослідження потенціалу і зокрема фінансового потенціалу, слід відмітити, що не досить висвітленими являються питання комплексного підходу щодо визначення сутності та складу фінансового потенціалу банку, розгляд яких закладає фундамент для подальшого його оцінювання як такого, який охоплює головні напрямки фінансової діяльності банку в їх нерозривному зв'язку.

Формулювання мети статті. Метою статті є розгляд та узагальнення підходів щодо визначення сутності фінансового потенціалу банку, а також визначення на цій основі його складу.

Виклад основного матеріалу. В сучасних умовах визначальною особливістю економічного розвитку є зростання впливу глобалізаційних процесів на абсолютно всі сфери життя суспільства. Головне місце у фінансово-кредитному секторі економіки України займає банківська система, яка забезпечує перетікання коштів між різними секторами економіки, що суттєво впливає на економічний розвиток країни. Трансформаційні процеси світового та національного розвитку віддзеркалюють посилення фінансової глобалізації та наростаючу активізацію руху різноманітних видів та форм фінансових ресурсів.

Залучення до економіки фінансових ресурсів відбувається за безпосередньої участі фінансових посередників, до яких відносяться зокрема і банківські установи. Нестабільність економічної ситуації в Україні та посилення конкурентної боротьби на ринку банківських послуг вимушує банки використовувати нові підходи для підвищення продуктивності та ефективності своєї діяльності, створювати новітні банківські продукти та запроваджувати зміни технологій здійснення банківської діяльності. В таких умовах наявність належного фінансового потенціалу є запорукою прибуткової та сталої банківської діяльності.

Для подальшого дослідження необхідним є аналіз трактувань дефініції «фінансовий потенціал банку» і формування обґрунтованого її визначення, на основі якого буде сформовано склад фінансового потенціалу банку.

Для формування повного розуміння поняття фінансового потенціалу на мікрорівні проаналізуємо його визначення, представлені в економічній літературі (табл. 1).

Таблиця 1 – Визначення поняття «фінансовий потенціал» фінансової установи

Джерело	Визначення	Підхід
1	2	3
Кривич Я. [1]	Сукупність усіх грошових коштів банку, що перебувають у його безпосередньому розпорядженні, і коштів, які можуть бути потенційно залучені банком унаслідок проведення ефективної повномасштабної банківської діяльності, або прирощені чи втрачено в разі проведення активних операцій.	Ресурсний
Базилевич В. [2, с. 563]	Сукупність фінансових ресурсів, що перебуває в господарському обороті для забезпечення проведення операцій та здійснення інвестиційної діяльності.	Ресурсний
Вольська С. [3]	Наявність ресурсів у даний період часу, можливості їх подальшого формування та забезпечення ефективного руху банківських ресурсів у перспективі.	Об’єднаний
Герасимович А. [4, с. 181]	Фінансовий потенціал комерційного банку характеризується обсягом і структурою його необоротних та оборотних активів, що формуються за рахунок готівкових фінансових ресурсів	Об’єднаний
Вовк В., Вядрова Н. [5]	Сукупність усіх наявних фінансових ресурсів, що є в безпосередньому розпорядженні банку, і ресурсів, які можуть бути потенційно залучені у процесі проведення банківської діяльності в майбутньому для формування та нарощення сукупних активів і забезпечення ефективного функціонування та сталого розвитку в довгостроковій перспективі.	Ресурсний
Кирилейза І. [6]	Комплекс фінансових ресурсів та компетенцій, що є в розпорядженні банку та використовуються ним з метою забезпечення у майбутньому належного рівня фінансової стійкості, платоспроможності, ліквідності та інших показників фінансового стану.	Об’єднаний

Аналіз визначень поняття фінансовий потенціал фінансової установи засвідчив, що стосовно саме фінансових установ переважає об'єднаний та ресурсний підходи до трактування фінансового потенціалу, які є не такими складними як процесний та системний з точки зору оцінювання.

Це свідчить як про складність процесу оцінювання, так і вказує на відставання розвитку теорії фінансового потенціалу фінансових установ від практичних та теоретичних розробок в сфері оцінювання і аналізу потенціалу виробничих підприємств.

Результати дослідження дефініції «фінансовий потенціал» фінансової установи дали можливість виокремити такі характерні риси дефініції «фінансовий потенціал» фінансової установи, і зокрема банку:

базування на сукупності фінансових ресурсів (ті, що є в наявності, і ті, що можуть бути мобілізовані);

поєднання в своєму складі прихованих та наявних (використаних і невикористаних) можливостей;

віддзеркалення фінансової діяльності; направлення на досягнення мети; віддзеркалення максимуму, границі можливостей;

існування динамічного характеру, розвитку, направленість на майбутнє;

залежність від визначеної системи управління і умов діяльності фінансової установи.

Задля визначення ступеня урахування характерних рис було проаналізовано визначення дефініції «фінансовий потенціал» фінансової установи [1-6]. Результати аналізу представлено в табл. 2.

Таблиця 2 – Матриця врахування характерних рис фінансового потенціалу в визначеннях поняття «фінансовий потенціал» фінансової установи

Автор	Характерні риси поняття «фінансовий потенціал»									
	Внутрішня структура		Ресурси	Можливості, спроможності компетенції	Характеристика діяльності	Мета, спрямованість на результат	Максимум, межа можливостей	Система управління	Динамічність, розвиток, перспектива	Умови діяльності
	Система	Сукупність								
Кривич Я.М.				-		-			-	
Вовк В.Я., Вядрова Н.Г.				-		+			+	
Вольська С.П.				+		-			+	
Базилевич В.Д.				-		-			-	
Герасимович А.М.				-		-			-	
Кирилейза І.С.				-		+			-	
Частота врахування характерної риси у визначеннях				1		2			2	

Отже, з табл. 2 видно, що у жодному з розглянутих визначень не враховуються всі характерні риси поняття «фінансовий потенціал», окрім того ні одне визначення не базується на системному підході та не враховує якості системи управління і умови діяльності, що наявні у визначеннях фінансового потенціалу підприємства.

Тобто, за результатами здійсненого аналізу, визначених характерних рис фінансового потенціалу фінансової установи, виходячи з необхідності визначення уточненого комплексного поняття фінансового потенціалу банку, пропонуємо сформулювати його так:

фінансовий потенціал банку – це система граничних можливостей банку стосовно залучення, розміщення та відтворення фінансових ресурсів, реалізація яких відбивається в показниках фінансової діяльності та що забезпечує досягнення цілі банку на основі ефективного менеджменту з врахуванням умов функціонування і розвитку банку.

Визначення видового складу фінансового потенціалу банку набуває особливої важливості у процесі формування теоретичних основ для наступного його оцінювання.

Дослідження складу фінансового потенціалу банку не лише уточнює сутність, а й дає додаткову інформацію, що може бути використана задля оцінювання фінансового потенціалу.

Авторами роботи [7] виокремлюються як складові фінансового потенціалу: фінансовий потенціал розвитку, фінансовий потенціал стійкості та фінансовий потенціал забезпечення, що визначають можливості проведення, результат і можливості розвитку діяльності підприємства, однак ці складові є дещо абстрактними.

А. С. Харевич при дослідженні структури економічного потенціалу зазначає, що функціональна та ресурсна складові можуть існувати лише спільно за умови доповнення одна одної [8]. Отже, відповідно із представленим визначенням фінансового потенціалу банку, потенціал характеризується можливостями залучення, розміщення і відтворення коштів (нереалізовані і реалізовані), та процесом їх реалізації. В результаті аналізу існуючих підходів до визначення структури фінансового потенціалу в наукових роботах [7, 8], у відповідності до сформованого автором визначення дефініції «фінансовий потенціал банку», склад фінансового потенціалу банку в залежності від ступеня, функціональної спрямованості і періоду реалізації представлена на рис. 1.

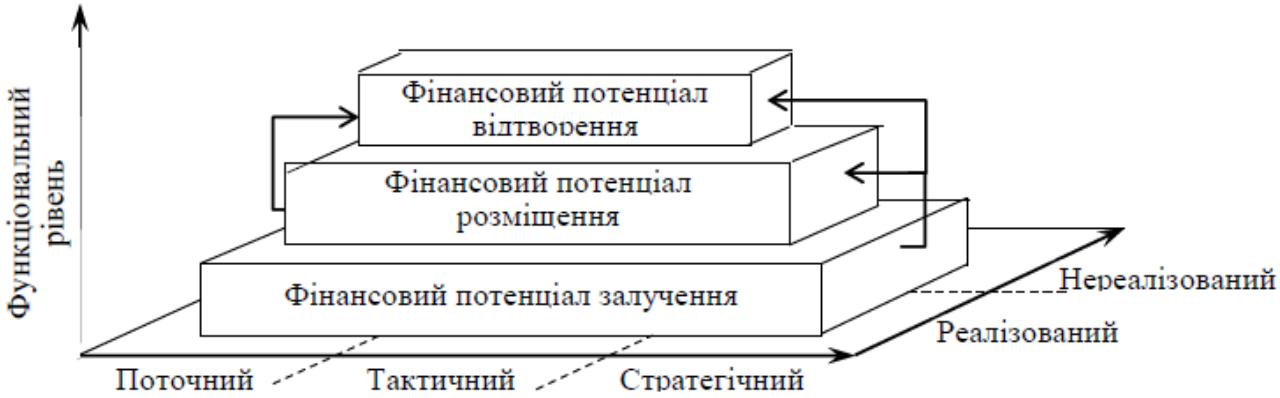


Рисунок 1 – Склад фінансового потенціалу банку

Джерело: побудовано автором за [7, 8]

Таким чином, з рис. 1 видно, що головними функціональними рівнями фінансового потенціалу банку являються такі елементи:

потенціал залучення фінансових ресурсів на ринку (нереалізований та реалізований);

потенціал розміщення залучених фінансових ресурсів;

потенціал відтворення результату фінансової діяльності банку на ринку.

На рис. 1 представлений ієрархічний триєдиний склад фінансового потенціалу банку. Причому фінансовий потенціал залучення банку виступає первинним щодо потенціалу розміщення, оскільки саме від обсягів і ефективності процесів першого залежать обсяги та відповідна процентна ставка розміщення коштів, а, відповідно, і кінцевий результат. Так само, від ступеня формування і реалізації фінансового потенціалу залучення, а також

фінансового потенціалу розміщення залежать обсяги майбутнього можливого доходу, іншими словами фінансового потенціалу відтворення.

Висновки. У представленому визначенні враховано всі характерні риси фінансового потенціалу, вказано на нероздільність можливостей щодо залучення і розміщення фінансових ресурсів від результату їх реалізації, та на взаємозалежність фінансової діяльності банку та фінансового потенціалу, реалізація якого є фундаментальною умовою досягнення цілі банку. З врахуванням динамічного та складного характеру фінансового потенціалу банку, постійного розвитку теорії потенціалу в сучасній економіці, сформоване визначення не претендує на вичерпність, однак є надважливим етапом дослідження особливостей процесу оцінювання фінансового потенціалу банку та формує його підґрунтя. На основі видової характеристики сформовано склад фінансового потенціалу банку, де виділяються головні функціональні рівні – фінансовий потенціал залучення, фінансовий потенціал розміщення та фінансовий потенціал відтворення коштів. Напрямками подальших досліджень є формування методичного підходу до оцінювання фінансового потенціалу банку.

Список літератури

1. Кривич Я. М. Фінансовий потенціал як складова інноваційного потенціалу банку та особливості його оцінки. Збірник наукових праць Національного університету Державної податкової служби України. 2009. № 2. С. 153–161.
2. Базилевич В. Д. Страхування: Підручник. К., 2008. 1019 с.
3. Вольська С. П. Фінансова стійкість банку та механізми її забезпечення: автореф. дис. на здобуття наук. ступеня канд. екон. наук : спец. 08.00.08 – гроші, фінанси і кредит. Київ : КНЕУ ім. В. Гетьмана, 2011. 18 с.
4. Герасимович А. М. Аналіз банківської діяльності: Підручник. К., 2010. 599 с.
5. Вовк В. Я., Вядрова Н. Г. Аналіз фінансового потенціалу вітчизняних банків в умовах фінансово-економічної кризи. Вісник Університету банківської справи Національного банку України. 2012. № 3 (15). С. 149–152.
6. Кирилейза І. С. Теоретичні аспекти дослідження економічної сутності ресурсної бази банку. Науковий вісник Херсонського державного університету. 2013. Вип. 1. С. 90–93.
7. Кирилова Л. І., Тодорова Д. Д. Фінансовий потенціал підприємства та його складові. Сталий розвиток економіки. 2012. № 11. С. 298–302.
8. Харевич А. С. Кредитний потенціал банківської системи: теоретико-методологічні аспекти URL: http://www.nayca.com.ua/?op=18z=1398 (дата звернення 02.02.2020).

ЗМІСТ