МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ЦЕНТРАЛЬНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

Збірник праць молодих науковців ЦНТУ

Випуск 11

Кропивницький – 2021

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ЦЕНТРАЛЬНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

Збірник праць молодих науковців ЦНТУ

Випуск 11

Кропивницький – 2021

Збірник праць молодих науковців ЦНТУ. – Вип. 11. – Кропивницький: ЦНТУ, 2021 – 485 с.

Збірник праць молодих науковців складається зі змісту, статей та тез здобувачів вищої освіти по матеріалам дипломних робіт.

Рекомендовано до друку Науково-технічною радою Центральноукраїнського національного технічного університету, протокол № 6 від 14.06.2021

Автори опублікованих матеріалів несуть відповідальність за підбір і точність наведених фактів, цитат, економіко-статистичних даних, власних імен та інших відомостей, а також за те, що матеріали не містять дані, які не підлягають відкритій публікації. Друкується в оригіналі згідно поданих робіт.

УДК 004

В. Берладін, магістр гр. КІ-19М-1,4
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ КЕРУВАННЯ РОЗПОДІЛЕНОЮ СЗД ЗА ДОПОМОГОЮ СПЕЦИФІКАЦІЇ NVME OVER FABRICS

У статті розроблено програмне забезпечення, яке призначено для системи керування розподіленою СЗД за допомогою специфікації NVMe over Fabrics. Метою розробки є дослідження та програмна реалізація системи керування розподіленою СЗД за допомогою специфікації NVMe over Fabrics. Об'єктом дослідження є процес керування розподіленою СЗД за допомогою специфікації NVMe over Fabrics. Предметом дослідження є методи керування розподіленою СЗД за допомогою специфікації NVMe over Fabrics. Методи дослідження базуються на методах Big Data, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи керування розподіленою СЗД за допомогою специфікації NVMe over Fabrics. 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 зберігання даних, NVMe over Fabrics

Постановка проблеми. Майбутнє належить флеш-накопичувачам NVMe: уже зараз вони здатні забезпечити набагато більше високі швидкості передачі даних і при цьому порівняно недорогі. А специфікація NVMe over Fabrics відкриває шлях до створення розподілених систем зберігання даних (СЗД) із низьколатентною фабрикою. Ще в 2011 році була висунута ідея про те, що для роботи із твердотільними накопичувачами потрібний окремий протокол. Спеціально створена галузева група зайнялася стандартизацією функцій, регістрів і набору команд нового протоколу, що одержав назву Non-Volatile Memory Express (NVMe). Якщо відомі протоколи SAS і SATA споконвічно призначалися для механічних пристроїв зберігання даних, то NVMe розроблявся саме для твердотільних накопичувачів NAND. Його поява стала логічним наслідком значно більше високої продуктивності флеш-накопичувачів. NVMe – протокол для доступу до енергонезалежної пам'яті. Він створювався як один із протоколів для високошвидкісного підключення флеш-накопичувача через шину PCI Express. При її використанні колишній стек на основі SCSI не міг ефективно справлятися з операціями вводу-виводу: занадто багато переривань, тисячі інструкцій центрального процесора на блок даних. Було потрібно не тільки рішення, що дозволило б помітно скоротити число переривань, визволивши процесорні цикли для продуктивної роботи, але й метод передачі даних, що дозволяє по можливості взагалі обійтися без допомоги процесора.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи керування розподіленою СЗД за допомогою специфікації NVMe over Fabrics.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи керування розподіленою СЗД за допомогою специфікації NVMe over Fabrics. Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

Огляд існуючих систем керування розподіленою СЗД за допомогою специфікації NVMe over Fabrics.

Дослідження системи керування розподіленою СЗД за допомогою специфікації NVMe

over Fabrics.

Програмна реалізація системи керування розподіленою СЗД за допомогою специфікації NVMe over Fabrics.

Об’єктом дослідження є процес керування розподіленою СЗД за допомогою специфікації NVMe over Fabrics.

Предметом дослідження є методи керування розподіленою СЗД за допомогою специфікації NVMe over Fabrics.

Методи дослідження базуються на методах Big Data, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Уже протягом майже 15 років ми підключаємо накопичувачі до ПК через SATA – невелике універсальне 7-контактне рознімання, що є й у ноутбуках, і в десктопних комп'ютерах. Перша ревізія, SATA 1, з'явилася в 2003 році й забезпечувала швидкості до 150 МБ/с – цього більш ніж вистачало для підключення жорстких дисків (та й зараз вистачає), про SSD тоді ніхто ще не чув. У середині нульових стали з'являтися перші користувальницькі SSD. Вони були дорогими й малоємними (16-64 ГБ), але вже мали швидкості вище 150 МБ/с, так що з'явилася друга ревізія SATA, що могла працювати зі швидкостями до 300 МБ/с. Однак і цього незабаром стало мало, і в 2008 році з'явилася третя ревізія SATA зі швидкостями вже до 600 МБ/с. При цьому ми живемо в той час, коли продуктивність навіть найдешевших SSD упирається вже не у швидкість чипів, а в пропускну здатність інтерфейсу: майже всі сучасні SSD мають швидкості читання більше 500 МБ/с, тобто проблема вже в самому інтерфейсі. І останнім часом все більше число SSD стали виходити з підтримкою протоколу NVMe, що поки ще не стримує швидкості навіть кращих SSD – а вони становлять до 3 ГБ/с!

Історія появи NVMe

Ідея підключення SSD через шину PCI Express з'явилася й до NVMe, але проблема була в тім, що це були закриті протоколи – а вони найчастіше мали недоробки, що приводили до втрати швидкості. До того ж ціна таких рішень була надзвичайної, і багато хто не розуміли, навіщо за них переплачувати, якщо й звичайних жорстких дисках вистачало з лишком. Але у великих корпораціях розуміли, що за SSD – майбутнє, і от, в 2007 році, за підтримкою Intel був представлений новий інтерфейс – NVMCHI (Non-Volatile Memory Host Controller Interface). Його доробкою займалися цілих 4 роки, і перша версія NVMe вийшла тільки в 2011 році, однак серйозного поширення не одержала: по-перше, тоді SSD усе ще були долею або MacBook, або 2.5 ультрабуків, або топових ігрових комп'ютерів. Більшість користувачів сиділи на Windows 7 з жорсткими дисками й радувалися життю – тобто SSD були в принципі не потрібні, і головне – украй дороги. По-друге, навіть те невелике число користувальницьких моделей SSD мало швидкості відчутно менше 600 МБ/с, тобто NVMe з його декількома гігабайтами в секунду був не потрібний. І по-третє – в інтерфейсу була безліч дитячих хвороб: так, не можна було обновити прошивання такого SSD з його самого, не було розширеного керування живленням, були проблеми при підключенні відразу декількох таких SSD. Зрозуміло, все це було виправлено в нових ревізіях, і NVMe 1.2 від 2014 року був уже цілком працездатний. Плюс на той час уже були SSD, яким 600 МБ/с було обмаль, так що новий інтерфейс став досить активно розвиватися.

Технічні характеристики й відмінність від AHCI

SATA був лише фізичним інтерфейсом, за логічну частину відповідав AHCI (Advanced Host Controller Interface), що як з'явився разом з SATA 1 в 2003 році, так і не мінявся. Розроблявся він для жорстких дисків, і тому з SSD працював не дуже добре – на одному каналі (а на одне SATA-пристрій і був один канал) могла виконуватися лише одна команда. У випадку з жорсткими дисками проблем не було – головка диска в один момент часу фізично могла одержати доступ до одного осередку. Але от з SSD це не так, і тому така робота викликала істотні простої.

NVMe же споконвічно розроблявся для саме для твердотільних накопичувачів, і отут робився упор на найменші затримки й на паралельний доступ.

Таблиця 1 – Загальна порівняльна таблиця

Параметр	AHCI	NVMe
Максимальна глибина черги запитів	Одна черга, до 32 команд у черзі	65 536 черг до 65 536 команд у кожній черзі
Некешуєммі доступи до регістрів (2 000 циклів кожний)	Шість на команди позачергово; дев'ять на команди черги	Два на команду
MSI-X і керування перериваннями	Одне переривання, керування відсутнє	2 048 переривань, переданих повідомленнями або MSI-X (Message Signaled Interrupt Extended)
Багатопоточність і паралелізм	Потрібна фіксація синхронізації для видачі команди	Не потрібно
Ефективність для команд 4 Кбайт	Параметри команди вимагають два серійних запити DRAM	Всі параметри виходять в одному 64-байтному запиті

Як видно, NVMe краще у всім – до 64К черг, тобто навантаження розпаралелюється. Так само є можливість керування перериваннями, тобто при настанні пріоритетного завдання NVMe SSD почне неї виконувати швидше. Також серйозно нижче затримка при виконанні команд: у випадку з AHCI це 2 запити DRAM, тобто навіть із DDR4 це порядку 100-150 нс – менше час відповіді в SATA SSD бути не може. У випадку ж з NVMe запит тільки один, що дозволяє зменшити затримки вдвічі. Ну й самої головне – швидкості: NVMe SSD підключаються через PCI Express 3.0 x4, що в теорії забезпечує швидкість до 3.2 ГБ/с – до 5 разів швидше, ніж SATA SSD.

Форм-фактори NVMe SSD

Традиційно ці SSD підключаються як плати розширення PCI Express – тобто використовуються ті ж слоти, що й для відеокарт. Однак такий тип підключення усе більше сходить на немає: по-перше, усе більше користувачів переходить на ноутбуки, де повноцінного PCIe бути не може. По-друге, на ринку усе більше компактних материнських плат, де слотів PCIe або 1, або 2, але через «товсті» відеокарти другий найчастіше буває перекритий, а перший майже завжди зайнятий відео картою.

Другий форм-фактор це U.2. Звичайному користувачеві він мало цікавий, тому що використовується на серверах, має можливість «гарячої» заміни й менші (у порівнянні із платами розширення PCIe) розміри:

Ну й самий компактний і найбільш розвиваючийся форм-фактор це M.2 – його активно використовують у ноутбуках, а починаючи з 100ой лінійки чипсетів від Intel він став з'являтися вже й на материнських платах. Однак потрібно бути обережним: у цьому форм-факторі є й SATA SSD, і як їх відрізнити – можна почитати в цій статті:

Доцільність покупки NVMe SSD

На даний момент ціни на NVMe SSD досить сильно впали, і вже близькі до цін на звичайні SSD. Тому, зрозуміло, виникає питання – а є чи зміст їх брати? Для того, щоб відповісти на це питання, потрібно подивитися на встановлене у вашім пристрої «залізо»:

На пристрої немає M.2 слотів або вони підтримують тільки SATA. Якщо у вас ноутбук – то нічого зробити не можна, користуйтеся SATA. І, загалом кажучи, раз виробник не став робити M.2 слот, те це банально не потрібно – усе впреться в продуктивність процесора, і виграш від швидкого SSD не відчувався б. Якщо ж у вас ПК, і є вільний слот PCIe – все вже залежить від вас: якщо у вас стоїть потужний процесор (Core i5, i7), материнська плата підтримує NMVe, і ви часто працюєте з масивами даних – варто задуматися про покупку NVMe SSD, він може серйозно прискорити роботу. Ну а якщо у вас слабкий процесор (Core i3, Pentium), або материнська плата вийшла до 2011 року – ніякого

змісту в покупці NVMe ні, рада той же, що й з ноутбуком – користуйтеся SATA SSD, вам його заочі вистачить.

На пристрої є M.2 слот, що підтримує NVMe. Якщо у вас ноутбук – те, швидше за все, він ставиться до верхнього цінового сегмента, і в цьому розніманні вже коштує SSD (і, можливо, є другий диск – HDD). Більше того – у вас швидше за все й вибору-те немає: у дорогих ноутбуках звичайно один-два слота M.2 і один повнорозмірний SATA, але він уже зайнятий HDD, так що вам доведеться брати NVMe SSD. Якщо ж ви збираєте ПК, і на материнській платі є M.2 слот – все залежить від процесора: якщо у вас топовий i5 або i7, то варто переплатити й взяти NVMe SSD. Якщо ж у вас Pentium або i3 – змісти в цьому ні, швидше за все у вас і так складання бюджетна, і зайву тисячу гривень краще витратити на більший обсяг ОЗУ або могутнішу відеокарту, чим на більше швидкий SSD, що у найкращому разі прискорить завантаження системи на півсекунди.

У підсумку все вертається на круги свої: старий AHCI як був розрахований для SATA HDD, так з ним тепер в основному й використовується. Ну а розрахований для SSD NVMe усе більше набирає оберти, і, швидше за все, незабаром уже всі SSD будуть підтримувати тільки його.

Розробка структурної схеми

Протокол NVMe швидко розвивався в контексті рішення наступних проблем. NVMe – протокол для доступу до енергонезалежної пам'яті створювався як один із протоколів для високошвидкісного підключення флеш-накопичувача через шину PCI Express. При її використанні колишній стек на основі SCSI не міг ефективно справлятися з операціями вводу-виводу: занадто багато переривань, тисячі інструкцій центрального процесора на блок даних. Було потрібно не тільки рішення, що дозволило б помітно скоротити число переривань, визволивши процесорні цикли для продуктивної роботи, але й метод передачі даних, що дозволяє по можливості взагалі обійтися без допомоги процесора.

Прямий доступ до пам'яті по шині PCIe застосовувався як перевірений метод переміщення даних. Механізм передачі даних push, при якому потрібні передача запитів і одержання підтверджень, був змінений на pull, щоб приймаючий вузол міг одержувати дані в міру готовності. При такому підході навантаження на процесор знижується на кілька відсотків. Замість системи переривань стали використовувати метод черг, де один набір черг призначався для команд, що очікують передачі, а іншої – для статусів завершення операцій.

До числа недоліків протоколів SAS / SATA / Fibre Channel ставиться відсутність пріоритетів і ідентифікації відправників. В NVMe підтримується до 64 тис. черг, кожна з яких ідентифікує й відправника, і пріоритет. Це дозволяє, наприклад, передавати дані в конкретний додаток. Схема адресації стає ще більш розвиненою у розширенні протоколу за назвою NVMe over Fabrics.

Основні принципи, закладені в основу NVMe, – стандартизація й відхід від пропрієтарності, орієнтація на флеш-пам'ять, підтримка додатків як корпоративного, так і споживчого класу. При його створенні розроблювачі акцентували увагу на скороченні «накладних витрат» при передачі даних, зменшенні затримок і поліпшенні роботи із багатопоточними навантаженнями. Для корпоративних замовників передбачені розвинені засоби виявлення помилок, керування й шифрування.

Одне з найбільш важливих відмінностей від колишніх протоколів – підтримка значно більшої кількості черг, адже механічні пристрої в основному «однопотокові», до того ж для HDD не потрібні глибокі черги. У той же час при використанні накопичувачів NAND можлива одночасна робота з декількома мікросхемами пам'яті, що дозволяє прискорити операції читання-запису.

Якщо для «механічних» накопичувачів затримка при виконанні команд становить близько 2 мс, то використання флеш-пам'яті дозволяє скоротити цей час приблизно до 100 мкс. У результаті переходу з контролера SATA на спеціалізований програмний інтерфейс «накладні витрати» зменшуються до 5 мкс. Ефект підсилюється внаслідок загального збільшення пропускної здатності інтерфейсу при підключенні SSD по PCIe

Контролер NVMe є частиною накопичувача, а сам накопичувач підключається як пристрій PCI Express. Завдяки збільшеній кількості черг і команд в NVMe забезпечується високий ступінь паралелізму, і в результаті підвищується ефективність роботи із сучасними багатоядерними процесорами. Завдяки «легковагості» протоколу знижуються затримки при роботі із флеш-пам'яттю, а драйвери виходять «легенями».

NVMe дає набагато кращі результати в порівнянні з існуючими дисковими протоколами й може використовуватися як протокол серверної флеш-пам'яті PCIe.

Пристрої NVMe

Історія пристроїв NVMe почалася не дуже давно – в 2015 році, коли для завдань із важкими навантаженнями були випущені карти флеш-пам'яті з підтримкою NVMe. В 2016-м з'явилися накопичувачі SSD форм-фактора 2,5? на шині PCI з можливістю гарячої заміни, а також компактний форм-фактор M.2. Протокол NVMe не залежить від форм-фактора накопичувача. Це означає, що він може використовуватися з SSD формату PCI Express, M.2 або SATA Express.

В 2017 році з'явилися двопортові накопичувачі (з доступом по двох шляхах PCI), а також SSD у форм-факторі вентильної матриці, програмувальної користувачем (Field-Programmable Gate Array, FPGA). Крім цього, стала доступна новий різновид пристроїв – Essential NVMe (NVMe початкового рівня для корпоративного ринку) з більше низьким (до 12 Вт) енергоспоживанням для заміни SATA SSD (по продуктивності один такий накопичувач відповідає трьом SATA SSD). Пропонуються також дискові полки з накопичувачами NVMe і підключенням до СЗД за протоколом PCI або InfiniBand.

NVMe підтримується майже всіма системними платами Intel LGA1151 і LGA2011v3, багатьма системними платами з наборами системної логіки Intel Z97/H97 і деякими моделями Intel Z87. Однак весь потенціал NVMe може бути задіяний лише в системах на LGA2011v3 з достатнім числом ліній PCIe 3.0, але не в масових LGA115x. Крім того, ніж старіше системна плата, тим менше ймовірність того, що вона підтримує NVMe.

Зараз свою продукцію на ринок поставляють чотири виробники флеш-пам'яті: Samsung, Xenix, Intel-Micron, Toshiba-SanDisk (остання випускає 40% пам'яті NAND у світі, з них 50% поставляє компанія WD). У цей час спостерігається дефіцит пам'яті NAND – дуже високий попит на SSD у виробників гаджетів і хмарних провайдерів. Ціни ростуть, строки поставок збільшуються.

У формуванні екосистеми NVMe бере участь цілий ряд вендорів, включаючи E8, Enmotus (ПЗ тиринга), Excelero, Magnotics, Mellanox, Microsemi, Microsoft (Windows Server 2016 S2D, ReFS), галузеві організації NVM Express (наприклад, nvmexpress.org), Seagate, VMware (разрабивши драйвер NVMe для vSphere ESXi) і WD/Sandisk. У міру виходу нових продуктів з підтримкою NVMe розширюються й області застосування даного протоколу.

Для чого використовується NVMe?

З розмаїтістю пристроїв NVMe розширюється й спектр розв'язуваних завдань: в 2016 році накопичувачі з підтримкою NVMe почали застосовуватися не тільки для прискорення баз даних і кешування, але й для побудови горизонтально масштабованих (scale-out) СЗД із більшим числом серверних вузлів. Крім цього, NVMe-пристрою стали використовуватися в системах віртуалізації й хмарних платформах (зараз це основні їхні споживачі).

Які ще завдання дозволяють вирішувати пристрою NVMe? Крім «прискорення хмар», це «важкі» додатки для ПК, а перспективний і важливий напрямок на поточний рік – використання модулів NVMe для розширення оперативної пам'яті, оскільки висока вартість DRAM перешкоджає нарощуванню ємності оперативної пам'яті.

Крім того, багато корпоративних завдань, такі як підтримка інфраструктури VDI, транзакційні навантаження, обчислення в пам'яті й кешування даних, вимагають довговічних і високопродуктивних твердотільних накопичувачів, розрахованих на інтенсивний запис.

За прогнозами IDC, частка накопичувачів PCIe з підтримкою NVMe у корпоративному сегменті буде рости, у споживчому NVMe теж стане витісняти SATA. Розробки IBM і Intel-Micron можуть привести до стирання границь між оперативною

пам'яттю й сховищем даних у результаті появи модулів розширення оперативної пам'яті, не таких швидких, як DRAM, але набагато більше дешевих і ємних. Це послужить поштовхом до подальшого розвитку обчислень у пам'яті й багаторазово прискорить доступ до збережених даних.

NVMe і нові типи пам'яті

Протокол NVMe є спеціалізованою розробкою, значною мірою націленої в майбутнє. Поки що NVMe використовується із пристроями, що працюють на основі флеш-пам'яті, але потенційні можливості даного протоколу розкриються ще більше при освоєнні нових стандартів енергонезалежної пам'яті з низькими затримками.

У цей час створюються різні типи енергонезалежної пам'яті – зі зміною стану, PRM і PRAM, ReRAM/CBRAM і ін. Над пам'яттю RPM працюють Intel/Micron, над ReRAM – SanDisk. В PCM (Phase Change Memory) використовуються халькогенідне скло, що міняє агрегатний стан і провідність при нагріванні (аморфне або кристалічне). На відміну від звичайного DVD, точка, що представляє одиницю інформації, має в такій пам'яті на порядок менший розмір. Залежно від величини й тривалості подачі напруги на резисторі виходить аморфна або кристалічна структура, що представляє 0 або 1.

У пам'яті ReRAM застосовується непровідний оксид металу між електродами: при подачі напруги між ними вибудовується або руйнується провідна нитка. Характеристики обох типів пам'яті схожі й близькі до оперативного, але при цьому вони майже не вимагають витрат електроенергії. Вони характеризуються малими затримками й довговічністю, що на порядки вище, ніж в NAND. NVMe зможе підтримувати й ці види пам'яті.

Високопродуктивний протокол NVMe з низькою затримкою використовується сьогодні в серверах і флеш-масивах як внутрішній протокол, однак його можна інкапсулювати в інші протоколи, такі як Ethernet, FC і InfiniBand, що дозволяє масштабувати NVMe до рівня мережі.

Накопичувачі NVMe й форм-фактор M.2

M.2 – конфігурація форм-фактора SSD, що по суті являє собою невелику карту з мініатюрним з'єднувачем. M.2 заміняє форм-фактор mSATA, значно більший по розмірі. Він краще підходить для компактних систем і систем високої щільності. Специфікація для форм-фактора SSD M.2 передбачає різні стандартні ширину й довжину. Найбільш популярний розмір – ширина 20 мм і довжина від 30 до 110 мм.

Крайовий з'єднувач на модулі M.2 вставляється в рознімання, паралельний системній платі, а гвинт на іншому кінці рознімання втримує плату на місці. Це досить просто й недорого.

Для чого можна використовувати пристрої NVMe M.2? Наприклад, у якості локального кеш-буфера читання-запису або завантажувального пристрою в серверах, що мають слоти M.2. Багато серверів і невеликі робочі станції, у тому числі Intel NUC, підтримують M.2. Крім того, на ринку є пристрої M.2 від різних постачальників, включаючи Micron і Samsung.

M.2 підтримує або чотири лінії PCIe 3.0, або одне з'єднання SATA або USB 3.0. Підтримка PCIe 4.0 зараз у стадії розробки. Цього досить для найшвидших накопичувачів SSD. Форм-фактор M.2 дозволяє одержати дуже компактні твердотільні накопичувачі, у яких немає корпуса й інших елементів SSD, що дозволяє заощадити місце й знизити вартість рішення. Малий форм-фактор SSD M.2 добре підходить для нових серверних архітектур і, як очікується, допоможе домогтися ще більшої щільності систем. У сервер 1U помістяться 12 накопичувачів M.2. Однак, хоча накопичувачі M.2 SSD менше, ніж 2, 5-5- або 3, 5-дюймові SSD, різниця в розмірах відбивається на загальній ємності пам'яті. Самий ємний накопичувач M.2 уміщає 1 Тбайт даних, але анонси 2, 5-дюймових твердотільних накопичувачів на 100 Тбайт указують на те, що й у форм-факторі M.2 в 2017-м або в 2018 році повинні з'явитися накопичувачі ємністю 10 Тбайт або вище.

Зараз накопичувач Intel M.2 NVMe ємністю 1 Тбайт коштує всього 360 доларів. Це ненабагато більше, ніж вартість SATA SSD на 960 Гбайт (250 доларів), причому

накопичувачі NVMe набагато продуктивніше. Зважаючи на те, що M.2 теж надає підтримку PCIe, у тому числі підключення до локальної мережі, можна створювати сервери з накопичувачами NVMe і портами 100 Gigabit Ethernet Remote Direct Memory Access для доступу до віддаленого сховища.

Здавалося б, з появою NVMe можна говорити про старіння інтерфейсу SAS, однак поставки накопичувачів SAS продовжують рости, і аналітики прогнозують збереження цієї тенденції, на відміну від спаду продажів пристроїв SATA. На їхню думку, збереження SATA потрібно лише для того, щоб підтримувати штучну диференціацію цін на накопичувачі NVMe і SATA.

Ціноутворення на ринку SSD набагато складніше, ніж на ринку жорстких дисків. У розрахунок доводиться брати забезпечувані затримки, IOPS і довговічність накопичувачів, а також пропускну здатність. Тим часом розходження між корпоративними і споживчими SSD розмивається, оскільки великі постачальники хмарних рішень використовують для вибору потрібних їм продуктів інші критерії. Зрештою SATA може зникнути, поступившись місцем NVMe/PCIe.

NVMe over fabrics

У цей час накопичувачі NVMe в основному заміняють пристрої зберігання з технологіями SATA і SCSI (SAS), що застосовувалися в серверах і дискових масивах, але розробляються методи підвищення швидкості доступу до NVMe у мережах зберігання й комутуючих фабрик. NVMe доповнюється специфікацією NVMe over Fabrics, що дозволяє передавати команди поверх мережних протоколів, при цьому як транспорт NVMe можна використовувати мережі Fibre Channel, Ethernet і InfiniBand.

В основі протоколу NVMe over Fabrics лежить RDMA – прямій доступ до пам'яті віддаленої системи, тому застосунки й керуюче ПЗ не розрізняють локальні й віддалені пристрої, тим більше що затримка не перевищує 10 мс.

Його особливості:

мінімальний вплив на продуктивність центрального процесора;

транзакції на основі повідомлень;

до 65К черг, комплексний захист даних;

пріоритизація виконання команд і механізм арбітражу;

багатопоточний ввод-вивід;

підтримка безлічі адресних просторів і шляхів вводу-виводу (multipath i/o).

NVMe over Fabrics – ключова технологія для побудови масштабованих флеш-масивів. Як очікується, в 2019 році почнеться масовий вивід пристроїв NVMe на ринок. За прогнозами Gartner, NVMe буде використовуватися й у якості зовнішнього мережного інтерфейсу, подібного PCIe і InfiniBand. Наприклад, цей накопичувач може бути затребуваний у невеликих спеціалізованих мережах зберігання, що складаються з десятків вузлів, або в мережних сховищах. Однак основною областю застосування NVMe залишаться внутрішні накопичувачі. Завдяки M.2 SSD з підтримкою NVMe гіперконвергентні системи можуть стати значно могутніше вже в 2019 році, одержати значну ємність зберігання й набагато більше високу пропускну здатність.

Про прийдешню смерть Fibre Channel говорять хіба що ледве менше, ніж про смерть стрічкових накопичувачів. Ще коли швидкість була обмежена 4 Гбіт, уже тоді на зміну FC ладили новомодний iSCSI (нехай осудний бюджет тільки на 1 Гбіт варіант, але 10 десь уже зовсім поруч). Час ішов, а 10Гбит ethernet залишався занадто дорогим задоволенням і до того ж не міг забезпечити низьку латентність. ISCSI як протокол спілкування серверів з дисковими системами хоч і одержав значне поширення, але повністю витиснути FC так і не зміг.

Минулі роки показали, що інфраструктура Fibre Channel продовжує активно розвиватися, швидкість інтерфейсів росте й говорити про прийдешню кончину явно передчасно. А ще навесні цього (2016) роки був анонсований стандарт Gen 6, що подвоїв максимальну швидкість із 16GFC до 32GFC. Крім традиційного збільшення продуктивності,

технологія одержала й ряд інших нововведень.

Стандарт дозволяє об'єднати 4 лінії FC в один канал 128GFC для з'єднання комутаторів один з одним через високошвидкісний ISL лінк. Корекція помилок (Forward Error Correction, FEC) уже була доступна в продуктах FC п'ятого покоління у вигляді опції, але в Gen 6 її підтримка стала обов'язкової. На настільки високих швидкостях не тільки ймовірність виникнення помилок зростає (BER для Gen 6 становить 10-6), але й ще більше зростає вплив помилок на продуктивність через необхідність перепосилки кадрів. FEC дозволяє приймаючій стороні виправляти помилки без необхідності робити повторні запити на перепосилку кадру. Як наслідок, ми одержуємо більше «рівну» швидкість передачі даних. Не залишили без уваги й енергоефективність – для зниження енергоспоживання мідні порти можуть повністю відключатися, а оптичні знижувати потужність до 60%.

Як і раніше, сильною стороною технології FC є низька латентність (яка стала ще на 70% нижче в порівнянні із широко використовуваним зараз 8 Гбіт стандартом). Саме сполучення низкою латентності й високої продуктивності робить 32GFC підходящим рішенням для підключення All-Flash масивів. На обрії вже бачимо NVMe системи, що пред'являють найвищі вимоги до інфраструктури мережі зберігання й 32GFC має всі шанси завоювати гідне місце.

Чипи FC Gen 6, адаптери й комутатор Brocade G620 минулого оголошені навесні разом із самим стандартом, а не дуже давно були анонсовані й нові директори (шасійні комутатори) сімейства Brocade X6 Director. У максимальній конфігурації (8 слотів) він підтримує до 384 портів 32GFC + 32 порту 128GFC із сумарною пропускною здатністю 16 Тбіт. Залежно від шасі можна встановити 8 або 4 лінійні карти FC 32-48 (48 портів 32GFC), або мультипротокольні карти SX6 (16 портів 32GFC, 16 портів 1/10Gb і два порти 40Gb). Леза SX6 дозволяють використовувати IP-мережі для з'єднання комутаторів. На жаль, не обійшлося без апгрейда шасі й старий-добрий DCX-8510 не можна проапгрейдити до 32GFC, зате для лінійки X6 заявлена підтримка карт Gen 7 стандарту.

Значна увага приділена не тільки апаратним можливостям, але й системі керування. Brocade Fabric Vision з технологією IO Insight дозволяє здійснювати проактивний моніторинг за всім каналом вводу-виводу, у тому числі й не тільки до фізичних серверів, але й від окремих віртуальних машин до конкретних LUN на СЗД. В умовах, коли на одній системі зберігання консолідується безліч різних додатків, аналіз продуктивності всього комплексу досить складний і збір метрик на рівні комутатора може істотно спростити пошук проблеми. Що налаштовуються попередження допомагають швидше реагувати на потенційні проблеми й не допускати деградації продуктивності ключових додатків.

Але звичайно не єдиним Fibre Channel живемо й Mellanox оголосив про вихід, що готується, сімейства чипів BlueField. Це системи на кристалі (SoC) з підтримкою NVMe over Fabric і інтегрованим контролером Connec-5. Чип підтримує Infiniband аж до швидкостей EDR (100Gb/s), а також 10/25/40/50/100Gb Ethernet. BlueField націлений на застосування як в NVMe AllFlash масивах, так і в серверах для підключення NVMe over Fabric. Очікується, що використання подібних спеціалізованих пристроїв дасть можливість збільшити ефективність серверів, що дуже важливо для HPC. Використання як мережний контролер для NVMe СЗД рятує від PCI express комутаторів і потужних процесорів. Хтось може сказати, що такі спеціалізовані пристрої йдуть врозріз із ідеологією software defined storage і використання commodity hardware. Я ж уважаю, що як тільки ми одержуємо можливість знизити ціну рішення й оптимізувати продуктивність, це і є правильний підхід.

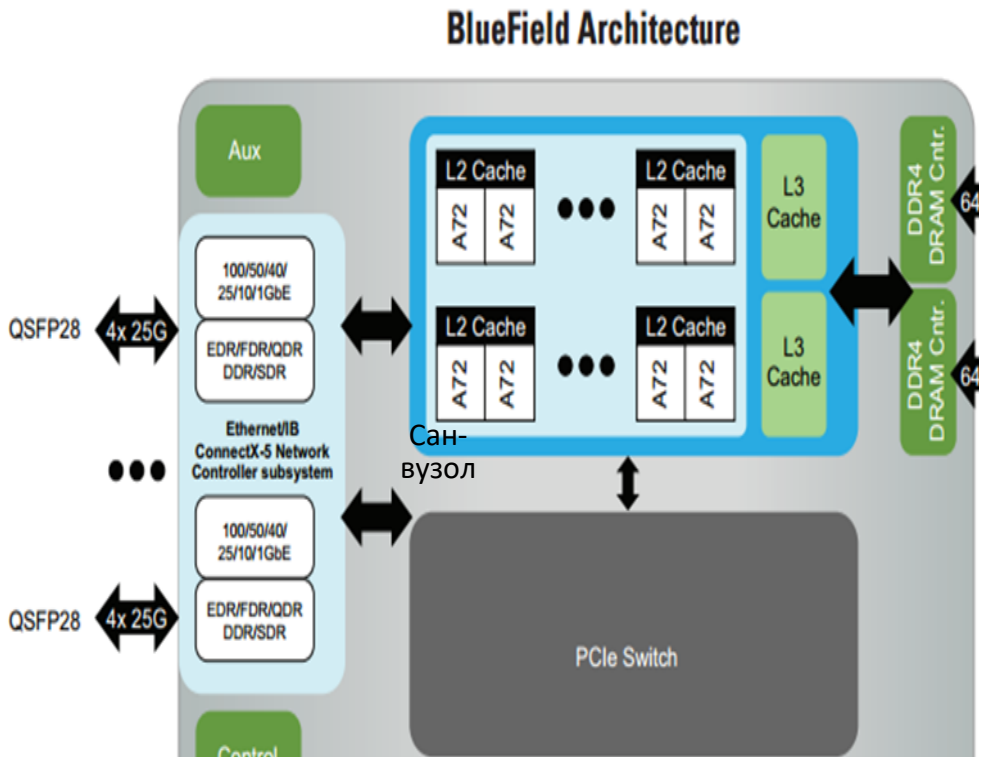


Рисунок 1 – Структурна схема системи

У найближчій перспективі кількість NVMe систем зберігання буде неухильно зростати. Підключення серверів через PCI-express комутатор хоча й забезпечує максимальну швидкість, але має цілий ряд недоліків, тому дуже до речі приспіла опублікована версія 1.0 стандарту «NVM Express over Fabrics» Як транспорт може використовуватися FC або RDMA фабрика, остання у свою чергу може бути фізично реалізована на базі Infiniband, iWARP або RoCE.

RDMA транспорт через Infiniband буде превалювати скоріше в HPC системах, а також там, де є можливість прикласти руки «самоделкіним». У цій фразі немає ніякого негатива – Fibre Channel уже багато років є визнаним корпоративним стандартом і ймовірність нарватися на проблеми набагато нижче, ніж при використанні RDMA. Це стосується як питань сумісності із широким колом прикладного ПЗ, так і простоті керування. Все це має ціну, за якої корпоративний ринок уважно стежить.

У свій час деякі виробники ладили великий успіх технології FCoE, що як дозволяє уніфікувати мережа зберігання зі звичайною мережею передачі даних, але по факті домогтися значимих успіхів по завоюванню ринку так і не вдалося. Зараз досить активно розвивається тема NVMe СЗД із підключенням до мережі Ethernet і передачі даних NVMe over Fabric через RoCE (RDMA over Converged Ethernet). Є ймовірність, що тут успіх буде більше значимим, чим із впровадженням FCoE у маси, але впевнений, що ми побачимо ще не одне покоління Fibre Channel пристроїв. І зараз дуже рано говорити про те, що «нарешті-те можна обійтися тільки ethernet» – так, часто можна, але далеко не факт, що це буде дешевше.

Сьогодні, якщо FC мережа вже розгорнута, те дуже рідко їсти зміст впроваджувати альтернативні рішення – краще провести модернізацію встаткування до Gen 6 або Gen 5 стандартів – ефект буде навіть при частковому апгрейді. Незважаючи на те, що наявна СЗД не підтримує максимальну швидкість, відновлення мережі зберігання часто дозволяє знизити латентність і збільшити інтегральну продуктивність усього комплексу.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів керування розподіленою СЗД за допомогою специфікації NVMe over Fabrics. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем керування розподіленою СЗД за допомогою специфікації NVMe over

Fabrics; Досліджена система керування розподіленою СЗД за допомогою специфікації NVMe over Fabrics; На основі отриманих результатів досліджень створена програмна реалізація системи керування розподіленою СЗД за допомогою специфікації NVMe over Fabrics. Розроблені під час виконання роботи алгоритми дозволяють успішно вирішувати завдання керування розподіленою СЗД за допомогою специфікації NVMe over Fabrics. 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. Берладін В.К. Дослідження та програмна реалізація системи керування розподіленою СЗД за допомогою специфікації NVMe over Fabrics // Збірник праць молодих науковців ЦНТУ. – Вип. 11. – Кропивницький: ЦНТУ, 2021.
2. Microsoft Corporation. Межсетевое взаимодействие. Ресурсы Microsoft Windows 2000 Server. /Пер, с англ. – М.: Издательско-торговый дом "Русская Редакция*, 2002. – 736 с.: ил,
3. 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.
4. Microsoft Corporation. Распределенные системы. Книга 1. Ресурсы Microsoft Windows 2000 Server. /Пер, с англ. – М.: Издательско-торговый дом "Русская Редакция", 2001. – 864 с.: ил.
5. 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.
6. В.Г. Олифер, Н.А. Олифер. Компьютерные сети: Принципы, технологии, протоколы.
7. Селезнев Д.А. Построение локальной компьютерной сети масштаба малого предприятия на основе сетевой OS Linux. /МГИФИ, М., – 1999.
8. 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.
9. 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.
10. Терентьев А.М. Задачи полноценного аудита корпоративных сетей. – «Концепции», N1(11), 2003, с.94-95.

УДК 004

В. Богаш, магістр гр. КН-19М-1,4
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ ІНТЕРНЕТУ РЕЧЕЙ НА БАЗІ СТАНДАРТУ IEEE 802.3BT

У статті розроблено програмне забезпечення, яке призначено для системи інтернету речей на базі стандарту IEEE 802.3bt. Метою розробки є дослідження та програмна реалізація системи інтернету речей на базі стандарту IEEE 802.3bt. Об’єктом дослідження є процес інтернету речей на базі стандарту IEEE 802.3bt. Предметом дослідження є методи інтернету речей на базі стандарту IEEE 802.3bt. Методи дослідження базуються на методах інтернету речей, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи інтернету речей на базі стандарту IEEE 802.3bt. 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, інтернет речей, IEEE 802.3bt

Постановка проблеми. Поряд зі штучним інтелектом і машинним навчанням Інтернет речей (IoT) – це ще одна технологія, що швидко розвивається. IoT з технологічної

точки зору – це, по суті, мережа мереж, що складаються з унікально ідентифікованих об'єктів (за фактом «речей»), які можуть взаємодіяти між собою через IP-підключення без втручання людини. Слід зазначити, що, вживаючи термін «IoT», ми говоримо про куди більш складне явище, ніж просто набір датчиків. Практика збору і аналізу даних про об'єкт – будь то механізм, будівля або людина, – за допомогою датчиків існує давно. Промисловий інтернет радикально відрізняється тим, що датчики об'єднуються в єдину мережу з аналітичними і / або керуючими системами. Таким чином, у об'єкта формується самостійна мережу. Усередині мережі йде обмін даними, на основі яких автоматично приймаються рішення і здійснюються дії з управління об'єктом. Так з'являються елементи штучного інтелекту і принципи саморегулювання. Нині IoT вже відноситься до мільярдам фізичних пристроїв по всьому світу, які підключені до Інтернету, аналізують і обробляють величезну кількість даних. Передбачається, що в майбутньому Інтернет-речі стануть активними учасниками бізнесу, інформаційних і соціальних процесів, де вони зможуть взаємодіяти між собою, обмінюючись інформацією про навколишнє середовище, не вимагаючи при цьому втручання людини. Завдяки процесорам і бездротових мереж в частину IoT можна перетворити що завгодно – від таблетки до літака. Це додає рівень цифрового інтелекту пристроїв, які в іншому випадку були б неактивними, дозволяючи їм спілкуватися без участі людини і злиття цифрових і фізичних світів.

У цій роботі інтернет речей буде застосований відносно розумного або, як його ще називають, інтелектуального будинку. Поняття «інтелектуальний будинок» було сформульовано в 70-і роки минулого століття: «Будинок забезпечуючий продуктивне й ефективне використання робочого простору». Варто розділяти поняття «інтелектуальний будинок» і «системи життєзабезпечення». Окремі системи мають лише необхідні інтерфейси керування й контролю. Концепція «Системи інтелектуального керування будинком» припускає новий підхід в організації життєзабезпечення будинку, при якому за рахунок комплексу програмно-апаратних засобів значно зростає ефективність функціонування й надійність керування всіх систем експлуатації й виконавчих пристроїв будинку.

Основною особливістю інтелектуального будинку є об'єднання окремих підсистем різних виробників у єдиний керований комплекс.

Під «інтелектуальним будинком» невірно розуміти прямий переклад з англійського як «мислячий будинок». Коректний переклад терміна intelligent building означає систему, що повинна вміти розпізнавати конкретні ситуації, що відбуваються в будинку, і відповідним чином на них реагувати: одна із систем може управляти поводженням інших по заздалегідь вироблених алгоритмах. Англійське слово intelligent, буквально означаюче «розумний», «тямущий», у сполученні зі словом building використано в значенні «гнучкий, що пристосовується». Будинок проектують таким чином, щоб всі системи його керування могли інтегруватися один з одним з мінімальними витратами, а їхнє обслуговування було б організоване оптимальним образом. Проект обов'язково припускає можливість нарощувати й видозмінювати конфігурації інстальованих систем.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи інтернету речей на базі стандарту IEEE 802.3bt.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи інтернету речей на базі стандарту IEEE 802.3bt.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

- Огляд існуючих систем інтернету речей на базі стандарту IEEE 802.3bt.
- Дослідження системи інтернету речей на базі стандарту IEEE 802.3bt.
- Програмна реалізація системи інтернету речей на базі стандарту IEEE 802.3bt.

Об'єктом дослідження є процес інтернету речей на базі стандарту IEEE 802.3bt.

Предметом дослідження є методи інтернету речей на базі стандарту IEEE 802.3bt.

Методи дослідження базуються на методах інтернету речей, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Сучасне житло людини, будь то котедж або міська квартира, надзвичайно складний по своїй технічній оснащеності об'єкт. Він начинений світильниками, кондиціонерами, холодильниками, вентиляційним устаткуванням, аудіо-відеотехнікою, системами відеоспостереження, охоронною сигналізація й багато чим ще. Все це вимагає постійного включення-вимикання й невсипущого контролю.

От перелік пристроїв, якими потрібно управляти:

– системи життєзабезпечення (електрика, газ, водопровід, опалення, освітлення);
– інформаційні системи (телефон, Internet, супутникове й кабельне телебачення);
– пристрою забезпечення безпеки (у тому числі й пожежної) і охорони;
– аудіо-відеосистеми, домашній кінотеатр та інші компоненти культурно-дозвільного комплексу.

Зібрати в ціле й додати системі завершеність у вигляді загального пульта керування – це і є завдання побудови Системи керування будинку. Система повинна жити як єдиний організм, що реагує на зміни зовнішніх і внутрішніх факторів. Ваші обов'язки по керуванню домашньою технікою будуть перекладені на мікропроцесорний контролер (або кілька контролерів). Можливості, які дає ця система безмежні.

Керування освітлювальними приладами

Це одна із самих корисних сторін Системи керування будинку. Спеціальні пристрої плавно регулюють освітленість вашого житла в різних кімнатах. Це можна робити вручну, а можна встановити датчик рівня освітленості. Якщо за вікнами стане темніти, то прилад подасть сигнал лампі, що негайно ввімкнеться. Якщо ж, навпроти, сонце піднялося, а ви не замовляли яскраве освітлення, то по команді датчика плавно закриються жалюзі. Вони ж регулюють розжарення ламп, що істотно заощаджує електроенергію.

При бажанні можна не тільки управляти рівнем освітленості різних кімнат, але й створювати особливе світлове оформлення усередині однієї з них, залежно від ситуації – на випадок романтичного побачення, наприклад. І не тільки усередині – при бажанні таке чутливе освітлення можна встановити й навколо будинку.

Останній писк – датчики руху. На їхній основі досить легко організувати автоматичний супровід світлом людини, що йде по будинку.

Системи клімат-контролю

Системи кліматичного контролю регулюють температуру й вологість у приміщенні, відповідають за роботу кондиціонерів і опалювальних приладів. Мікроклімат буде підтримуватися по заданій вами програмі. Ви також можете управляти температурою в будинку за допомогою кімнатного терморегулятора. Крім створення ідеальних температурних умов для життя, це також дозволяє заощадити на електриці.

Керування охороною й пожежною сигналізацією

Організація охорони вашого будинку з розумом забезпечується різними способами. По-перше, це оповіщувачі, що сигналізують про проникнення нежданих гостей. Вони включають системи спеціального оповіщення – спрацьовує сигнальна миготлива лампа, сирена, дзвінок у міліцію й усе, що ви запрограмуєте для цього випадку.

По-друге, будинок з розумом може бути постачений відеокамерою або їхньою мережею. Вони будуть невпинно стежити за що відбувається як усередині будинку, так і зовні. Зображення можна вивести на екран комп'ютерного монітора або телевізора.

Відомо, що взлому частіше піддаються будинку, хазяї яких відсутні. Тому, їдучи, ви можете дати Інтелектуальному будинку завдання створити ефект присутності в будинку на час вашого від'їзду. У кімнатах буде включатися-вимикатися світло, відкриватися-закриватися жалюзі. Навіть найближчі сусіди не догадаються, що в будинку нікого немає.

Неуважні люди, які ніколи не впевнені, чи виключили вони праска або телевізор, установивши в приміщенні димові оповіщувачі, можуть нарешті зітхнути спокійно. Якщо

ці прилади "відчують" дим, то вони самостійно будуть додзвонюватися в пожежну частину, хазяїнові на роботу або на мобільний телефон.

Домашні кінотеатри

Отже, культурно-дозвільний комплекс вашого будинку: тут в основі є той же системний підхід. По-перше, вся аудіовідеотехніка зв'язана в єдину мережу. По-друге, система охоплює цілий будинок – управляти можна з будь-якого куточка. Великій родині не обов'язково встановлювати в кожній кімнаті й відеомагнітофон, і аудіосистему – досить мати одну загальну на всіх: нові кабельні мережі дозволяють передавати відео– і аудіосигнали на приймаючі в будь-якій кімнаті. Отут-то й виникає загадкове поняття "мультирум", що означає джерела аудіо-відеосигналів, зібрані в єдиній стійці, у сполученні із системою розподілу A/V даних по будинку, що живлить звуко-візуальну атмосферу в інших кімнатах.

До того ж аудіо-відеотехніка з'єднана з усіма іншими системами. Тому, коли ви збираєтеся подивитися фільм, одночасно включається домашній кінотеатр, закриваються жалюзі, освітлення плавно гасне. До останнього часу словосполучення "домашній кінотеатр" асоціювалося з більшим телевізором, оточеним аудіоапаратурою. Однак в останні роки домашні кінотеатри звичайно створюють на основі відео проекторів і більших екранів, або на базі плазмених панелей.

А взагалі всіма встановленими у вашім будинку системами можна управляти не тільки за допомогою дистанційних пультів, про які ми згадували вище. При наявності необхідної програми вони будуть озиватися на ваш голос. Із Системою керування будинком ви можете зв'язатися з будь-якої точки земної кулі через Internet або по телефоні.

До речі, не тільки ви можете впливати на систему. Інтелектуальний будинок сам може нагадувати вам про те, що необхідно зробити, голосовим способом або по телефону. При автоматизації свого будинку кожний може вибрати систему, найбільш підходящу йому по функціях, складності й вартості. Звичайно, найкраще подумати про те, що будинок повинен бути інтелектуальним, ще на етапі будівництва. Але якщо ремонт уже зроблений, а автоматизувати будинок дуже хочеться, то й це можливо. Питання тільки в тому, у яку компанію ви звернетеся і якими засобами ви розташовуєте.

Система безпеки

В «розумному будинку» система безпеки побудована таким чином, щоб якомога раніше виявити й запобігти загрозливим життям і здоров'ю людини ситуації, ліквідуючи тим самим причини наших найпоширеніших «побутових» страхів.

Захист від зломів і крадіжок. Це завдання вирішується насамперед за рахунок добре продуманої системи сигналізації. В «розумному будинку» дуже часто використовуються два контури сигналізації: зовнішній, до якого підключені всі датчики відкриття вікон і дверей по периметрі будинку, і внутрішній, що складається з датчиків руху, розташованих усередині будинку. Ідучи на роботу, ви включаєте обидва контури. А, наприклад, увечері можна задіяти тільки зовнішній контур і спокійно відпочивати з родиною, зовсім не турбуючись про те, що місцеві хулігани проникнуть у будинок через вікно комори.

Цих же самих хуліганів і інших зловмисників «розумний будинок» легко введе в оману щодо присутності хазяїв. По заданій програмі буде включатися й вимикатися світло, відповідно піднімуться або опустяться жалюзі, періодично буде гавкати собака. Всі ці «хитрості» припиняють злочинні наміри випадкових і зовсім не випадкових перехожих. Якщо ж зловмисники все-таки захочуть проникнути у ваш «розумний будинок», їх злякають завивання сирени й миготіння світла, а на місцевий пост охорони й (або) ваш мобільний телефон відразу надійде сигнал про злом.

Захист від пожежі, витоків і витоку газу. Пожежна сигналізація в заміському будинку або квартирі – це вже норма життя. Система «розумний будинок» дозволяє реалізувати всі стандартні функції протипожежної сигналізації (наприклад, автоматичне відключення вентиляції при пожежі, звукове й світлове оповіщення). Для запобігання витоків у ванній, туалеті й на кухні встановлюються датчики, які контролюють появу води. При виявленні

витоку автоматично закриваються клапани на трубопроводах, що подають, холодного й гарячого водопостачання, а на ваш стільниковий телефон або по електронній пошті надходить повідомлення про аварійну ситуацію. Точно так само система «розумний будинок» реагує й при витоку газу в котельні або на кухні.

Додаткові функції безпеки. Навіть якщо до вас в «розумний будинок» під видом електрика проникнув підозрілий суб'єкт, ви завжди зможете подати сигнал тривоги, усього лише на парі секунд довше потримавши палець на кнопці звичайного вимикача, увімкнути світло. При цьому «незваний гість» навіть не запідозрить, що ви комусь про щось повідомили.

Ще одна з дуже зручних функцій, що реалізується в усіх без винятку системах «розумний будинок», умовно називається «Виключити всі». Ідучи останнім, ви натискаєте кнопку «Нікого немає будинку», і у всьому будинку відключаються світильники й всі розетки, у яких, можливо, залишилися включеними забута праска або фен. Одночасно перекриваються трубопроводи газу, холодної й гарячої води, система опалення починає працювати в економічному режимі, зовнішній і внутрішній контури системи сигналізації ставляться на охорону.

Первісні вкладення в систему «розумний будинок» перевищують витрати на стандартну систему керування електроустаткуванням. Мається на увазі зниження витрат при експлуатації «розумного будинку» за рахунок економії енергоресурсів (холодної й гарячої води, газу, електрики). Поки в нашій країні ця економія не настільки значна, як у країнах Європи, але, по всіх прогнозах, у найближчому майбутньому ціни на теплоносіїв і електроенергію істотно виростуть. Ще одна немаловажна стаття економії випливає з реалізованих «розумним будинком» функцій безпеки. Запобігання аварійних ситуацій, у першу чергу витоків і пожеж, знижує до мінімуму ймовірність непланових ремонтів.

IEEE 802.3bt

Далі, у даному розділі розглянемо основу технології IEEE 802.3bt, на якій будуються системи управління будинками.

IEEE 802.3bt – це універсальна платформа для побудови класичних шинних розподілених систем управління в системах «розумний будинок», в автоматизації будинків. IEEE 802.3bt – найбільш доступна на сьогоднішній день платформа для побудови шинних розподілених систем керування внутрішнім і вуличним освітленням, силовими навантаженнями, електроприладами, а також такими системами, як опалення, кондиціювання, вентиляція, охоронна сигналізація, контроль доступу й утікань води. Також можливе керування аудіо– і відеотехнікою, домашніми кінотеатрами, жалюзі, рольставнями, шторами, воротами, насосами, двигунами. В основному орієнтована на застосування в складі «розумного будинку», але останнім часом всі частіше застосовується в системах обліку й заощадження енергоресурсів, контролю доступу, охоронно-пожежних системах.

Структурно система складається із центрального контролера й виконавчих модулів, зв'язаних між собою польовою шиною (мережею). До виконавчих модулів підключаються кероване устаткування.

Для взаємодії система використовує на фізичному рівні стандарт RS-485. Для взаємодії на прикладному рівні використовується широко відомий протокол Modbus/RTU. Устаткування підтримує швидкість обміну інформацією в режимах 2400, 4800, 9600, 19200, 38400, 57600, 76800, 115200 біт/с, що, досить для миттєвого виконання команд. Максимальна кількість пристроїв, керованих одним головним контролером (ПЛК) – 100. Можливе об'єднання декількох головних контролерів в одну мережу. Через використання стандартних протоколів можливе включення в систему устаткування сторонніх виробників, також можливе використання пристроїв серії IEEE 802.3bt в інших системах.

Елементи системи:

– Центральний керуючий контролер, що дозволяє управляти всіма пристроями за заданими сценаріями.

– Релейні модулі, що забезпечують комутацію потужного навантаження до 1,2 кВт, а також опитування датчика типу «сухий контакт».

– Діммируючі модулі, що забезпечують можливість плавної зміни потужності в навантаженні.

– Модулі інфрачервоного зв'язку, що забезпечують прийом команд із пультів дистанційного керування й передачу збережених команд на побутові пристрої.

– Модулі з 4-мя цифровими входами, що забезпечують опитування декількох датчиків.

– Модулі розширення з аналоговими входами-виходами, що забезпечують опитування аналогових датчиків, наприклад, температури, і керування аналоговими пристроями.

– Модулі й датчики збору інформації: температури, вологості, руху.

– Опціональні комунікаційні модулі GSM.

– Блоки живлення всієї системи й центрального контролера.

У цій системі необхідне програмування тільки головного контролера. Для програмування використовується спеціалізоване програмне забезпечення – IEEE 802.3bt Configurator Pro.

Система може управлятися за допомогою великого переліку програмного забезпечення:

– SCADA-додатки.

– OPC-сервери Modbus.

– Спеціальні додатки для керування будинками, розумними будинками, такі як IridiumMobile, IdomMedia.

Весь перелік додатків дозволяє здійснювати оперативне візуалізоване керування розумним будинком, у тому числі:

– керування системою IEEE 802.3bt із сенсорних моніторів, панелей;

– керування системою IEEE 802.3bt з кишенькових комп'ютерів;

– керування системою IEEE 802.3bt з iPhone, iPod, iPad;

– керування системою IEEE 802.3bt через Інтернет по захищеному каналу;

– об'єднання безлічі центральних контролерів SPIDER у єдину мережу;

– створення власних віртуальних панелей керування будинком;

– можливість інтеграції з устаткуванням сторонніх виробників.

Центральний контролер

Центральний контролер може використовуватися як у настільному варіанті, так і монтуватися на DIN-рейку. Програмується з персонального комп'ютера за допомогою програми IEEE 802.3bt Configurator через USB-порт або Ethernet-підключення. Після програмування комп'ютер не використовується для роботи системи. Центральний контролер є високоінтегрованим пристроєм у широким набором периферії. За допомогою нього можливе створення:

– дротових мереж «розумного» будинку;

– бездротових мереж «розумного будинку»;

– комплексні системи збору й обліку даних про споживання ресурсів, АСКУЕ по Ethernet, Internet

– систем охоронно-пожежної сигналізації, у тому числі й по мережах GSM;

– систем оповіщення й вилученого керування по мережах GSM, Ethernet, Internet

– систем доступу;

– систем витоку води й витоку газу;

– систем клімат-контролю;

– систем керування встаткуванням "мультирум";

– систем диспетчеризації, розподіленого керування й моніторингу по інтернет і локальні мережі, у тому числі груп будинків у котеджних селищах, стільникових станцій, очисних споруджень, серверних по мережах GSM, Ethernet, Internet

– систем автоматичного введення резерву (АВР);

– систем керування котельнями по мережах GSM, Ethernet, Internet.

Релейні модулі

Керовані релейні модулі випускаються у двох виконаннях – мініатюрному для вбудовування, наприклад, у стакани розеток під вимикачі й розетки, і для установки на DIN рейку. Пристрої, установлювані на DIN-рейку, мають більшу потужність.

Діммуючі модулії

Керовані діммуючі модулі випускаються у двох модифікаціях – потребуючі підведення нуля й фази, і «розривні». Другі зручні для монтажу в склянки вимикачів, де не проведений нуль.

Модулі інфрачервоного зв'язку

Трансівери (приймачепередатчики) інфрачервоних сигналів виконуються у вигляді, що вбудовуються. Комплектуються шліфованою металевою панеллю. Є універсальними, дозволяють розпізнавати, запам'ятовувати й відтворювати ІЧ-команди будь-якого виробника.

Модулі із цифровими входами

Випускаються в мініатюрних корпусах, що дозволяє вбудовувати в стандартні стакани вимикачів. До клем модулів підключаються датчики виходи, що мають, типу «сухий контакт».

Модулі розширення

Розширені модулі для підключення датчиків з універсальною кількістю входів і виходів керування. Випускаються в DIN-корпусах.

Датчики

Датчики руху, освітленості й т.д. Можливо підключення датчиків різних виробників.

Блоки живлення

Стабілізовані промислові блоки живлення. Система на вибір комплектується блоком живлення відповідної потужності.

Монтаж

Монтаж системи ведеться класичною екранованою крученою парою FTP. Кабель приховано прокладається по периметру приміщення з відгалуженнями до кожного пристрою IEEE 802.3bt. У місці з'єднання, у кабелю знімається зовнішня й внутрішня оплітка на відрізку приблизно 1,5-2,0 см., далі він скручується й закріплюється обтиск наконечниками. Якщо монтаж здійснюється раніше установки модулів на тривалий час, необхідно не розрізаючи шину, залишити запаси кабелю (петлі) у місцях майбутнього розташування модулів. Кабель підводить до всіх стаканів вимикачів, розеток (якщо необхідно їхню автоматизацію), в усі стелі. Крім цього необхідно прокинути кабель по всіх периметрах всіх приміщень. Це вирішить всі питання по раптовій зміні планів точок автоматизації замовниками.

Розробка структурної схеми

Опишемо основні складові інтелектуального будинку.

Інформаційні системи:

–локальна комп'ютерна мережа;

–домашній офіс;

–широкополосний доступ у глобальну мережу (Інтернет).

Безпека:

–пожежна сигналізація й система автоматичного пожежогасіння;

–охоронна сигналізація;

–система контролю доступу;

−система зовнішнього й внутрішнього відео спостереження;
−система управління паркінгом;
−система внутрішнього оповіщення (радіомережа);
−аварійний контроль інженерних систем;
−система екологічного контролю.
Зв'язок:
−телефонний зв'язок внутрішня (інтерком) і локальні АТМ;
−телефонний зв'язок зовнішня провідна, радіорелейна, супутникова;
−Інтернет-телефонія;
−системи відеоконференцій.
Мультимедіа:
−наземне й кабельне телебачення;
−супутникове телебачення;
−домашнє відео;
−домашній кінотеатр;
−мульти– аудіо й відео (multiroom).
−один пульт управління для всіх систем
Система електроживлення:
−безперебійне й гарантоване електропостачання;
−захист від поразки електричним струмом людей і тварин;
−автоматизація управління електроживленням побутових приладів;
−запобігання перевантажень і короткого замикання в електричній мережі;
−управління якістю електроживлення – моніторинг, стабілізація й фільтрація;
−облік витрат й управління споживанням електроенергії.
Освітлення внутрішнє й зовнішнє:
−аварійне й чергове освітлення;
−автоматизація управління світлом;
−гнучке настроювання світлових груп;
−дистанційне й віддалене управління світлом;
−програмування світлових сцен.
Опалення, вентиляція, кондиціювання:
−автоматизація управління температурою повітря;
−контроль якості повітря;
−узгодження роботи різних кліматичних систем;
−облік витрати й управління споживанням теплової енергії.
Водопостачання й газопостачання:
−автоматичне наповнення ванн, басейнів і накопичувальних резервуарів;
−автономне й резервне нагрівання води;
−запобігання витоку водопроводу й витоку газу;
−управління ландшафтними водяними системами (фонтани, водоспади);
−управління температурою води у ваннах і басейнах (термостатування);
−облік витрат й управління споживанням води й/або газу.

Тепер спробуємо створити зі звичайного будинку інтелектуальний. Для цього нам потрібно всі прилади, які виконують перераховані вище функції, об'єднати в одну систему й підключити її до віддаленого сервера. Тим самим буде управління кожним компонентом, та всіма воєдино. І необхідно щоб контроль за станом всіх приладів користувач міг одержати в будь-який момент часу, навіть перебуваючи поза будинком. Для цього треба організувати мережу в будинку, об'єднавши всі прилади й системи над якими треба здійснити контроль, та потім вибрати спосіб підключення до віддаленого сервера.

На рисунку 1 зображена узагальнена структурна схема системи управління домом.

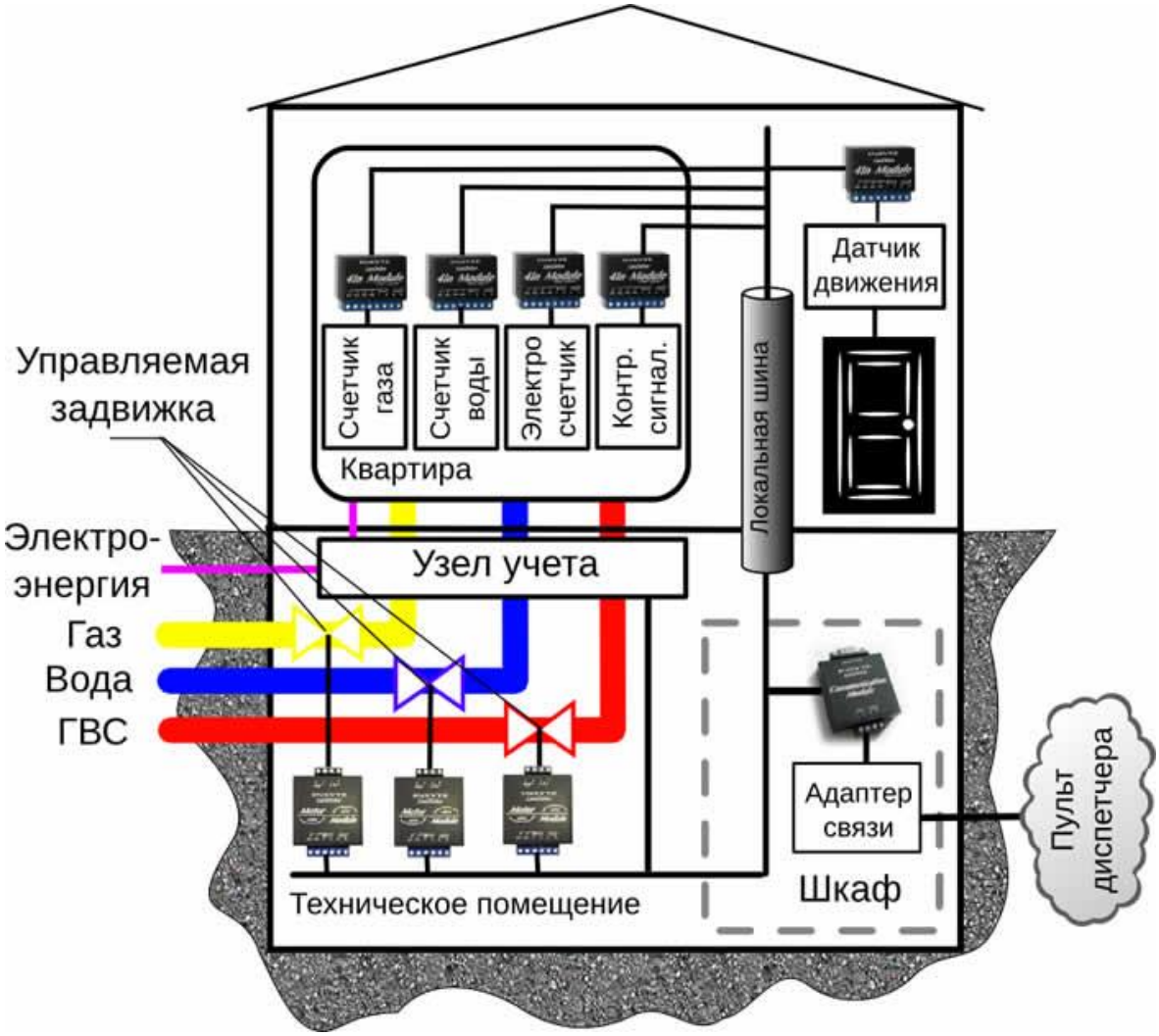


Рисунок 1 – Структурна схема системи

Система складається з набору модулів IEEE 802.3bt, об'єднаних у єдину мережу по інтерфейсу RS-485 на основі крученої пари. Всі лічильники, датчики й виконавчі механізми підключаються до модулів системи IEEE 802.3bt по інтерфейсах типу сухий контакт, рахунковий і аналоговий входи, а також через релейні виходи модулів.

Система заживляється постійною напругою 12-24В силою току з розрахунку 0,5Вт на один модуль. Для заживлювання системи передбачається резервне джерело живлення, бажано автономне на 24 години функціонування.

Як середовище передачі даних на диспетчерський пульт використовується мережа провайдеру з виділеним VPN-каналом. Фізичне підключення здійснюється за допомогою Ethernet-адаптера с виділеним IP-адресою. Для передачі використовується шифрування SSL 128 біт.

Для взаємодії на прикладному рівні використовується широко відомий протокол Modbus/RTU.

Як було відзначено вище, сучасний інтелектуальний будинок – це дуже складне інженерне рішення, що складається з наступного набору систем:

– Система безпеки.
– Система комфорту.
– Інформаційна система.
– Система диспетчеризації.

Розглянемо які підсистеми входять у перераховані вище системи.

Система безпеки:

–Система цифрового відеоспостереження з можливістю одночасного спостереження, перегляду, архівування. Режим віддаленого перегляду й управління через Інтернет.

–Бездротова пожежна й охоронна сигналізація з можливістю обміну інформацією через GSM модуль.

–Система контролю доступу в приміщення (у тому числі віддалене управління гаражними воротами).

Система комфорту:

–Внутрішня телефонна система, голосний зв'язок усередині будинку.

–Система супутникового, ефірного телебачення з можливістю перегляду в будь-якій кімнаті.

–Система «Домашній кінотеатр».

–Система «Мультирум» аудіо– й відео– (система «звук навколо»).

–Цифровий розважальний комплекс, оцифровка відео, печать фотографій, створення особистих цифрових фото– і відео– альбомів і т.д.

–Управління світлом у всьому будинку, світлові сцени й сценарії.

–Управління системою вентиляції й кондиціювання.

–Управління системою опалення.

–Управління сауною, басейном.

Інформаційна система:

–Установка локальної обчислювальної мережі в будинку, мережна печать, мережні ігри (можлива використання бездротових технологій).

–Вихід в Інтернет з будь-якого комп'ютера в будинку (у тому числі з мобільного).

–Віддалене управління всіма системами будинку через Інтернет.

–«Домашній офіс» з віддаленим підключенням до корпоративної мережі робочого офісу.

Система диспетчеризації:

–Система безперебійного електропостачання

–Управління системою опалення, казаном водонагрівача

–Контроль витоку води, газу.

–Система управління здатна погоджувати роботу інженерних систем, оцінюючи стан сенсорів, датчиків, відпрацьовуючи команди з пультів управління, прив’язуючись до часу доби, пори року й т.п. При цьому виключаються ситуації, коли домашнє устаткування, покликане вирішувати спеціалізовані проблеми, працює в режимах, взаємовиключаючих один одного.

Інтелектуальний будинок дозволяє замінити всі пульти управління однією або декількома (по кількості зон або кімнат) сенсорними панелями. Вони дозволяють не ламати голову над тим, як підбудувати середовище перебування під необхідні умови.

Використання сучасного устаткування дозволяє створити в будинку єдиний комплекс із систем безпеки (охоронна й пожежна сигналізація, відеоспостереження, контроль доступу), систем зв'язку й комунікації (телефонна й комп'ютерна мережі, оповіщення, екстрений виклик), систем управління опаленням, вентиляцією, освітленням і т.д., що працює по обраному алгоритму.

Як ілюстрацію можна привести приклад, коли автоматизація й включення в єдиний контур управління освітлювальної системи й систем клімат-контролю (опалення, кондиціювання й вентиляція) будинку (окремої квартири) дозволяють реалізувати автоматичне управління цими системами залежно від пори року й доби, умов навколишнього середовища, присутності людей і інших ,факторів. У результаті досягається істотне зниження витрат на електроенергію й теплопостачання. Досвід показує, що економія експлуатаційних витрат у цьому випадку може досягати 15-20%.

Состав системи:

– Центральний процесор. Обробка керуючих команд від керуючих сенсорних панелей, відправлення команд для ІЧ банків, диммерів, релейних модулів. Обробка вхідної информації від датчиків, контролерів, модемів. Установлюється програмне забезпечення розроблене у результаті виконання дипломного проектування, його серверна частина.

– Керуючі сенсорний панелі. Передача в центральний процесор команд керування, відеомоніторинг, подання на екрані всієї необхідної інформації/пов'язані із центральним процесором по мережі Ethernet (TCP/IP)

– Діммери. Регулювання яскравості світіння ламп, управляються центральним процесором або по командах від сенсорних панелей або відповідно до закладеного алгоритму (сценарію), пов'язані із центральним процесором RS-485 інтерфейсом.

– Релейні модулі. Керування релейними контактами й прийом сигналів на входи типу 0-1 управляються Центральним процесором або по командах від Керуючих сенсорних панелей або відповідно до закладеного алгоритму(сценарієм)/пов'язані із Центральним процесором RS-485 інтерфейсом.

– Банки ІЧ команд. Випромінювання ІЧ команд із пам'яті контролера, раннє туди записаних. Керування апаратурою що має ІЧ інтерфейс. Управляються центральним процесором або по командах від керуючих сенсорних панелей або відповідно до закладеного алгоритму/пов'язані із центральним процесором RS-485 інтерфейсом.

Отже, для того щоб зробити розумний будинок потрібно:

– Зробити схему розташування периферійного встаткування на об'єкті, робиться на поетажних планах.

– Пронумерувати всі приміщення в будинку.

– Скласти список проводів/тип кабелю, маркування, звідки й куди йде проведення, які повинні підходити до кожному елементу системи кабельний журнал.

– Відкрити вікно «Редактор системи управління домом» і мишкою створити необхідні елементи системи спочатку сторінки кімнат, потім на цих сторінках і інші елементи керування будинком. Під час роботи в редакторі ви створюєте графічний інтерфейс керування системи.

– Тепер залишилося додати графічному інтерфейсу індивідуальний дизайн і підключити до центрального процесора необхідне встаткування/список цього встаткування також формується в процесі роботи редактора.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів інтернету речей на базі стандарту IEEE 802.3bt. В межах України в недостатній мірі представлені вітчизняні розробки в цій області. У роботі наведені теоретичне узагальнення й рішення наукового завдання дослідження методів інтернету речей на базі стандарту IEEE 802.3bt. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем інтернету речей на базі стандарту IEEE 802.3bt; Досліджена система інтернету речей на базі стандарту IEEE 802.3bt; На основі отриманих результатів досліджень створена програмна реалізація системи інтернету речей на базі стандарту IEEE 802.3bt. Розроблені під час виконання роботи алгоритми дозволяють успішно вирішувати завдання інтернету речей на базі стандарту IEEE 802.3bt.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. 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.
2. 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.

3. 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.
4. 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.
5. Коваленко А.С. Удосконалення методу технічного обслуговування об'єктів інтегрованої інформаційної системи / А.С. Коваленко, О.А. Смірнов, О.В. Коваленко, О.П. Доренський // Системи озброєння і військова техніка. – Х.: ХУПС, 2016. – № 2(46). – С. 109-114.
6. Коваленко А.С. Метод визначення оптимального комплексу робіт з відновлення працездатності інтегрованої системи технічної діагностики в умовах ресурсних обмежень / А.С. Коваленко // Системи обробки інформації. – Х.: ХУПС, 2016. – Вип. 3(140). – С. 69-72.
7. Kovalenko A.S. Information model and its element for displaying information on technical condition of objects of integrated information system / A.S. Kovalenko, A.A. Smirnov, A.V. Kovalenko, A.P. Dorensky // International Journal of Computational Engineering Research (IJCER). – India: Delhi, 2016. – Volume 6, Issue 1. – P. 21-27.
8. Кожанова А.С. Система технічної діагностики інтегрованих інформаційних систем – обґрунтування необхідності створення, визначення понятійного апарату та напрямів досліджень / А.С. Кожанова, О.А. Смірнов, М.П. Савченко, Д.М. Ізосімов, В.В. Мороз // Створення та модернізація озброєння і військової техніки в сучасних умовах: Тринадцята наук.-техн. конф., 5-6 вер. 2013 р., м. Феодосія: тези доп. – Феодосія: ДНВЦ, 2013. – С. 187-188.
9. Кожанова А.С. Визначення основних напрямків досліджень щодо створення системи технічної діагностики інтегрованих інформаційних систем / А.С. Кожанова, О.А. Смірнов, А.В. Челпанов // Проблемні питання розвитку озброєння та військової техніки Збройних Сил України: IV наук.-техн. конф., 16-20 груд. 2013 р., м. Київ: зб. тез. – Київ: ЦНДІ ОВТ ЗСУ, 2013. – С. 293.
10. 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.

УДК 004

І. Богданова, магістр гр. КІ-19М-1,4
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ ПРОЕКТУВАННЯ СТРУКТУРОВАНИХ КАБЕЛЬНИХ МЕРЕЖ НА БАЗІ ВИКОРИСТАННЯ LINK CONTROL

У статті розроблено програмне забезпечення, яке призначено для системи проектування структурованих кабельних мереж на базі використання Link Control. Метою розробки є дослідження та програмна реалізація системи проектування структурованих кабельних мереж на базі використання Link Control. Об'єктом дослідження є процес проектування структурованих кабельних мереж на базі використання Link Control. Предметом дослідження є методи проектування структурованих кабельних мереж на базі використання Link Control. Методи дослідження базуються на методах теорії телетрафіку, методах математичної статистики, методах розробки програмного забезпечення.
комп'ютерна інженерія, структуровані кабельні мережі, Link Control

Постановка проблеми. Незважаючи на деяку зовнішнє уповільнення з темпів удосконалювання, техніка структурованих кабельних систем (СКС) продовжує розвиватися досить високими темпами. «Локомотивами» технічного прогресу в області СКС стають кабельні системи для центрів обробки даних (ЦОД) і промислових підприємств – у них акумулюється найбільша кількість новинок системного й, відповідно, компонентного плану.

Концепція побудови СКС на об'єкті нерухомості була розроблена наприкінці 80-х років минулого сторіччя. Перший стандарт TIA/EIA-568 був орієнтований на офісне

застосування. При переносі його положень на інші області була потрібна корекція ряду підходів без зміни базових принципів. Мова йде про формування універсальних трактів передачі, нормовані характеристики яких відбивають досягнутий рівень техніки й розраховуються з певним запасом, що дозволяє, по-перше, не міняти проводку протягом усього міжремонтного терміну служби архітектурного об'єкта, а по-друге, дає можливість компенсувати підвищені капітальні витрати за рахунок зниження експлуатаційних витрат протягом розумного періоду часу.

Адекватність нормативної бази поточним потребам досягається завдяки наступним факторам:

- стандарти переглядаються з певною періодичністю, що дозволяє відповідати досягнутому рівню техніки;
- при виході за межі типового офісу враховуються специфічні особливості нової області.

Сильною стороною такого підходу є те, що стандартизація стає стимулом для усе більше масового поширення як нових системних рішень, так і перспективної елементної бази.

Розширення області застосування СКС виявлялося можливим завдяки розробці окремих стандартів, у яких ураховувалися особливості побудови й умови експлуатації техніки. Втім, це не виключало внесення додавань у базовий документ. Наприклад, деякі фахівці вважають популярні кабельні системи для відкритих офісів самостійним різновидом кабельних систем. Із точки ж зору стандартів вони є підкласом звичайних офісних СКС.

Органи стандартизації жорстко дотримувалися принципу відкритості: кабельний тракт у максимально складній конфігурації повинен мати визначені параметри при його побудові з компонентів різних виробників. Галузь уперше зштовхнулася з масовим порушенням такого підходу при впровадженні техніки Категорії 6, коли провідні виробники стали виводити на ринок закриті рішення. З появою техніки Категорії 6_А подібного небажаного явища вдалося уникнути, що дозволяє споживачеві застрахуватися від можливих фінансових втрат, викликаних несумісністю окремих елементів тракту передачі.

Принцип універсальності безумовно дотримується тільки на рівні горизонтальної підсистеми офісних кабельних систем або її аналогів в інших системах. Рівень сучасної техніки не дозволяє поширити його на магістральні підсистеми.

Конектор LC (Link Control) – оптичний конектор з наконечником 1,25 мм в пластиковому прямокутному корпусі. Розроблено на замовлення компанії Lucent Technologies (США). LC є малогабаритним варіантом коннектора SC і має такий же механізм підключення – push-pull (лінійне підключення і фіксація за допомогою засувки).

LC коннектори випускаються як для одномодового, так і для багатомодового оптичного волокна. Торець коннектора може мати пряму (PC) або кутову (APC) полірування. LC коннектори бувають не тільки симплексними, але і дуплексними. Крім стандартних дуплексних LC конекторів випускаються також коннектори Mini LC (зі зменшеним відстанню між наконечниками) і LC Uniboot (з одним хвостовиком для круглого дуплексного кабелю).

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи проектування структурованих кабельних мереж на базі використання Link Control.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи проектування структурованих кабельних мереж на базі використання Link Control.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

- Огляд існуючих систем проектування структурованих кабельних мереж на базі використання Link Control.
- Дослідження системи проектування структурованих кабельних мереж на базі використання Link Control.
- Програмна реалізація системи проектування структурованих кабельних мереж на базі використання Link Control.

Об'єктом дослідження є процес проектування структурованих кабельних мереж на базі використання Link Control.

Предметом дослідження є методи проектування структурованих кабельних мереж на базі використання Link Control.

Методи дослідження базуються на методах теорії телетрафіку, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Значимі відмінності в інформаційній проводці промислового призначення обумовлені жорсткими умовами експлуатації термінального устаткування й відсутністю потреби в передачі більших обсягів даних. Внаслідок наявності безлічі низькошвидкістних термінальних пристроїв промислової автоматизації ці кабельні системи уступають за рівнем швидкості своєму офісному прототипу, однак мають порівнянну частку електропровідних рішень.

На системні рішення сильний вплив роблять жорсткі умови експлуатації. У промислових СКС масово застосовується електропровідна техніка високих категорій. Запас по передатних характеристиках трактів дозволяє надійно захистити сигнал від впливу зовнішньої перешкоди, а також наростити кількість проміжних з'єднувачів.

Частина промислових кабелів пропонується у дво- і навіть однопарному варіантах. Завдяки поліпшенню вагогабаритних характеристик лінійних виробів знижується витрата дорогих полімерів, використання яких гарантує нормальну експлуатацію кабелів на різних виробництвах.

Однопарна техніка розробляється насамперед в інтересах автомобільної промисловості, але по основних параметрах (сполучення швидкості й дальності зв'язку) вона цілком придатна й для інших виробничих областей.

СКС безпосередньо сполучається з мережевими інтерфейсами локальної мережі. До останнього часу кожне нове покоління техніки для локальної мережі забезпечувало 10-кратне збільшення швидкості передачі даних. Через об'єктивний схемотехнічних проблем і зниження економічної ефективності випереджального впровадження нового обладнання (низьких темпів росту його завантаженості) для мідножильної техніки передбачений крок нарощування 4? (після 10 Гбіт/с з'явилися 40 Гбіт/с), у швидкісному діапазоні 1-10 Гбіт/с уведені проміжні значення 2,5 і 5 Гбіт/с, а до діапазону 10-40 Гбіт/с додано 25 Гбіт/с.

Підтримка нових номіналів швидкостей відбувається не тільки шляхом впровадження компонентів нової категорії, але й за рахунок того, що раніше створені лінії заново сертифікуються для використання в розширеному частотному діапазоні.

Оптична підсистема розвивається по схожих принципах: у швидкісному діапазоні 10-400 Гбіт/с і ставка робиться на схему паралельної передачі й використання комбінації техніки просторового (паралельна передача) і спектрального ущільнення. Пропонується наступна сітка проміжних номіналів швидкостей: 25, 40, 50, 100 і 200 Гбіт/с. Кабелі й роз'єми для них спеціально не розробляються.

Припустимі конфігурації кабельних трактів

Збільшення числа споживачів ресурсів СКС зажадало ревізії переліку припустимих конфігурацій ліній. У стандарті ANSI/TIA-568-C2-1 уведена конфігурація прямого тракту (Direct Attach Channel): порти мережевого устаткування з'єднуються шнуром або претермінованим складанням. У класичних трактах вилки, які вставляються в апаратуру, уважаються частиною останньої й не враховуються при тестуванні. Контроль характеристик прямого тракту здійснюється разом з вилками, що вимагає модернізації кабельних сканерів.

Пряме підключення (Direct Connection), що припускає установку вилки на стороні термінального пристрою, широко застосовується при обслуговуванні точок бездротового доступу, IP-камер дистанційного спостереження й інших аналогічних пристроїв. Качана включається безпосередньо в активний пристрій. Лінії Direct Connection можна тестувати за допомогою існуючих кабельних сканерів, якщо лінії працюють по моделі Channel.

Оптимізація комплексу активного й пасивного устаткування

ІТС будується відповідно до принципу семирівневої моделі. Найбільші втрати, як правило, відбуваються на інтерфейсах між окремими рівнями. Їх можна зменшити, якщо споконвічно враховувати, що СКС взаємодіє з іншими рівнями в моделі відкритих систем.

Прикладом обліку такої взаємодії на рівні електропровідної системи є відпрацьовування інтерфейсу із системами PoE для дистанційного живлення термінальних пристроїв. При потужності споживання понад 30 Вт температура внутрішніх кабелів регулярного джгута може перевищити гранично припустимі 60°С. Ця обставина стала стимулом до розробки серійних конструкцій з максимальною робочою температурою +75°С. Застосування таких кабелів дозволяє не тільки зберегти естетику кабельних пакетів, але й поліпшити ступінь заповнення кабельних трас.

На рівні роз'єми в інтересах PoE+ і вище контактам розеточних модулів надається розтягнута U-образна форма. Це дозволяє рознести області електроіскрової ерозії й взаємодії контактів качани й розетки, гарантовано поліпшивши якісні показники тракту.

В оптичній підсистемі першою ластівкою стало волокно Signature Core компанії Panduit. Градієнтний профіль показника переломлення цих світловодів скоректований з урахуванням ефекту залежності довжини хвилі оптичного випромінювання VCSEL-Лазера від апертурного кута. У результаті з'являється можливість частково компенсувати міжмодову дисперсію за рахунок хроматичної й збільшити гарантовану дальність мережевих інтерфейсів дії не менш чим на 20%.

Відмова від фіксації максимальних довжин симетричних ліній

Розширення областей застосування змусило розроблювачів відмовитися від дотримання постулату про 100-метрову або іншу нормовану довжину тракту. Причини зміни базових підходів досить різноманітні:

мала (по різних причинах) популярність довгих ліній у нових областях застосування;

неможливість прямої повторної сертифікації раніше створених ліній, з урахуванням підтримки більше швидкісного активного мережевого устаткування;

технічні складності досягнення необхідної довжини тракту в новій області;

економічна недоцільність дотримання вищезгаданого постулату.

Найбільше часто практикується відмова від класичного 100-метрової межі горизонтального тракту. Це може виражатися як у зменшенні, так і в збільшенні максимальної дальності зв'язку.

Прикладом зменшення дальності може служити стандарт на Категорію 8. Залежно від калібру провідника він передбачає найбільшу довжину тракту – 28-32 м.

У контексті підключення точок бездротового доступу члени альянсу NBase-T обговорюють можливість повторної сертифікації кабельних систем Категорій 5е й 6 на швидкість 2,5 і 5 Гбіт/с. Необхідні якісні показники досягалися обмеженням максимальної довжини лінії 50-75 м.

Європейські виробники СКС, навпроти, пропонують електропровідну техніку з параметрами класу D і вище при довжинах лінії до 125 м (Draka, Corning Cable Systems), що викликано необхідністю підтримки камер систем відеоспостереження й контролерів СКУД з дистанційним живленням.

Розширене трактування концепції адміністрування

Удосконалювання обчислювальної техніки дозволяє ефективно зв'язати систему адміністрування й процес інсталяції СКС. Стандарти на адміністрування (TIA-606 і IEC 14763-3) опираються на бази даних і унікальні ідентифікатори окремих компонентів. Вузьке місце існуючого підходу – відсутність твердого взаємозв'язку між первісним проектом і кабельною системою. Це приводить до того, що реальна СКС не погодиться з її образом у базі, а процес інсталяції утрудняється.

Для усунення даного недоліку компанія Fluke Networks запропонувала концепцію централізованого керування процесом реалізації СКС, що припускає безперервний контроль монтажу. У результаті її реалізації усувається вплив людського фактора на якість інсталяції й

гарантується відповідність фактичної конфігурації інформаційної проводки її образу в БД системи адміністрування.

Дана концепція опирається на пряму залежність між проектною документацією, формуванням маркування, тестуванням і іншими процедурами. Додатково враховується, що:

– формати сучасної проектної документації при необхідності конвертуються в потрібну форму;
– монтажник і технік у реальному часі доступні через смартфон;
– технологічне устаткування СКС (принтери етикеток, що маркірують, кабельні сканери, рефлектометри й т.д.) має штатний або додатковий бездротової інтерфейс малого радіуса дії.

Контроль забезпечується шляхом передачі на смартфон монтажника:

– даних по реалізованому пробросу, стаціонарній лінії й тракту;
– форматів і змісту етикеток, що маркірують;
– налаштувань тестуючих приладів.

Потім ця інформація надходить на відповідний пристрій, а після завершення монтажних процедур знову ж через смартфон вертається менеджерові проекту для відбиття у виконавській документації.

Позитивний ефект досягається за рахунок впровадження м'якого інформаційного зворотного зв'язка, в область дії якої включаються проектна документація, інстальована СКС і система адміністрування в розширеній формі.

Незважаючи на деяку з темпів удосконалювання, техніка СКС продовжує розвиватися досить високими темпами. Локомотивом технічного прогресу в області СКС стають кабельні системи для ЦОД і промислових підприємств – у них акумулюється найбільша кількість новинок системного й, відповідно, компонентного плану. При цьому зростаючі потреби ЦОД задовольняються за рахунок поліпшення волоконо-оптичної техніки, а в промислових системах – електропровідних рішень.

Основним способом підвищення техніко-економічної ефективності створюваного об'єкта при переході в нову область стає відмова від ряду вихідних постулатів прототипу (офісних СКС). Найчастіше змінюються дозволена довжина тракту й структури формованих ліній. Потенційно перспективним підходом для системного вдосконалювання СКС є облік особливостей її взаємодії з активним мережевим устаткуванням.

Доступність відповідні ПО, застосування сучасної техніки й належна організація виробничого процесу дозволяють повністю контролювати за допомогою технічних засобів не тільки наступну експлуатацію СКС, але й процедуру її інсталяції.

Розробка структурної схеми

Під структурою СКС розуміють модель побудови системи зі структурних елементів і підсистем. Даний розділ визначає також інтерфейси точки для підключення термінального устаткування до структурованої системи й самої СКС – до мережі загального користування. Групи структурних елементів утворять підсистеми СКС. Відмінності термінів американських стандартів виділені червоним кольором.

Структурні елементи СКС

Структурована кабельна система – середовище передачі електромагнітних сигналів – складається з елементів – кабелів і роз’ємів. Кабелі, оснащені роз’ємами й прокладені за певними правилами, утворять лінії й магістралі. Лінії, магістралі, точки підключення й комутації становлять структурні елементи СКС.

В американському стандарті до структурних елементів відносять два типи кабелів, три типи приміщень, елемент конструкції ЦОД й документацію телекомунікаційної інфраструктури. Крім того, у даних групах стандартів використовується різна термінологія.

Структурні елементи СКС:

– Розподільний пункт комплексу (ЦОД) (РП комплексу).
– Магістраль комплексу (МК).
– Розподільний пункт ЦОД (РП ЦОД).

– Магістраль ЦОД (МБ).
– Розподільний пункт поверху (РП поверху).
– Горизонтальні кабелі (ГК).
– Точка переходу (ТП).
– Телекомунікаційні роз'єми (ТР).
– Робоча область.
– Телекомунікаційні приміщення.
– Апаратні.
– Вводи в ЦОД.
– Адміністрування.

Рисунок 1 – Структурна схема системи

Міжнародні /європейські стандарти підрозділяють СКС на вісім структурних елементів, американський – на сім. Тільки два з них збігаються. У першому випадку структурні елементи становлять середовище передачі, тобто властиво структуровану кабельну систему. Це дозволяє виділити підсистеми й провести точні границі між ними.

У другому до складу структурних елементів не ввійшла магістраль комплексу й всі інтерфейси СКС і додані приміщення, елементи ЦОД і система документування. Це приведе до плутанини й змішування понять у технічній літературі, проспектах виробників і документації, створюваних по американській моделі.

Підсистеми СКС. Міжнародні /європейські стандарти підрозділяють СКС на три підсистеми: магістральна підсистема комплексу, магістральна підсистема ЦОД, горизонтальна підсистема.

Розподільні пункти забезпечують можливість створення топології каналів типу «шина», «зірка» або «кільце».

Магістральна підсистема комплексу включає магістральні кабелі комплексу, механічне закінчення кабелів (роз'єми) у РП комплексу й РП будинки й комутаційні з'єднання в РП комплексу. Магістральні кабелі комплексу також можуть з'єднувати між собою розподільні пункти ЦОД.

Магістральна підсистема ЦОД включає магістральні кабелі ЦОД, механічне закінчення кабелів (роз'єми) у РП будинки й РП поверху, а також комутаційні з'єднання в РП будинки.

Магістральні кабелі ЦОД не повинні мати точок переходу, електропровідні кабелі не слід з'єднувати сплайсами.

Горизонтальна підсистема включає горизонтальні кабелі, механічне закінчення кабелів (роз'єми) у РП поверху, комутаційні з'єднання в РП поверху й телекомунікаційні роз'єми. У горизонтальних кабелях не допускається розривів. При необхідності допускається одна точка переходу. Усе пари й волокна телекомунікаційного роз'єми повинні бути підключені. Телекомунікаційні роз'єми не є точками адміністрування. Не допускається включення активних елементів і адаптерів до складу СКС.

Абонентські кабелі для підключення термінального устаткування не є стаціонарними й перебувають за рамками СКС. Однак, стандарти визначають параметри каналу, до складу якого входять абонентські й мережеві кабелі.

Топологія СКС – «ієрархічна зірка», що допускає додаткові з'єднання розподільних пунктів одного рівня. Однак такі з'єднання не повинні заміняти магістралі основної топології. Число й тип підсистем залежить від розмірів комплексу або будинки й стратегії використання системи. Наприклад, у СКС один будинки досить одного РП ЦОД й двох підсистем – горизонтальної й магістральної. З іншого боку, великий ЦОД можна розглядати як комплекс, що включає всі три підсистеми, і в тому числі, декілька РП ЦОД.

Розподільні пункти розміщаються в телекомунікаційних приміщеннях і апаратних. Телекомунікаційні приміщення призначені для установки панелей і шаф, мережевого й серверного устаткування, що обслуговують весь або частина поверху. Апаратні виділяють для телекомунікаційного устаткування, що обслуговує користувачів усього ЦОД (наприклад, УАТМ, мультиплексори, сервери) і розміщення РП ЦОД /комплексу. Панелі /шафи й устаткування РП поверху, сполучені із РП ЦОД /комплексу, також можуть перебувати в приміщенні апаратної.

Інтерфейси СКС це закінчення підсистем, що забезпечують підключення устаткування й кабелів зовнішніх служб методом підключення або комутації.

Для підключення до СКС досить одного мережевого кабелю. У варіанті комутації використовують мережевий і комутаційний кабель і додаткову панель.

Підключення до мережі загального користування здійснюється за допомогою інтерфейсу мережі загального користування. Місце розташування інтерфейсу мережі загального користування визначається національними, регіональними й місцевими правилами. Якщо інтерфейси мережі загального користування й СКС не з'єднані комутаційним кабелем або за допомогою устаткування, необхідно враховувати параметри проміжного кабелю.

Конфігурація. Розподільний пункт поверху

Як мінімум один РП поверху рекомендується на кожні 1000 квадратних метрів офісної площі. На кожному поверсі повинен бути, принаймні, один РП поверху. Якщо число робочих місць на поверсі невелико, його можна обслуговувати за допомогою розподільного пункту на суміжному поверсі.

Рекомендовані типи кабелів

У таблиці 1 дані рекомендації застосування різних типів середовища передачі в кожній з підсистем.

Таблиця 1 – Рекомендоване середовище передачі підсистем СКС

Підсистема	Тип середовища передачі	Застосунки
1	2	3
Горизонтальна підсистема	Симетричні кабелі	Мовні й інформаційні
	Оптоволоконі кабелі	Інформаційні
Магістральна підсистема ЦОД	Симетричні кабелі	Мовні й інформаційні класів А и В
	Оптоволоконі кабелі	Інформаційні класів В и вище

1	2	3
Магістральна підсистема комплексу	Оптоволоконі кабелі	Для всіх застосунків
	Симетричні кабелі	Для застосунків класу А (наприклад, лінії УАТМ)

Дані рекомендації застаріли – інформаційні застосунки класів А (до 0,1 МГц) і В (до 1,0 МГц) у локальних мережах практично не застосовуються. Вибір середовища передачі для магістралі ЦОД залежить від також від довжини каналів. Якщо довжина магістральної лінії не перевищує 90 метрів, симетричні кабелі відповідної категорії покликані забезпечити роботу всіх діючих застосунків.

З іншого боку, більшість багатомодових кабелів непридатні для роботи Gigabit Ethernet при довжині лінії більше 220 метрів (у відповідності зі стандартами максимальна довжина ОВ ММ магістралі – 2000 метрів).

Телекомунікаційні роз'єми (ТР)

Телекомунікаційні роз'єми розташовують на стіні, підлозі або в іншій точці робочої області. При проектуванні СКС варто забезпечити зручність доступу до всіх роз'ємів. Висока щільність роз'ємів підвищує гнучкість системи й полегшує зміни телекомунікаційних ресурсів робочих місць. У багатьох країнах на 10 м2 використовуваній площі повинні встановлюватися два телекомунікаційних роз'єми.

Допускається установка роз'ємів поодиноко або групами, однак кожне робоче місце повинне мати не менш двох роз'ємів.

На кожному робочому місці повинен бути передбачений, принаймні, одне роз'єми, установлений на симетричному кабелі 100 ом або 120 ом (перевага віддається кабелям 100 ом). Інші ТР потрібно встановлювати або на симетричним, або на оптоволоконому кабелі.

Симетричний кабель повинен мати дві або чотири пари; усе пари повинні бути змонтовані на роз'єми. Якщо передбачено менш чотирьох пар, це потрібно відбити в маркуванні. Додатка збалансованої передачі можуть мати обмеження по затримці поширення сигналів по кожній з пар. Особливості специфікації ТР, що відповідають перерахованим вище типам кабелів, дані в розділі «Вимоги до роз'ємів».

Роз'єми повинні бути позначені постійним маркуванням, видної користувачеві. Варто звертати увагу на те, щоб реєструвалося первісне призначення пар, а також всі наступні зміни. Хвильові й інші адаптери, використовувані для узгодження різних передавальних середовищ, повинні перебувати із зовнішньої сторони роз'єми. Дозволяється міняти призначення пар за допомогою адаптерів.

Телекомунікаційні приміщення й апаратні

Телекомунікаційне приміщення покликане забезпечувати наявність всіх засобів (простір, електроживлення, обігрів, вентиляція) для розташованих усередині нього пасивних елементів, активних пристроїв, а також інтерфейсів мережі загального користування. Для кожного телекомунікаційного приміщення варто передбачити прямий доступ до магістралі ЦОД.

Апаратна – простір у межах ЦОД, де розміщається телекомунікаційне устаткування й можуть перебувати або бути відсутніми розподільні пункти. До апаратної висувають інші вимоги, ніж до телекомунікаційних приміщень, оскільки устаткування, установлюване в них, є більше складним (наприклад, УАТМ або сервери). В апаратній може перебувати більше одного розподільного пункту. Якщо телекомунікаційне приміщення служить для розміщення двох і більше розподільних пунктів, його варто вважати апаратної.

Термін «телекомунікаційне приміщення» часто переводять як «телекомунікаційна шафа». Ці поняття не збігаються. Якщо використовується кілька шаф /стійок, неправильний переклад приводить до непорозумінь. Особливо серйозні помилки виникають при проектуванні системи заземлення й тлумаченні стандартів, що також використовують даний термін.

Пункт вводу в ЦОД

Пункти вводу в ЦОД обладнаються у випадку, коли зовнішні кабелі магістралі комплексу, приватних мереж і мережі загального користування (включаючи антену) уводять у ЦОД і здійснюють перехід на внутрішні кабелі. Місцеві правила можуть вимагати спеціального

комутаційного устаткування для оснащення зовнішніх кабелів роз'ємами. Це устаткування дозволяє перейти від зовнішніх до внутрішніх кабелів.

Електромагнітна сумісність

Міжнародні стандарти електромагнітних випромінювань і стійкості (наприклад, CISPR 22) і місцеві правила повинні бути прийняті в увагу. Кабельна система вважається пасивної й не може бути протестована на відповідність вимогам EMC індивідуально. Активне устаткування повинне відповідати вимогам відповідних стандартів EMC із урахуванням використовуваного середовища передачі.

Заземлення

Елементи системи заземлення повинні відповідати вимогам відповідних норм і правил. Інструкції й вимоги виробників устаткування варто виконувати, якщо вони сумісні з електричними нормативами.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів проектування структурованих кабельних мереж на базі використання Link Control. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем проектування структурованих кабельних мереж на базі використання Link Control; Досліджена система проектування структурованих кабельних мереж на базі використання Link Control; На основі отриманих результатів досліджень створена програмна реалізація системи проектування структурованих кабельних мереж на базі використання Link Control. Розроблені під час виконання роботи алгоритми дозволяють успішно вирішувати завдання проектування структурованих кабельних мереж на базі використання Link Control. 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. Богданова І.А. Дослідження та програмна реалізація системи проектування структурованих кабельних мереж на базі використання Link Control // Збірник праць молодих науковців ЦНТУ. – Вип. 11. – Кропивницький: ЦНТУ, 2021.
2. Semenov S. The method of processing and identification of telecommunication traffic based on BDS-tests / S. Semenov, A.Smirnov., E.Meleshko // The book of materials International Conference «Statistical Methods of Signal and Data Processing (SMSDP-2010)» –Kiev, Ukraine, National Aviation University "NAU-Druk" Publishing House, October 13-14, 2010. – С.166-168. – engl.
3. Семенов Ю.А. Сети Інтернет. Архитектура и протоколы / Ю.А. Семенов. – М.: Блик плюс, 1998. – 424 с.
4. 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.
5. 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.
6. 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.
7. 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.
8. Столлингс В. Современные компьютерные сети / Вильям Столлингс.– СПб.: Питер, 2003. – 778 с.
9. Сэломон Д. Сжатие данных, изображений и звука / Д. Сэломон. – М.: Техносфера, 2004. – 368 с.
10. Таненбаум Э. Компьютерные сети / Эндрю Таненбаум; пер. с англ. А. Леонтьев. – СПб.: Питер, 2002. — 848 с.

УДК 004

Д. Гіцеларь, магістр гр. КІ-19М-1,4
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ ІНТЕЛЕКТУАЛЬНОГО КЕРУВАННЯ ВІРТУАЛЬНОЮ МОБІЛЬНОЮ ПЛАТФОРМОЮ

У статті розроблено програмне забезпечення, яке призначено для системи інтелектуального керування віртуальною мобільною платформою. Метою розробки є дослідження та програмна реалізація системи інтелектуального керування віртуальною мобільною платформою. Об'єктом дослідження є процес інтелектуального керування віртуальною мобільною платформою. Предметом дослідження є методи інтелектуального керування віртуальною мобільною платформою. Методи дослідження базуються на методах інтелектуального керування, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи інтелектуального керування віртуальною мобільною платформою. 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, інтелектуальне керування, віртуальна мобільна платформа

Постановка проблеми. Враховуючи величезне поширення штучного інтелекту, недаремним буде рішення освоїти його роботу та навчитися з ним працювати. Тому у даній роботі була описана сфера використання штучного інтелекту. Наведені приклади використання у різних галузях. Також описано призначення систем емуляції дій людини та які взагалі вони бувають. Вказані переваги та недоліки кожної з них та чим вони відрізняються. Оскільки ця робота присвячується нейронним мережам, були описані їх підвиди та пояснений принцип функціонування. Увага наділилася й алгоритмам навчання нейронних мереж як важливій їх частині.

У ході роботи зустрічалися й певні проблеми. Тому була розписана суть цих проблем, пояснені причини виникнення та наведені конкретні способи їх вирішення, опираючись на дану роботу. Далі увага сконцентрувалася вже на реалізації самої системи. Спочатку були виділені підсистеми, які повинні виконувати назначену роль. На прикладі структурної, функціональної схем, діаграми процесів, а також блок-схем був описаний принцип дії всієї системи загалом та кожної з її підсистем. Були встановлені функціональні зв'язки між кожним модулем.

Наступним кроком детально описувався процес реалізації всіх модулів. Для кожного методу, що використовувався були вказані вхідні та вихідні дані, а також призначення. Після завершення реалізації залишалося лише навчити нейронну мережу. Для навчання був розроблений план дій та два етапи: попереднє навчання та основне навчання.

У результаті всієї виконаної роботи ми отримали мережу, яка по рівню гри лише трохи поступається звичайній людині.

Дана робота може використовуватися для демонстрації працюючої нейронної мережі студентам вищих навчальних закладів під час навчання. Вона може допомогти з поясненням функціонування нейронних мереж та віртуального середовища Unity як окремих елементів, так і систем, які взаємодіють одна з одною. Також отримані у результаті мережі можна використати у якості ворогів при розробці схожої комп'ютерної гри.

При роботі над проектом були використані такі наукові підходи:

– Порівняння. Використовувалося при визначенні найбільш оптимальних алгоритмів для реалізації поставленої задачі. Конкретні приклади: пошук способу отримання вхідних

даних для мережі; визначення алгоритму навчання мереж. Вимірювання. Використовувалося при створенні масивів вхідних даних, таких як дистанція до об'єктів.

- Формалізація. Використовувалася для опису алгоритмів при реалізації програмного забезпечення.
- Системний підхід. Допоміг уявити розроблювану гру у вигляді взаємодіючих систем.
- Аналіз та структурно-функціональний метод. Використовувалися, щоб розбити кожну систему на її складові.
- Абстрагування. Використовувався при дослідженні нейронної мережі, щоб виділити лише важливі для роботи його властивості.
- Моделювання. За його допомогою створювалося віртуальне середовище, танки, якими мали керувати нейронні мережі, а також при створенні самої нейронної мережі, яка є моделлю мозку людини.

Гіпотетико-дедуктивний метод та ймовірність. Використовувалися, щоб передбачити поведінку нейронних мереж для їх подальшого навчання.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи інтелектуального керування віртуальною мобільною платформою.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи інтелектуального керування віртуальною мобільною платформою.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем інтелектуального керування віртуальною мобільною платформою.

– Дослідження системи інтелектуального керування віртуальною мобільною платформою.

– Програмна реалізація системи інтелектуального керування віртуальною мобільною платформою.

Об'єктом дослідження є процес інтелектуального керування віртуальною мобільною платформою.

Предметом дослідження є методи інтелектуального керування віртуальною мобільною платформою.

Методи дослідження базуються на методах інтелектуального керування, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Тут ми переглянемо існуючі методи навчання та проаналізуємо їх. Розібравши їх принципи роботи, переваги та недоліки оберемо спосіб навчання, що найбільше відповідає умовам поставленої задачі.

Персептрон, зворотне розповсюдження похибки

Перцептрон, або персептрон – математична або комп'ютерна модель сприйняття інформації мозком (кібернетична модель мозку), запропонована Френком Розенблатом в 1957 році і вперше реалізована у вигляді електронної машини «Марк-1» в 1960 році. Перцептрон став однією з перших моделей нейромереж, а «Марк-1» – першим у світі нейрокомп'ютером.

Перцептрон складається з трьох типів елементів, а саме: сигнали, що надходять від датчиків (сенсорів, рецепторів), передаються асоціативним елементам, а потім реагуючим елементам. Таким чином, перцептрони дозволяють створити набір «асоціацій» між вхідними стимулами і необхідною реакцією на виході. У біологічному плані це відповідає перетворенню, наприклад, зорової інформації в фізіологічну відповідь від рухових нейронів. Відповідно до сучасної термінології, перцептрони можуть бути класифіковані як штучні нейронні мережі:

–з одним прихованим шаром;

–з пороговою функцією передачі;

–з прямим розповсюдженням сигналу.

Елементарний перцептрон складається з елементів трьох типів: S-елементів, A-елементів та одного R-елемента. S-елементи – це шар сенсорів або рецепторів. У фізичному втіленні вони

відповідають, наприклад, світлочутливим клітинам сітківки ока або фоторезисторам матриці камери. Кожен рецептор може перебувати в одному з двох станів – спокою або збудження, і тільки в останньому випадку він передає одиничний сигнал в наступний шар, асоціативним елементам.

А-елементи називаються асоціативними, тому що кожному такому елементу, як правило, відповідає цілий набір (асоціація) S-елементів. А-елемент активізується, як тільки кількість сигналів від S-елементів на його вході перевищило деяку величину θ. Таким чином, якщо набір відповідних S-елементів розташовується на сенсорному полі в формі літери «Д», А-елемент активізується, якщо достатня кількість рецепторів повідомило про появу «білої плями світла» в їх околиці, тобто А-елемент буде як би асоційований з наявністю / відсутністю літери «Д» в деякій області.

Сигнали від збуджених А-елементів, у свою чергу, передаються в суматор R, причому сигнал від i-го асоціативного елемента передається з коефіцієнтом w[i]. Цей коефіцієнт називається вагою A-R зв'язку.

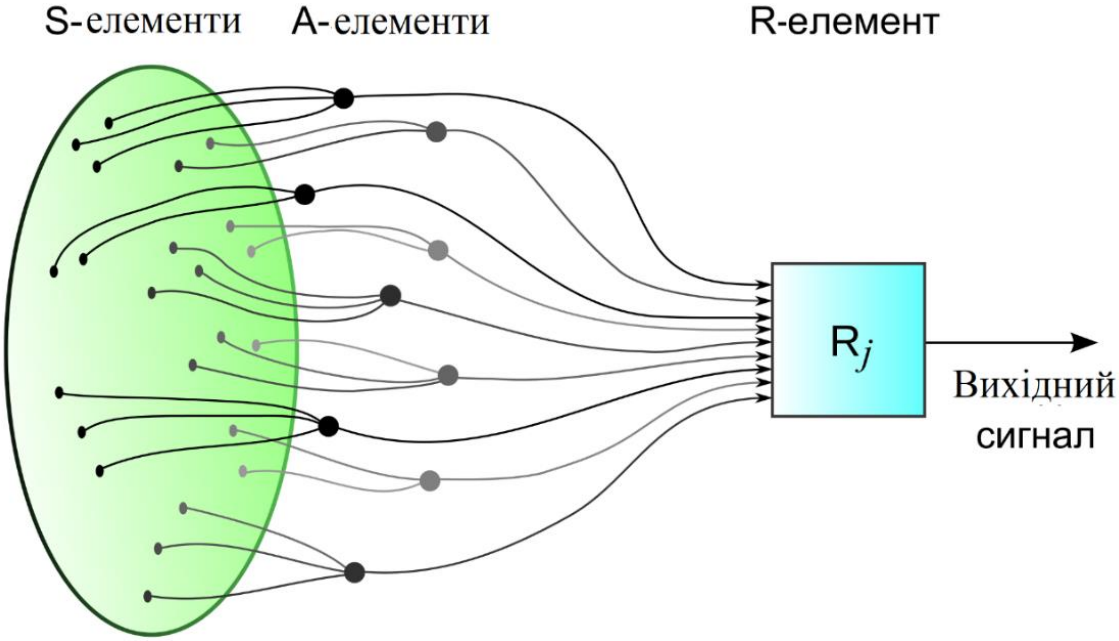


Рисунок 1 – Надходження сигналів з сенсорного поля в вирішальні блоки елементарного перцептрона в його фізичному втіленні[10]

Так само як і А-елементи, R-елемент підраховує суму значень вхідних сигналів, помножених на вагу (лінійну форму). R-елемент, а разом з ним і елементарний перцептрон, видає «1», якщо лінійна форма перевищує поріг θ, інакше на виході буде «-1». Математично, функцію, реалізовану R-елементом, можна записати так:

$$f(x) = sign\left(\sum_{i=1}^{n} wixi - \emptyset\right) \qquad (3.1)$$

Навчання елементарного перцептрона полягає в зміні вагових коефіцієнтів w[i] зв'язків A-R. Ваги зв'язків S-A (які можуть набувати значень {-1; 0; +1}) і значення порогів А-елементів вибираються випадковим чином на самому початку і потім не змінюються.

Після навчання перцептрон готовий працювати в режимі розпізнавання або узагальнення. В цьому режимі перцептрону пред'являються раніше невідомі йому об'єкти, і перцептрон повинен встановити, до якого класу вони належать.

INCLUDEPICTURE
"https://upload.wikimedia.org/wikipedia/commons/thumb/1/1e/Simple_perceptron.svg/1280px-Simple_perceptron.svg.png" * MERGEFORMATINET INCLUDEPICTURE
"https://upload.wikimedia.org/wikipedia/commons/thumb/1/1e/Simple_perceptron.svg/1280px-

Simple_perceptron.svg.png" * MERGEFORMATINET INCLUDEPICTURE "https://upload.wikimedia.org/wikipedia/commons/thumb/1/1e/Simple_perceptron.svg/1280px-Simple_perceptron.svg.png" * MERGEFORMATINET INCLUDEPICTURE "https://upload.wikimedia.org/wikipedia/commons/thumb/1/1e/Simple_perceptron.svg/1280px-Simple_perceptron.svg.png" * MERGEFORMATINET INCLUDEPICTURE "https://upload.wikimedia.org/wikipedia/commons/thumb/1/1e/Simple_perceptron.svg/1280px-Simple_perceptron.svg.png" * MERGEFORMATINET INCLUDEPICTURE "https://upload.wikimedia.org/wikipedia/commons/thumb/1/1e/Simple_perceptron.svg/1280px-Simple_perceptron.svg.png" * MERGEFORMATINET INCLUDEPICTURE "https://upload.wikimedia.org/wikipedia/commons/thumb/1/1e/Simple_perceptron.svg/1280px-Simple_perceptron.svg.png" * MERGEFORMATINET INCLUDEPICTURE "https://upload.wikimedia.org/wikipedia/commons/thumb/1/1e/Simple_perceptron.svg/1280px-Simple_perceptron.svg.png" * MERGEFORMATINET INCLUDEPICTURE "https://upload.wikimedia.org/wikipedia/commons/thumb/1/1e/Simple_perceptron.svg/1280px-Simple_perceptron.svg.png" * MERGEFORMATINET INCLUDEPICTURE "https://upload.wikimedia.org/wikipedia/commons/thumb/1/1e/Simple_perceptron.svg/1280px-Simple_perceptron.svg.png" * MERGEFORMATINET INCLUDEPICTURE "https://upload.wikimedia.org/wikipedia/commons/thumb/1/1e/Simple_perceptron.svg/1280px-Simple_perceptron.svg.png" * MERGEFORMATINET INCLUDEPICTURE "https://upload.wikimedia.org/wikipedia/commons/thumb/1/1e/Simple_perceptron.svg/1280px-Simple_perceptron.svg.png" * MERGEFORMATINET INCLUDEPICTURE "https://upload.wikimedia.org/wikipedia/commons/thumb/1/1e/Simple_perceptron.svg/1280px-Simple_perceptron.svg.png" * MERGEFORMATINET INCLUDEPICTURE "https://upload.wikimedia.org/wikipedia/commons/thumb/1/1e/Simple_perceptron.svg/1280px-Simple_perceptron.svg.png" * MERGEFORMATINET INCLUDEPICTURE "https://upload.wikimedia.org/wikipedia/commons/thumb/1/1e/Simple_perceptron.svg/1280px-Simple_perceptron.svg.png" * MERGEFORMATINET INCLUDEPICTURE "https://upload.wikimedia.org/wikipedia/commons/thumb/1/1e/Simple_perceptron.svg/1280px-Simple_perceptron.svg.png" * MERGEFORMATINET INCLUDEPICTURE "https://upload.wikimedia.org/wikipedia/commons/thumb/1/1e/Simple_perceptron.svg/1280px-Simple_perceptron.svg.png" * MERGEFORMATINET INCLUDEPICTURE "https://upload.wikimedia.org/wikipedia/commons/thumb/1/1e/Simple_perceptron.svg/1280px-Simple_perceptron.svg.png" * MERGEFORMATINET INCLUDEPICTURE "https://upload.wikimedia.org/wikipedia/commons/thumb/1/1e/Simple_perceptron.svg/1280px-Simple_perceptron.svg.png" * MERGEFORMATINET INCLUDEPICTURE "https://upload.wikimedia.org/wikipedia/commons/thumb/1/1e/Simple_perceptron.svg/1280px-Simple_perceptron.svg.png" * MERGEFORMATINET INCLUDEPICTURE "https://upload.wikimedia.org/wikipedia/commons/thumb/1/1e/Simple_perceptron.svg/1280px-Simple_perceptron.svg.png" * MERGEFORMATINET INCLUDEPICTURE "https://upload.wikimedia.org/wikipedia/commons/thumb/1/1e/Simple_perceptron.svg/1280px-Simple_perceptron.svg.png" * MERGEFORMATINET INCLUDEPICTURE "https://upload.wikimedia.org/wikipedia/commons/thumb/1/1e/Simple_perceptron.svg/1280px-Simple_perceptron.svg.png" * MERGEFORMATINET INCLUDEPICTURE "https://upload.wikimedia.org/wikipedia/commons/thumb/1/1e/Simple_perceptron.svg/1280px-Simple_perceptron.svg.png" * MERGEFORMATINET INCLUDEPICTURE "https://upload.wikimedia.org/wikipedia/commons/thumb/1/1e/Simple_perceptron.svg/1280px-Simple_perceptron.svg.png" * MERGEFORMATINET INCLUDEPICTURE "https://upload.wikimedia.org/wikipedia/commons/thumb/1/1e/Simple_perceptron.svg/1280px-Simple_perceptron.svg.png" * MERGEFORMATINET INCLUDEPICTURE "https://upload.wikimedia.org/wikipedia/commons/thumb/1/1e/Simple_perceptron.svg/1280px-Simple_perceptron.svg.png" * MERGEFORMATINET INCLUDEPICTURE "https://upload.wikimedia.org/wikipedia/commons/thumb/1/1e/Simple_perceptron.svg/1280px-

Simple_perceptron.svg.png" * MERGEFORMATINET INCLUDEPICTURE "https://upload.wikimedia.org/wikipedia/commons/thumb/1/1e/Simple_perceptron.svg/1280px-Simple_perceptron.svg.png" * MERGEFORMATINET INCLUDEPICTURE "https://upload.wikimedia.org/wikipedia/commons/thumb/1/1e/Simple_perceptron.svg/1280px-Simple_perceptron.svg.png" * MERGEFORMATINET INCLUDEPICTURE "https://upload.wikimedia.org/wikipedia/commons/thumb/1/1e/Simple_perceptron.svg/1280px-Simple_perceptron.svg.png" * MERGEFORMATINET INCLUDEPICTURE "https://upload.wikimedia.org/wikipedia/commons/thumb/1/1e/Simple_perceptron.svg/1280px-Simple_perceptron.svg.png" * MERGEFORMATINET INCLUDEPICTURE "https://upload.wikimedia.org/wikipedia/commons/thumb/1/1e/Simple_perceptron.svg/1280px-Simple_perceptron.svg.png" * MERGEFORMATINET INCLUDEPICTURE "https://upload.wikimedia.org/wikipedia/commons/thumb/1/1e/Simple_perceptron.svg/1280px-Simple_perceptron.svg.png" * MERGEFORMATINET INCLUDEPICTURE "https://upload.wikimedia.org/wikipedia/commons/thumb/1/1e/Simple_perceptron.svg/1280px-Simple_perceptron.svg.png" * MERGEFORMATINET INCLUDEPICTURE "https://upload.wikimedia.org/wikipedia/commons/thumb/1/1e/Simple_perceptron.svg/1280px-Simple_perceptron.svg.png" * MERGEFORMATINET INCLUDEPICTURE "https://upload.wikimedia.org/wikipedia/commons/thumb/1/1e/Simple_perceptron.svg/1280px-Simple_perceptron.svg.png" * MERGEFORMATINET INCLUDEPICTURE "https://upload.wikimedia.org/wikipedia/commons/thumb/1/1e/Simple_perceptron.svg/1280px-Simple_perceptron.svg.png" * MERGEFORMATINET INCLUDEPICTURE "https://upload.wikimedia.org/wikipedia/commons/thumb/1/1e/Simple_perceptron.svg/1280px-Simple_perceptron.svg.png" * MERGEFORMATINET INCLUDEPICTURE "https://upload.wikimedia.org/wikipedia/commons/thumb/1/1e/Simple_perceptron.svg/1280px-Simple_perceptron.svg.png" * MERGEFORMATINET INCLUDEPICTURE "https://upload.wikimedia.org/wikipedia/commons/thumb/1/1e/Simple_perceptron.svg/1280px-Simple_perceptron.svg.png" * MERGEFORMATINET INCLUDEPICTURE "https://upload.wikimedia.org/wikipedia/commons/thumb/1/1e/Simple_perceptron.svg/1280px-Simple_perceptron.svg.png" * MERGEFORMATINET INCLUDEPICTURE "https://upload.wikimedia.org/wikipedia/commons/thumb/1/1e/Simple_perceptron.svg/1280px-Simple_perceptron.svg.png" * MERGEFORMATINET INCLUDEPICTURE "https://upload.wikimedia.org/wikipedia/commons/thumb/1/1e/Simple_perceptron.svg/1280px-Simple_perceptron.svg.png" * MERGEFORMATINET INCLUDEPICTURE "https://upload.wikimedia.org/wikipedia/commons/thumb/1/1e/Simple_perceptron.svg/1280px-Simple_perceptron.svg.png" * MERGEFORMATINET INCLUDEPICTURE "https://upload.wikimedia.org/wikipedia/commons/thumb/1/1e/Simple_perceptron.svg/1280px-Simple_perceptron.svg.png" * MERGEFORMATINET INCLUDEPICTURE "https://upload.wikimedia.org/wikipedia/commons/thumb/1/1e/Simple_perceptron.svg/1280px-Simple_perceptron.svg.png" * MERGEFORMATINET

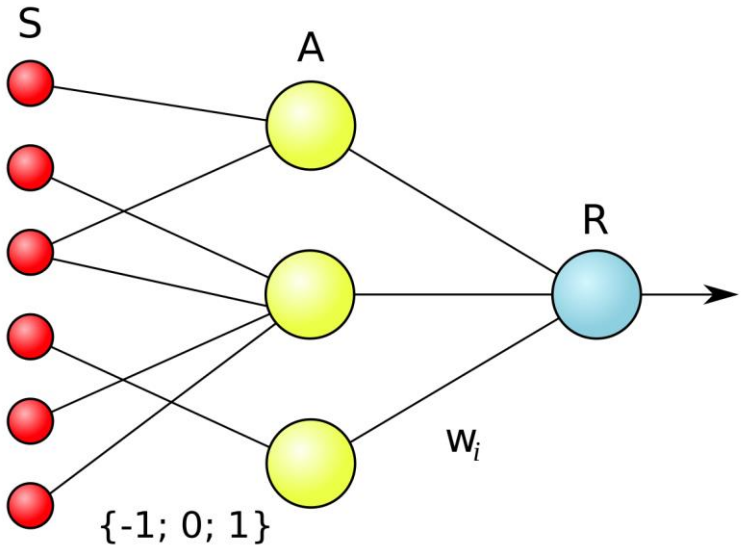


Рисунок 2 – Логічна схема елементарного перцептрона. Ваги S-A зв'язків можуть мати значення -1, +1 або 0 (тобто відсутність зв'язку). Ваги A-R зв'язків W можуть бути будь-якими[10]

Для навчання багатошарових мереж рядом вчених, в тому числі Д.Румельхартом, був запропонований градієнтний алгоритм навчання з учителем, який проводить сигнал помилки, обчислений виходами перцептрону, до його входів, шар за шаром. Зараз це найпопулярніший метод навчання багатошарових перцептронів. Його перевага в тому, що він може навчити всі шари нейронної мережі, і його легко прорахувати локально. Однак цей метод є дуже довгим, до того ж, для його застосування потрібно, щоб передавальна функція нейронів могла диференціюватися. При цьому в перцептронах довелося відмовитися від бінарного сигналу, і користуватися на вході безперервними значеннями.

Нейронні мережі без вчителя, класифікатори

Головна риса, що робить навчання без учителя привабливим, – це його "самостійність". Процес навчання, як і в разі навчання з учителем, полягає в підлаштуванні ваг синапсів. Деякі алгоритми, правда, змінюють і структуру мережі, тобто кількість нейронів і їх взаємозв'язки, але такі перетворення правильніше назвати більш широким терміном – самоорганізацією, і в рамках цього розділу вони розглядатися не будуть. Очевидно, що підлаштування синапсів може проводитися тільки на підставі інформації, доступної в нейроні, тобто його стану і вже наявних вагових коефіцієнтів. Виходячи з цього міркування і, що більш важливо, за аналогією з відомими принципами самоорганізації нервових клітин, побудовані алгоритми навчання Хебба.

Сигнальний метод навчання Хебба полягає в зміні ваг за наступним правилом:

$$w_{ij}(t) = w_{ij}(t-1) + a * y_i^{(n-1)} * y_j^{(n)}, \qquad (3.2)$$

де $y_i^{(n-1)}$ – вихідне значення нейрона і шару (n-1), $y_j^{(n)}$ – вихідне значення нейрона j шару n; $w_{ij}^{(t)}$ і $w_{ij}^{(t-1)}$ – ваговий коефіцієнт синапсу, що з'єднує ці нейрони, на ітераціях t і t-1 відповідно; a – коефіцієнт швидкості навчання. Тут і далі, для спільності, під n мається на увазі довільний шар мережі. При навчанні за цим методом посилюються зв'язки між збудженими нейронами.

Існує також і диференційний метод навчання Хебба.

$$w_{ij}(t) = w_{ij}(t-1) + a * \left[y_i^{(n-1)}(t) - y_i^{(n-1)}(t-1)\right] * \\ * \left[y_j^{(n)}(t) - y_j^{(n)}(t-1)\right] \qquad (3)$$

Тут $y_i^{(n-1)}(t)$ і $y_i^{(n-1)}(t-1)$ – вихідне значення нейрона і шару n-1 відповідно на ітераціях t і t-1; $y_j^{(n)}(t)$ і $y_j^{(n)}(t-1)$ – те ж саме для нейрона j шару n. Як видно з формули, найсильніше навчаються синапси, що з'єднують ті нейрони, виходи яких найбільш динамічно змінилися в бік збільшення.

Повний алгоритм навчання із застосуванням вищенаведених формул буде виглядати так:

1. На стадії ініціалізації всім ваговим коефіцієнтам привласнюються невеликі випадкові значення.

2. На входи мережі подається вхідний образ, і сигнали збудження поширюються по всім верствам згідно з принципами класичних прямопоточних (feedforward) мереж, тобто для кожного нейрона розраховується зважена сума його входів, до якої потім застосовується активаційна (передавальна) функція нейрона, в результаті чого виходить його вихідне значення $y_i^{(n)}$, i = 0 ... M_i-1, де M_i – число нейронів в шарі i; n = 0 ... N-1, а N – число шарів в мережі.

3. На підставі отриманих вихідних значень нейронів по одній з формул проводиться зміна вагових коефіцієнтів.

4. Цикл з кроку 2, поки вихідні значення мережі не стабілізуються із заданою точністю. Застосування цього нового способу визначення завершення навчання, відмінного від зворотного поширення, обумовлено тим, що значення синапсів, що підлаштовуються, фактично не обмежені.

На другому кроці циклу поперемінно пред'являються всі образи із вхідного набору.

Слід зазначити, що вид відгуків на кожен клас вхідних образів не відомий заздалегідь і буде являти собою довільне поєднання станів нейронів вихідного шару, обумовлене випадковим розподілом ваг на стадії ініціалізації. Разом з тим, мережа здатна узагальнювати схожі образи, відносячи їх до одного класу. Тестування навченої мережі дозволяє визначити топологію класів у вихідному шарі. Для приведення відгуків навченої мережі до зручного подання можна доповнити мережу одним шаром, який, наприклад, за алгоритмом навчання одношарового перцептрона необхідно змусити відображати вихідні реакції мережі в необхідні образи.

Інший алгоритм навчання без учителя – алгоритм Кохонена – передбачає підлаштування синапсів на підставі їх значень від попередньої ітерації.

$$w_{ij}(t) = w_{ij}(t-1) + a * \left[y_i^{(n-1)} - w_{ij}(t-1) \right] \qquad (3.4)$$

З вищенаведеної формули видно, що навчання зводиться до мінімізації різниці між вхідними сигналами нейрона, які надходять з виходів нейронів попереднього шару $y_i^{(n-1)}$, і ваговими коефіцієнтами його синапсів.

Повний алгоритм навчання має приблизно таку ж структуру, як в методах Хебба, але на кроці 3 з усього шару вибирається нейрон, значення синапсів якого максимально схожі на вхідний образ, і підлаштування ваг за формулою (4) проводиться тільки для нього. Ця, так звана, акредитація може супроводжуватися загальмуванням всіх інших нейронів шару і введенням обраного нейрона в насичення. Вибір такого нейрона може здійснюватися, наприклад, розрахунком скалярного добутку вектора вагових коефіцієнтів з вектором вхідних значень. Максимальний добуток дає потрібний нейрон.

Інший варіант – розрахунок відстані між цими векторами в p-вимірному просторі, де p – розмір векторів.

$$D_j = \sqrt{\sum_{i=0}^{p-1} \left(y_i^{(n-1)} - w_{ij} \right)^2}, \qquad (3.5)$$

де j – індекс нейрона в шарі n, i – індекс підсумовування по нейронах шару (n-1), w_{ij} – вага синапсу, що з'єднує нейрони; виходи нейронів шару (n-1) є вхідними значеннями для шару n. Корінь у формулі (5) брати не обов'язково, так як важлива лише відносна оцінка різних D_j.

В даному випадку, "перемагає" нейрон з найменшою відстанню. Іноді нейрони, які занадто часто отримують акредитацію, примусово виключаються з розгляду, щоб "зрівняти права" всіх нейронів шару. Найпростіший варіант такого алгоритму полягає в гальмуванні нейрона, який тільки що виграв.

При використанні навчання за алгоритмом Кохонена існує практика нормалізації вхідних образів, а також – на стадії ініціалізації – і нормалізації початкових значень вагових коефіцієнтів.

$$x_i = x_i \Big/ \sqrt{\sum_{j=0}^{n-1} x_j^2}\,, \qquad (3.6)$$

де x_i – і-а компонента вектора вхідного образа або вектора вагових коефіцієнтів, а n – його розмірність. Це дозволяє скоротити тривалість процесу навчання.

Ініціалізація вагових коефіцієнтів випадковими значеннями може привести до того, що різні класи, яким відповідають щільно розподілені вхідні образи, зіллються або, навпаки, розділяться на додаткові підкласи в разі близьких образів одного й того ж класу. Для уникнення такої ситуації використовується метод опуклої комбінації. Суть його зводиться до того, що вхідні нормалізовані образи піддаються перетворенню:

$$x_i = a(t) * x_i + \big(1 - a(t)\big) * \frac{1}{\sqrt{n}}\,, \qquad (3.7)$$

де x_i – і-а компонента вхідного образу, n – загальне число його компонент, а (t) – коефіцієнт, що змінюється в процесі навчання від нуля до одиниці, в результаті чого спочатку на входи мережі подаються практично однакові образи, а з плином часу вони все більше сходяться до вихідних. Вагові коефіцієнти встановлюються на кроці ініціалізації рівними величині

$$w_o = \frac{1}{\sqrt{n}}\,, \qquad (3.8)$$

де n – розмірність вектора ваг для нейронів шару, що ініціалізується.

На основі розглянутого вище методу будуються нейронні мережі особливого типу – так звані структури, що самоорганізуються – self-organizing feature maps. Для них після вибору з шару n нейрона j з мінімальною відстанню D_j (5) навчається за формулою (4) не тільки цей нейрон, але і його сусіди, розташовані в околиці R. Величина R на перших ітераціях дуже велика, так що навчаються всі нейрони , але з плином часу вона зменшується до нуля. Таким чином, чим ближче кінець навчання, тим точніше визначається група нейронів, що відповідають кожному класу образів.

Еволюційні методи навчання мереж

Найбільш прийнятним способом налаштування вагових коефіцієнтів штучних нейронних мереж можна вважати генетичні алгоритми. Це пов'язано з тією обставиною, що на початковій стадії немає абсолютно ніякої інформації про напрямок руху в плані налаштування ваг матриці. В умовах невизначеності еволюційні методи, в тому числі і генетичні алгоритми, мають найбільш високі шанси для досягнення необхідних результатів. Класичний генетичний алгоритм оперує двійковій системою числення, хоча останнім часом часто зустрічаються роботи, в яких оператори генетичних алгоритмів виконують операції над безліччю дійсних чисел. Це дозволяє істотно розширити можливості застосування описуваних алгоритмів.

Як тільки певний вид еволюції вводиться в штучну нейронну мережу, відразу виникає потреба у відповідній йому схемі хромосомного представлення даних, тобто повинен бути створений спосіб генетичного кодування особин популяції.

Розглянемо математичну модель поставленої задачі. Дано вектор X з розмірністю 256, який являє собою закодоване зображення відомого символу, що розпізнається. Також є вектор Y з розмірністю 10, який відображає необхідний результат розпізнавання, що вказує приналежність символу до еталонному зразку. Необхідно знайти вагову матрицю W, елементами якої є дійсні числа в відрізку [0;1], щоб виконувалася рівність:

$$X*W = Y \qquad (9)$$

Необхідно здійснити корегування вагової матриці W за допомогою генетичного алгоритму. В рамках розв'язуваної задачі розглянута матриця має таку розмірність: кількість рядків дорівнює 10, що представляє собою всі символи, що описують арабські цифри; кількість стовпців визначається розміром знакомісця, що відводиться під кожен символ, 256 стовпців.

З точки зору очевидності і простоти розуміння слід кожен стовпець матриці ваг розглядати як хромосому, що призведе до наявності 256 хромосом, які в сукупності будуть відображати кожну особину. Однак при практичній реалізації набагато зручніше використовувати більш просту структуру, хоча і менш наочну. Це пов'язано з тим, що досить важко реалізувати операції кросинговеру і мутації при наявності декількох хромосом. Кожну особину в генетичному алгоритмі, який розробляється, можна представити у вигляді тільки однієї хромосоми, що значно спростить програмну реалізацію на ЕОМ. Цього можна досягти наступним способом. Хромосома буде починатися з першого стовпчика матриці ваг, і кожен наступний стовпець буде просто додаватися в кінець вже існуючої «єдиної» хромосоми. Даний метод проілюстровано на рисунку 3.

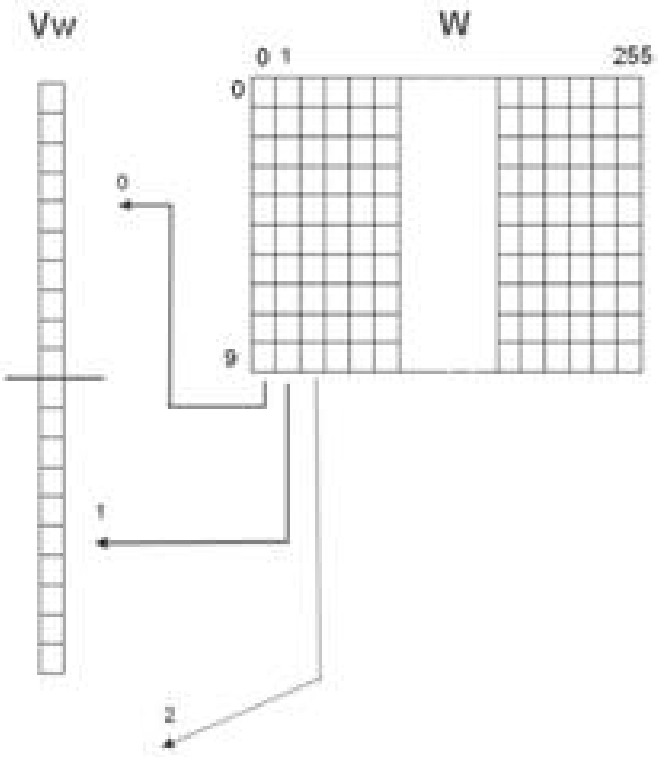


Рисунок 3 – Перетворення вагової матриці W в вектор ваг Vw

Класичний генетичний алгоритм складається з ряду найбільш важливих етапів. Фактично дані етапи можна розташувати в хронологічному порядку.

- Ініціалізація – формування початкової популяції.
- Оцінка пристосувань – обчислення функції придатності для кожної особини (в нашому випадку хромосоми).
- Селекція – вибірка на основі оцінки пристосованості найбільш пристосованих хромосом, яким буде надано право участі в операціях кросинговеру.
- Кросинговер – схрещування двох особин.
- Мутація – навмисна штучна зміна певних генів в хромосомах особини.
- Формування нової популяції – зниження кількості особин на основі оцінки пристосованості разом з вибором «найкращої» особини.
- Перевірка критерію зупинки алгоритма – якщо необхідна умова пошуку досягнута – вихід, в іншому випадку – перехід до етапу № 3.
- Витяг найкращого рішення – найкращим рішенням вважається особина з максимальним значенням функції придатності.

Метод створення систем керування з використанням віртуального простору

Як я вже описував у попередньому розділі, система буде керуватися тридцятьма двома променями, які побудовані рівномірно по колу від напрямку руху танку за допомогою вбудованих можливостей Unity Raycast. Промені посилаються у певному напрямку до відстані «горизонту», як показано на рисунку 4. Червоним позначено побачені перешкоди, а зеленим напрям та відстань до ворога.

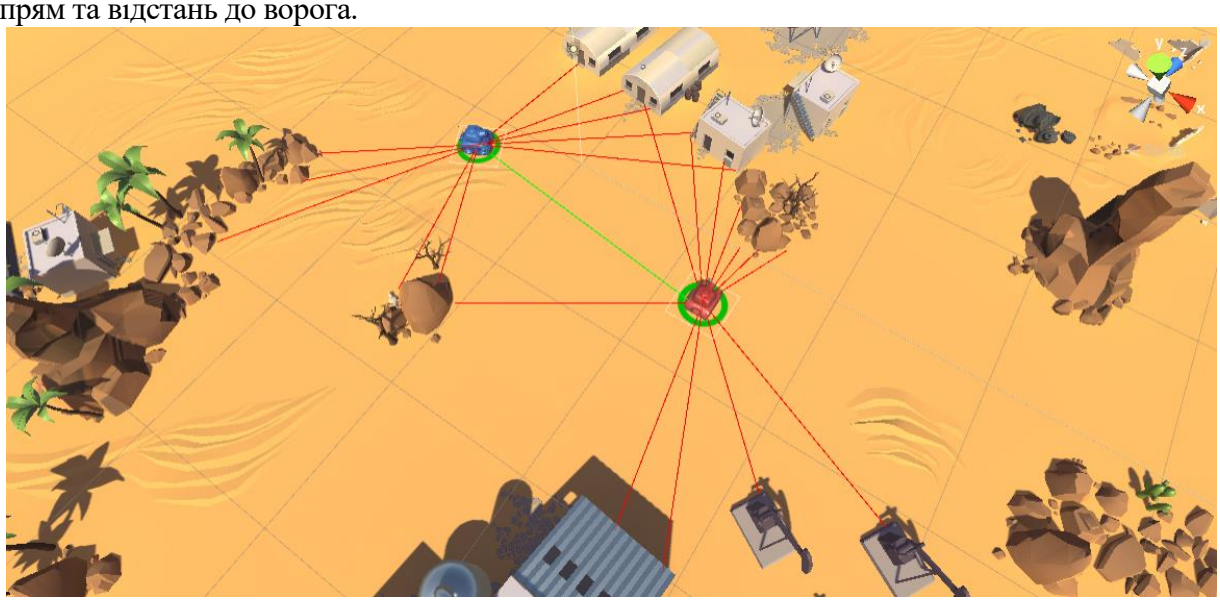


Рисунок 4 – Демонстрація створення рейкастів

Відповідно випущеним 32-м променям формується одновимірний масив з 32-х елементів зі значенням від 0 до 1, які відповідають відносній відстані по відповідному напрямку до перешкод. Відстань 1 позначає відсутність перешкод до лінії горизонту; 0 – перешкода знаходиться впритул до танку. Аналогічно будується масив пошуку супротивника або супротивників – одиничні значення означають відстань до супротивника за умовним горизонтом, а значення менше одиниці пропорційне відстані до суперника.

Відповідно двом масивам по 32 значення, тридцять два вхідні нейрони будуть відповідати за відстань до перешкод, така ж кількість за напрям до супротивника. Ці вхідні масиви формують вхідний шар з 64-х нейронів. Наступним шаром з 64-х нейронів повинна проводиться попередня обробка інформації, після чого інформація передається до шару суміщення інформацій від перешкод та положення супротивника. Вихідний шар має п’ять виходів. Прийнятим рішенням вважається вихід, який має максимальний вихідний рівень.

Отримана архітектура НМ проілюстрована на рисунку 5:

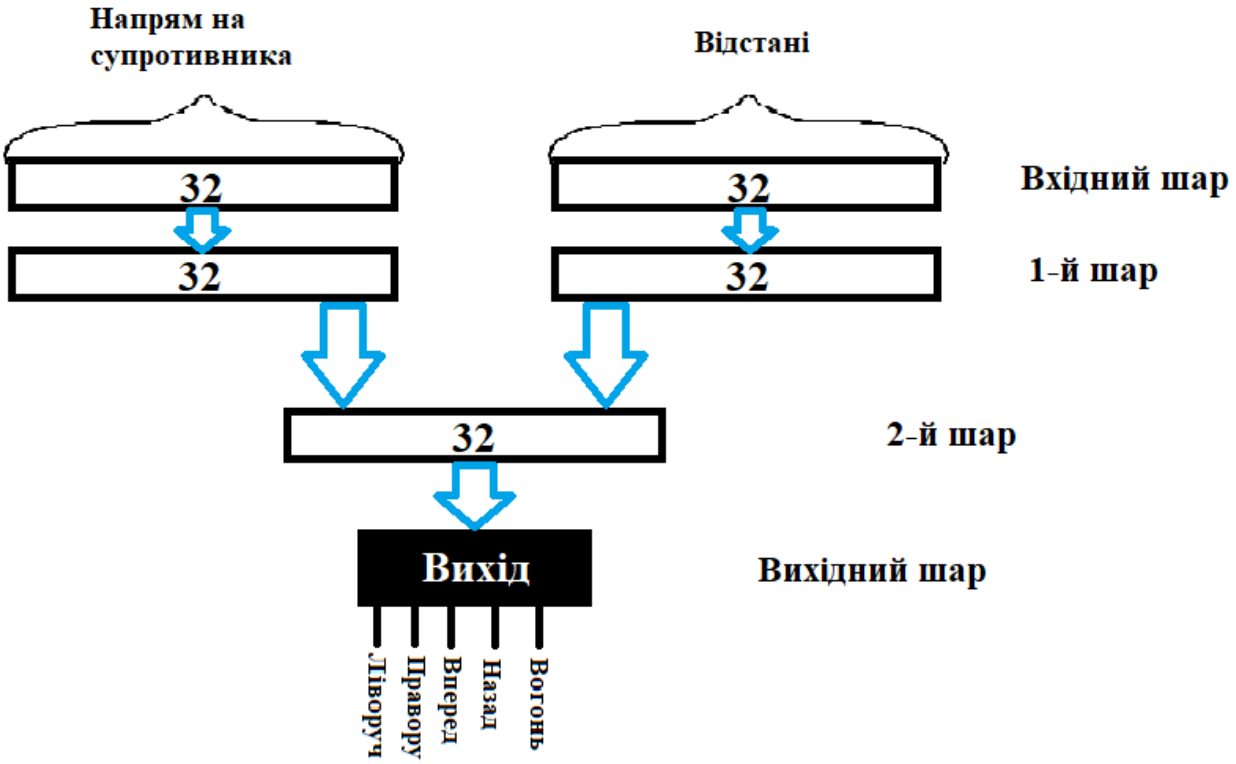


Рисунок 5 – Архітектура нейронної мережі

Наступним етапом є навчання нейронної мережі для отримання правильного вихідного сигналу в залежності від значень вхідних даних. Для цього спочатку потрібно забезпечити мережу початковими знаннями. Інакше вона буде не здатна виконати навіть найпростіші дії. Реалізувати початкове навчання можна використовуючи алгоритм зворотного розповсюдження похибки. При цьому варто застосовувати різні методи оптимізації та швидкість навчання. Дані, на які має рівнятися мережа, візьмемо зігравши певну кількість разів вручну. Необхідно записати до файлу вхідні масиви та стани нажатих людиною кнопок у кожен момент часу під час гри.

У результаті початкового навчання отримаємо вихідні файли із корегованими вагами нейронних мереж, які ми передаємо до основного алгоритму навчання, яке буде відбуватися автоматично. Повністю навчити мережу використовуючи зворотне розповсюдження похибки не вдасться тому, що необхідна велика кількість вхідних даних, отримання яких займе багато часу. Хід процесу початкового навчання показаний на рисунку 6 у вигляді графіку.

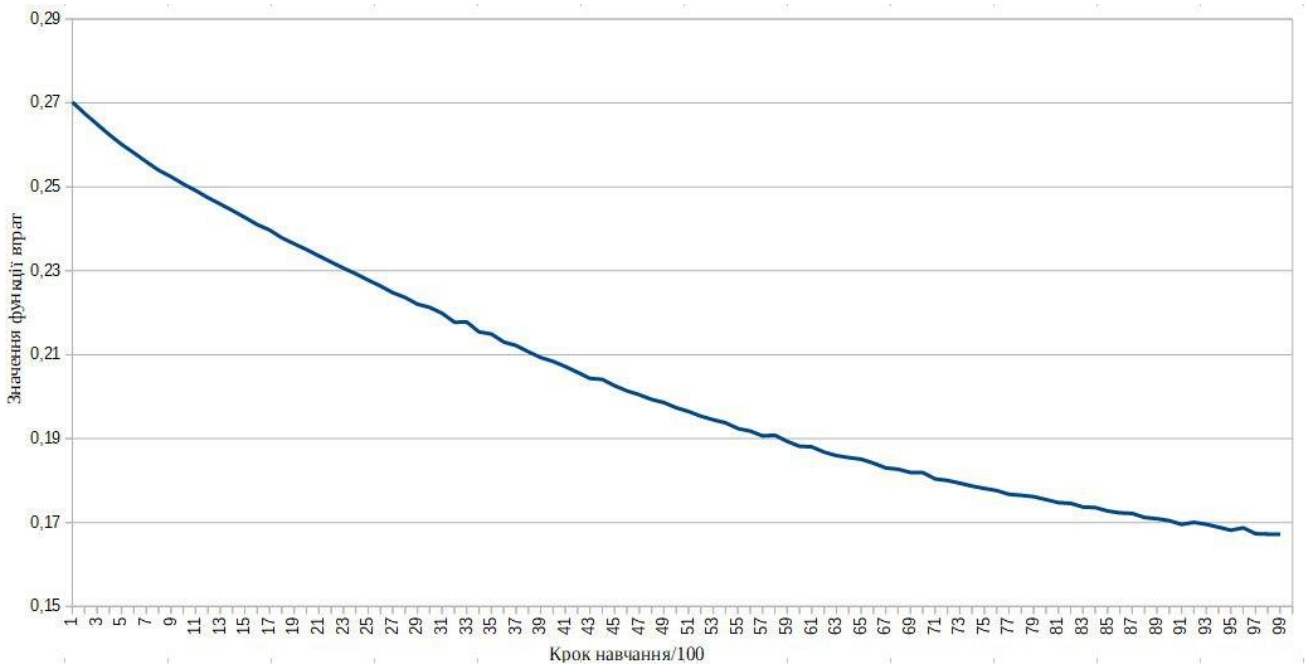


Рисунок 6 – Динаміка функції похибки в процесі навчання мережі

Розробка структурної схеми

Навчання системи повинна забезпечувати значна кількість факторів. До них належить віртуальний світ із різноманітними перешкодами. Вони слугуватимуть місцем для навчання. Система виявлення перешкод та супротивника надаватиме нейронній мережі вхідні дані, які оброблятимуться у подальшому для отримання потрібного вихідного сигналу. Система формування унікальної вибірки двох мереж відповідатиме за вибір двох мереж які будуть битися між собою. Система керування забезпечить інтерфейс взаємодії як мережі, так і людини з віртуальною платформою. Система забезпечення розрахунків нейронної мережі завантажуватиме потрібну мережу з файлу, оброблятиме отримані вхідні дані та видаватиме вихідний сигнал. Система оцінювання дій мережі допомагатиме виявляти найбільш здібні мережі, нараховуючи бали або віднімаючи їх за конкретні дії. Система запуску сеансу змагання мереж починатиме бій та визначатиме переможця.

Система сортування мереж за ефективністю по набраним балам сумуватиме усі бали, нараховані системою оцінювання дій та сортуватиме мережі за цим показником від більшого до меншого.

Система зберігання популяції мереж вилучатиме всі мережі крім десятки найкращих, з яких потім породжуються по дев’ять нащадків. Це дозволить утримувати кількість мереж у числі 100.

Це компоненти основного ПЗ. Крім нього буде створений невеликий додаток де встановлюватимуться початкові налаштування до головної системи.

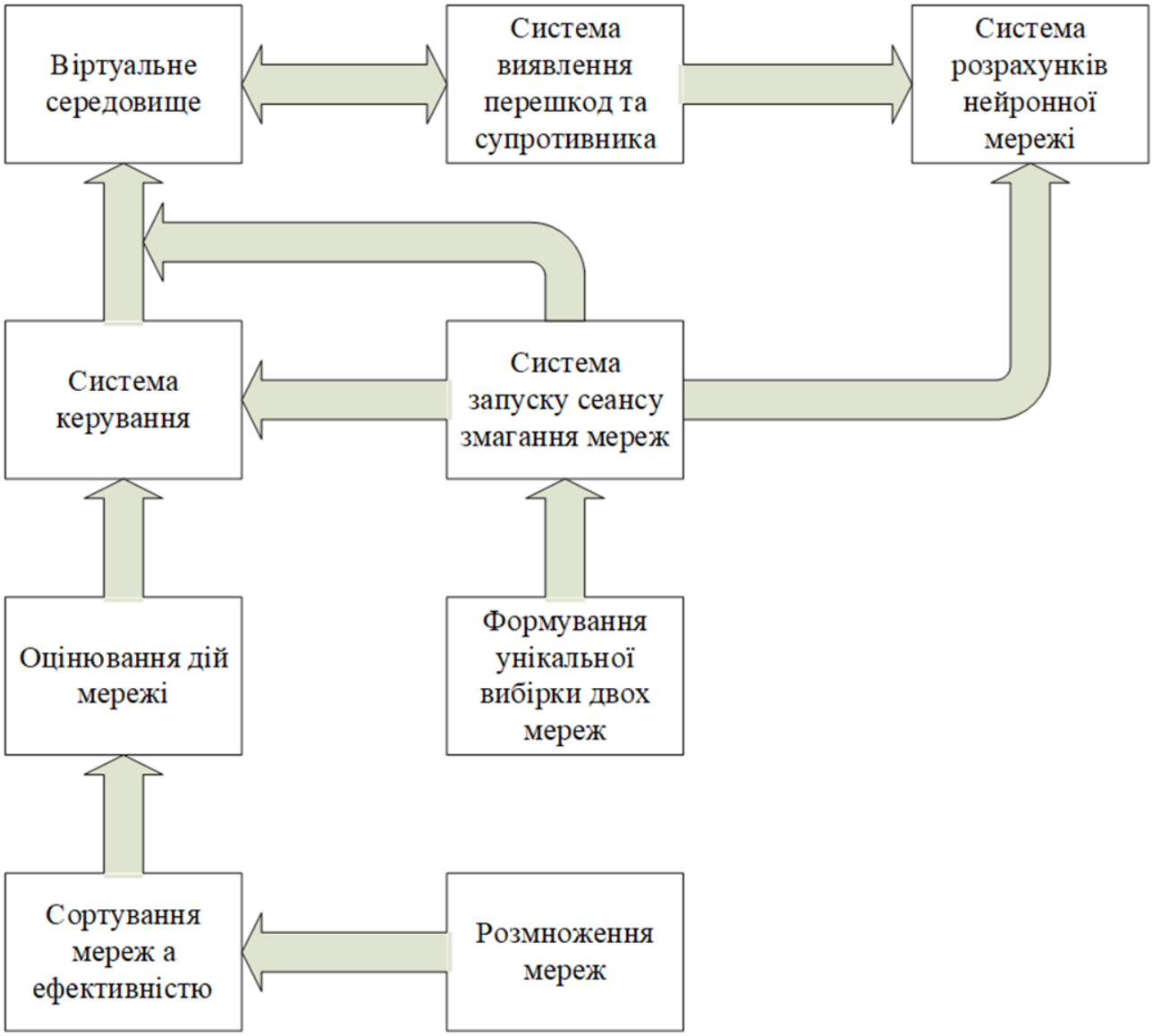


Рисунок 7 – Структурна схема ПЗ

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів інтелектуального керування віртуальною мобільною платформою. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем інтелектуального керування віртуальною мобільною платформою; Досліджена система інтелектуального керування віртуальною мобільною платформою; На основі отриманих результатів досліджень створена програмна реалізація системи інтелектуального керування віртуальною мобільною платформою. Розроблені під час виконання роботи алгоритми дозволяють успішно вирішувати завдання інтелектуального керування віртуальною мобільною платформою. 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. 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.
2. Гіцеларь Д.В. Дослідження та програмна реалізація системи інтелектуального керування віртуальною

мобільною платформою // Збірник праць молодих науковців ЦНТУ. – Вип. 11. – Кропивницький: ЦНТУ, 2021.
3. 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.
4. 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.
5. 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.
6. 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.
7. 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.
8. 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
9. 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
10. Джарратано Д. Экспертные системы: принципы разработки и программирование / Д. Джарратано, Г. Райли. – Москва: Издательский дом "Вильямс", 2007. – 1125 с.

УДК 004

В. Головатій, магістр гр. КІ-19МЗ
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ МОНІТОРИНГУ МЕРЕЖІ ПІДПРИЄМСТВА НА ОСНОВІ КОМУТАТОРІВ NEXUS 9000

У статті розроблено програмне забезпечення, яке призначено для системи моніторингу мережі підприємства на основі комутаторів Nexus 9000. Метою розробки є дослідження та програмна реалізація системи моніторингу мережі підприємства на основі комутаторів Nexus 9000. Об'єктом дослідження є процес моніторингу мережі підприємства на основі комутаторів Nexus 9000. Предметом дослідження є методи моніторингу мережі підприємства на основі комутаторів Nexus 9000. Методи дослідження базуються на методах теорії телетрафіку, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи моніторингу мережі підприємства на основі комутаторів Nexus 9000.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, моніторингу мережі, Nexus 9000

Постановка проблеми. Проблеми в роботі мережі можуть значно погіршувати якість обслуговування користувачів, знижуючи ступінь їхньої задоволеності мережевими сервісами й породжуючи невдоволення тими, хто надає ці сервіси. Тому надто важливо максимально швидко виявляти, діагностувати й усувати проблеми. Різні системи мережевого моніторингу й діагностичні засоби прискорюють виявлення й аналіз проблем і тим самим сприяють скороченню періоду часу між появою проблеми і її усуненням. Більше того, збираючи й аналізуючи інформацію про роботу мережі, засоби моніторингу дозволяють виявляти можливі проблеми й не допускати їхнього виникнення.

Для забезпечення якості мережевих послуг IT-фахівці усе більше уваги приділяють контролю роботи застосунків і сервісів замість моніторингу стану окремих інфраструктурних мережевих пристроїв. Щоб оцінювати якість роботи сервісів, необхідно захоплювати їх трафік у різних точках мережі (наприклад, до й після балансувальника навантаження, сервера бази даних і ін.) і аналізувати його. Аналіз трафіку здійснюється також для оптимізації роботи мережі, виявлення хакерської активності й в інших цілях.

Підприємства зацікавлені в повному контролі роботи своїх мереж. При цьому збирається й аналізується інформація про обсяги переданого трафіку, що породжують найбільший трафік вузлах, затримках у роботі мережі й застосунків, споживанні смуги пропущення мережі різними додатками й клієнтами й ін. Ці відомості допомагають виявляти ті вузли, які найбільше навантажують мережа й усувати проблеми в роботі застосунків.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи моніторингу мережі підприємства на основі комутаторів Nexus 9000.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи моніторингу мережі підприємства на основі комутаторів Nexus 9000.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем моніторингу мережі підприємства на основі комутаторів Nexus 9000.

– Дослідження системи моніторингу мережі підприємства на основі комутаторів Nexus 9000.

– Програмна реалізація системи моніторингу мережі підприємства на основі комутаторів Nexus 9000.

Об'єктом дослідження є процес моніторингу мережі підприємства на основі комутаторів Nexus 9000.

Предметом дослідження є методи моніторингу мережі підприємства на основі комутаторів Nexus 9000.

Методи дослідження базуються на методах теорії телетрафіку, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Очевидно, куди простіше попередити неполадки в мережі, ніж виправляти вже виниклі проблеми. Моніторинг серверів, виконуваних на них застосунків і мережевих пристроїв допоможе завчасно довідатися про потенційні несправності й запобігти їх наслідкам. Відслідковуючи функціонування мережі й зберігаючи передісторію її роботи, адміністратор до того ж може надати точну інформацію користувачам, у яких іноді складається невірне подання про частоту появи різних несправностей. Не менш важливо, що мережевий моніторинг дозволяє одержувати точні відомості про події в мережі, а також часу й джерелах звернень до мережі.

Отже, існує два типи моніторингу. Перший з них ми будемо називати оперативним моніторингом (operations monitoring), а другий – моніторингом безпеки (security monitoring).

Великі підприємства іноді ділять ці два типи моніторингу на два окремих процеси, виконувані співробітниками виробничих підрозділів і IT-безпеки, але малі й середні компанії з ряду причин частіше організують загальний процес моніторингу. Незалежно від розміру бюджету й числа співробітників, мережі малих і середніх компаній звичайно не мають потреби в такому ж рівні поточного оперативного моніторингу, як у великих корпораціях. Мережі малих підприємств завантажені не настільки інтенсивно, як корпоративні, і обслуговувати їх не так складно. Крім того, технічні проекти малих компаній простіше, і вони не мають потреби в детальному аналізі тенденцій і звітах, необхідних в установах з більше повільними процедурами прийняття рішень.

Спочатку розглянемо ті різні пристрої й системи малого підприємства, які необхідно контролювати як з метою безпеки, так і по виробничих причинах, і визначимо типові джерела даних, що відслідковуються, у тому числі журнали подій Windows, Syslog і SNMP. Далі

покажемо, як побудувати елементарне рішення для моніторингу мережі за допомогою безкоштовних і недорогих інструментів.

Об'єкти моніторингу

Дані, що надходять від контрольованих пристроїв, називаються телеметричними. Які протоколи й формати даних звичайно використовуються для передачі телеметрії? Як відслідковувати різні джерела даних і генерувати попередження й звіти, щоб перетворити дані в інформацію? Одне з найважливіших завдань – вирішити, на підставі яких даних необхідно генерувати попередження в реальному часі, які дані варто вносити в щоденні й щотижневі звіти і які дані потрібно просто архівувати.

З метою безпеки корисно контролювати всі мережеві пристрої (наприклад, брандмауери, шлюзи, VPN-пристрої, бездротові вузли доступу – AP) на границі мережі – периметрі безпеки, а також будь-які сервери, на яких розміщаються інформація й процеси, що вимагають конфіденційності або цілісності. Для виробничих цілей варто контролювати всі пристрої й сервери, відказостійкість яких важлива для нормальної роботи підприємства. Для Windows необхідний моніторинг не тільки операційної системи, але й важливих застосунків, таких як Microsoft Exchange Server, Microsoft ISA Server, Microsoft IIS і Microsoft SQL Server. Корисно контролювати високорівневі застосунки (наприклад, Microsoft SharePoint Portal Server), якщо в такий спосіб вдається виявити важливі події, що ставляться до сфери безпеки або виробництва, які можуть залишитися непоміченими засобами нижчележачих баз даних, на яких вони працюють.

Джерела телеметричних даних

Головне джерело телеметричної інформації про сервери Windows – журнал подій Security, а найважливіше джерело виробничої телеметрії – журнали подій System і Application. Досвідчені користувачі оснащення Event Viewer консолі Microsoft Management Console (MMC) знають, що у всіх журналах подій Windows застосовується один формат файлів (.evt). Запис про кожну подію містить стандартні поля (наприклад, дата, час, джерело події, категорія, ID події), за яких треба поле опису з даними у вільній формі, унікальними для конкретної події. Будь-який застосунок моніторингу, сумісне з журналами подій Windows, дозволяє генерувати попередження й звіти на основі джерела, категорії або ID події, але в ідеальному випадку потрібно мати можливість відфільтровувати запису за даними в описі події.

Мережеві пристрої, такі як маршрутизатори, комутатори, бездротові AP і брандмауери, незмінно передають телеметричні дані через протокол SNMP або Syslog. SNMP був спроектований наприкінці 1980-х для керування безліччю пристроїв у бурхливо, що розвивається мережі, Internet. Диспетчери SNMP збирають телеметричну інформацію від агентів через UDP-порт 162. Диспетчери можуть використовувати SNMP-команди Get для запиту конкретних телеметричних даних, називаних змінними (variable), або пасивно чекати звіту про важливі події від агентів через повідомлення Trap. Для моніторингу в сферах виробництва й безпеки досить збирати повідомлення Trap. Для поглибленого аналізу тенденцій і планування ресурсів варто опитувати агентів за допомогою команд Get.

Syslog

Syslog – стандарт протоколювання подій для UNIX. Перевага Syslog перед механізмом протоколювання подій Windows полягає в тому, що весь процес консолідації потоків подій від численних систем – невід'ємна частина Syslog. У дійсності Syslog одночасно мережевий протокол і формат журналу, і за замовчуванням він використовує UDP-порт 514. Кожне повідомлення Syslog містить поля дати, часу, пріоритету, ім'я хоста й тексту повідомлення. З технічної точки зору пріоритет – число від 0 до 191. Однак більшість застосунків Syslog відображають пріоритет у вигляді двох складових: Facility і Level.

Facility. Спочатку Syslog проектувався для моніторингу BSD Unix, і величина Facility використовувалася для ідентифікації процесу Unix про яке свідчить подію. Значення від 0 до 15 відповідають найважливішим процесам Unix, а значення від 16 до 23 (з іменами від Local0 до Local7) призначені для застосунків і пристроїв. Більшість мережевих пристроїв

використовують значення від Local0 до Local7 (наприклад, пристрою Cisco задіють Local6 і Local7), але не все. Маршрутизатор Xincom Twin Wan використовує майже всі низькі значення Facility.

Level. Інший елемент пріоритету повідомлень Syslog – Level, значення якого перебувають у межах від 0 до 7. Level характеризує ступінь важливості повідомлення.

Продуктивність і стан

Для повного функціонального моніторингу корисно контролювати об'єкти продуктивності (performance-object) і стан серверів з окремого комп'ютера або від провайдеру послуг. Адміністратори, не знайомі з об'єктами продуктивності, можуть досліджувати їх за допомогою оснащення Performance консолі MMC. Різниця між моніторингом журналу подій і об'єкта продуктивності наступна: з журналів подій можна витягти інформацію про будь-яку частину системи, у якій відбулися неполадки, а об'єкт продуктивності дозволяє переконатися, що конкретні параметри перебувають у припустимих межах. Наприклад, за допомогою об'єктів продуктивності можна стежити за простором жорсткого диска, тому що системний журнал видає попередження, тільки коли тім заповнюється настільки, що користувач уже починає випробовувати незручності.

Ще одна типова перевірка із застосуванням об'єкта продуктивності – моніторинг коефіцієнта використання центрального процесора з відстеженням певних рівнів протягом тривалих періодів часу (наприклад, понад 90% протягом 10 хвилин). Однак при перевірках коефіцієнта використання центрального процесора варто проявляти обережність; неважко переплутати корисне навантаження з некерованим процесом і згенерувати помилкове повідомлення про проблему. Чудова властивість об'єктів продуктивності полягає в тому, що інші застосунки можуть створювати власні об'єкти продуктивності й публікувати телеметричні дані, специфічні для даного застосунку. Наприклад, Active Directory (AD), SQL Server і Exchange Server мають у своєму розпорядженні власні об'єкти продуктивності.

Відсутність повідомлень про помилки в журналі й показники продуктивності в межах припустимих порогів – гарні індикатори коректного функціонування. Однак деякі проблеми не знаходять відбиттів в індикаторах. Перевірки стану серверів – найефективніший спосіб переконатися в тому, що сервери й застосунки працюють у мережі й успішно обробляють запити. Перевірки стану серверів надійні, тому що вони виконують тестову транзакцію. Багато провайдерів застосунків і служб в Internet дозволяють регулярно проводити тестові транзакції із сервером через обрані споживачем інтервали часу. Для Web-сервера можна періодично запитувати дану Web-сторінку й перевіряти, чи успішно вона передана. Для системи SQL Server можна періодично виконувати запит і перевіряти результати.

Однак навіть перевірки стану не розкривають всіх проблем. Наприклад, простий сигнал ping, переданий через кожні 5 хвилин, дозволяє переконатися, що операційна система й набір протоколів активні, але не містять ніякої інформації про стан самого застосунку. Мені доводилося зустрічати завислі сервери, які відповідали на сигнали ping. Аналогічно простий запит HTML-сторінки із сервера не доводить, що відповідний застосунок електронної комерції на базі Active Server Pages (ASP) працює коректно.

Тому перевірки стану повинні бути як можна більше функціональними. Якщо застосунок або служба перевірки стану забезпечує таку можливість, можна створити тестовий обліковий запис для застосунку електронної комерції й використовувати неї для пробного додавання товару в кошик покупок.

Ще одне застереження: програму перевірки стану варто розміщати поза контрольованим виробничим середовищем. Якщо помилково розмістити програму перевірки стану на контрольованому сервері, те, наприклад, не вдасться визначити відмова сервера або серверного з'єднання, тому що застосунок не зможе передати адміністраторові відповідне повідомлення. Але якщо застосунок перевірки працює на окремому сервері (і якщо цей сервер доступний з Internet), то єдиний випадок, коли важливий застосунок буде не готовий до роботи без введеня адміністратора, – одночасна відмова виробничого й контролюючого середовища.

Необхідний інструментарій

Отже, що потрібно для моніторингу всіх пристроїв, серверів, журналів, пасток SNMP і подій Syslog? Очевидно, необхідні один-два інструмента за доступною ціною, що охоплює всі елементи, які потрібно відслідковувати. Продукти моніторингу високого рівня, такі як Argent Guardian і Microsoft Operations Manager (MOM), дозволяють контролювати всі об'єкти продуктивності, журнали подій Windows, пастки SNMP, потоки подій Syslog і навіть виконувати різні перевірки стану. Деякі не настільки великі, менш дорогі пакети, такі як Sentry II компанії Engagent, EventTracker компанії Prism Microsystems і комплекс Event Log Management компанії Dorian, охоплюють підмножина телеметричних джерел і обмежений набір об'єктів продуктивності.

Збираючись придбати інструмент, варто скласти список всіх характеристик, які необхідно знати, і підібрати інструмент, що контролює їх усе. Якщо інструмент не забезпечує моніторинг важливого параметра, наприклад SNMP, то заповнити пробіл можна за допомогою безкоштовної або недорогої умовно безкоштовної утиліти. Далі буде розглянутий ряд таких інструментів, з яких можна скласти ефективний комплекс моніторингу.

Розробка структурної схеми

Комп'ютерна мережа є сьогодні практично в кожній процвітаючій фірмі, компанії. Мережа вже не вважається чимсь розкішним, а є прекрасною можливістю ефективно оптимізувати роботу, виробництво, об'єднавши всі комп'ютери в єдину систему.

Стежити за роботою всієї мережі, вчасно реагувати на проблеми допомагає програма моніторингу. З її допомогою керівництво стежить за тим, що відбувається в службових комп'ютерах, як функціонує виробництво, налагоджуються й підтримуються контакти.

Крім цього, програма блокує спам, попереджає вірусні атаки, робить перевірки контенту й файлів, які поступають,. Моніторинг мережі підприємства – це реальна можливість контролювати й убезпечити робочий процес, що пов'язаний з інтернетом і комп'ютерами.

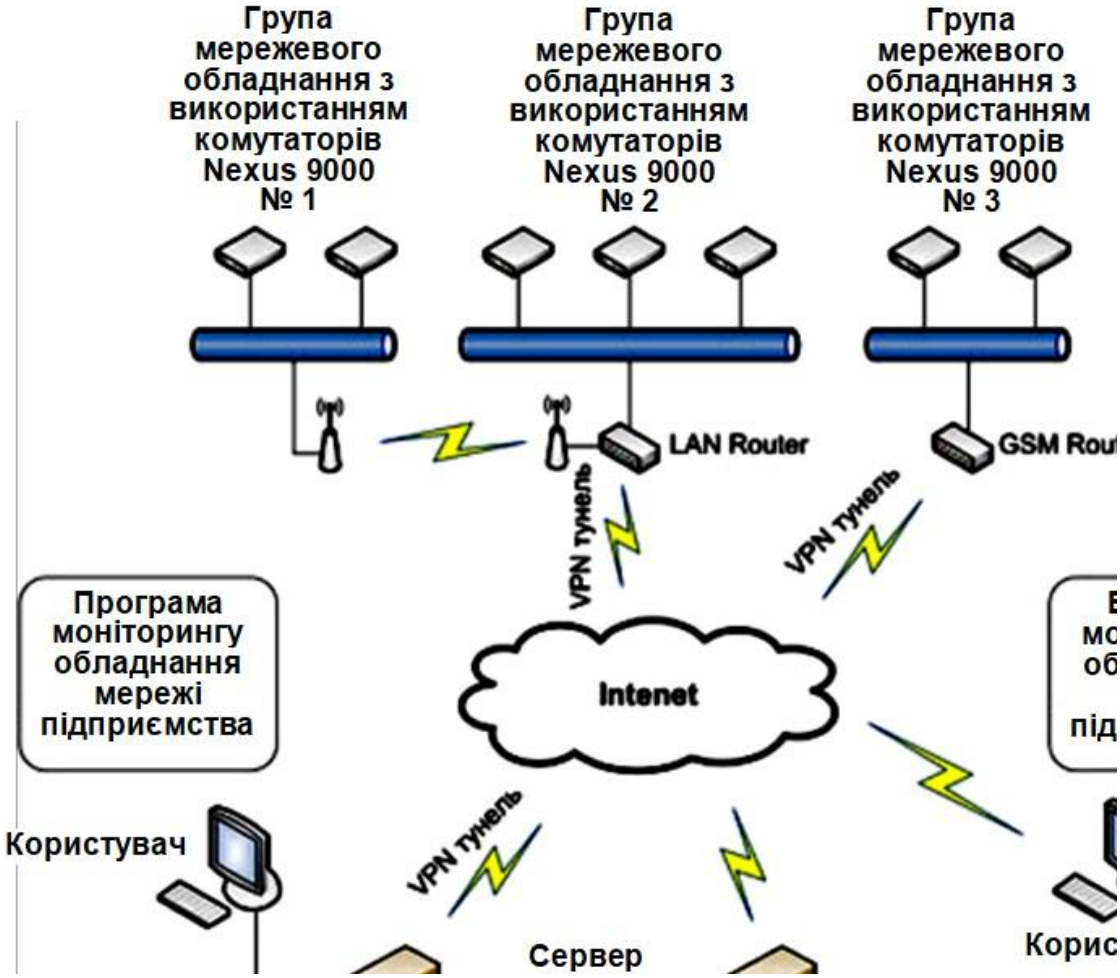


Рисунок 1 – Структурна схема системи

Уже доведено, що неполадки в комп'ютерній мережі легше попередити, ніж потім вирішувати проблеми. Регулярний моніторинг локальної мережі, сервера, мережевих пристроїв дозволяє заздалегідь дізнаватися про можливі неполадки й запобігати їхня поява. Крім того, відслідковуючи історію, адміністратор може дати відомості про частоту появи різних несправностей, що теж є запорукою безпроблемної роботи.

Сьогодні можна виділити два різновиди моніторингу мережі підприємства:

- оперативний;
- моніторинг безпеки.

На великих підприємствах дані різновиди можуть бути виділені у два процеси, які виконуються окремими фахівцями. У малі ж і середніх фірмах моніторинг звичайно буває загальним. Це правильно, оскільки невелика комп'ютерна мережа не має потреби в скрупульозних оперативних перевірках, вона завантажена не так серйозно й обслуговується простіше. У них немає потреби в докладному аналізі звітів, завдань і тенденцій, які необхідні на великих підприємствах.

Які об'єкти піддаються моніторингу

Для того щоб гарантувати безпека важливо піддавати контролю всі наявні в наявність мережеві пристрої. До них відносять бездротові точки доступу, різні шлюзи, VPN-пристрою, брандмауери різних конфігурацій і сервери, на яких розміщені конфіденційні дані й цілісні процеси. Для Windows проводиться перевірка ОС і ключових застосунків різного типу. Контролю повинні піддаватися й високорівневі застосунки, щоб відразу виявити події, які безпосередньо ставляться до збереження безпеки життєдіяльності підприємства й проведенню виробничих процесів.

Моніторинговій перевірці повинні піддаватися як об'єкти продуктивності, так і стан безпечної роботи сервера. Відмінність між перевіркою конкретного об'єкта й журналу подій, що відбуваються, полягає в тому, що з журналу беруть дані про проблеми в будь-якій системній частині, тоді як об'єкт продуктивності показує, що певні параметри мають припустимі межі. Так, завдяки об'єктам продуктивності, можна контролювати простір жорсткого диска, а журнал усього лише видасть попередження, коли він заповниться до критичного стану.

Моніторинг ступеня використання ЦП – це ще одне корисне дослідження із застосуванням об'єкта продуктивності. Відслідковувати прийде досить довгий час. Однак такий моніторинг вимагає обережності, розуміння суті процесів і уваги, оскільки досить легко можна переплутати корисне навантаження з певним некерованим процесом.

Головними індикаторами коректної, правильної роботи системи є відсутність у журналі відомостей про помилки й безперебійні показники продуктивності. Але варто знати, що є проблеми, які не відбиваються в індикаторах. І тут необхідна перевірка серверного стану, як підходящий спосіб упевнитися в тому, що застосунку, сервери функціонують правильно й обробляють всі запити.

Для цієї мети варто проводити іноді транзакції-тести із сервером через певні тимчасові інтервали. Для веб-серверу можна час від часу запитувати певну веб-сторінку й контролювати, як вона передається. Для SQL сервера виконуються запити й перевіряються результати.

Зверніть увагу, що не всі проблеми навіть після перевірки стану можуть бути не виявлені. Так, звичайний пінг-сигнал, переданий регулярно через п'ять хвилин, дозволяє впевнитися, що протоколи й ОС активні, але він не скаже нічого про стан певного застосунку. Буває й так, що на пінг-сигнали відповідають сервера, які перебувають у стані зависання. Точно так само, запит із сервера конкретної HTML-сторінки ще не гарантує, що застосунок електроної комерції на базі ASP працює коректно.

Саме тому, важливо домогтися максимальної функціональності перевірок стани. Якщо є можливість, варто зробити облікові записи-тест для застосунку на базі ASP.

Ще одна тонкість: розміщати дану програму треба поза зоною, що буде контролюватися. Якщо так не зробити й розташувати її прямо на контрольованому сервері, то складно буде визначити відсутність з'єднання, серверна відмова. У цьому випадку застосунок не зможе передати системним адміністраторам необхідні повідомлення.

Якщо ж розмістити на окремому сервері застосунок перевірки, то воно буде працювати завжди, за винятком моменту, коли одночасно відмовляють середовища контролю й виробництва.

Що буде потрібно для моніторингу мережі

За допомогою інструмента для моніторингу можливо:

– довідатися про виниклі проблеми (розривах з'єднання, зупинці процесів і служб, ушкодженні каналу зв'язку, відсутності місця на диску).

– усунути проблему відразу, ще до того, як вона стане нерозв'язаної: будуть порушені процеси, загублені дані.

– вести перевірку файлів і папок, хостов і серверів, служб і баз даних на мережевому встаткуванні й комп'ютерах, яких укладені в загальну виробничу мережу.

Дуже важливо, щоб будь-яка сучасна програма моніторингу локальної мережі підприємства накопичувала й зберігала статистику опитувань. З її допомогою можна провести IT аудит і проаналізувати продуктивність і поводження конкретних пристроїв і мережі в цілому.

Комутатори Cisco Nexus серії 9000

Комутатори Nexus серії 9000, представлені в різних типорозмірах, забезпечують високу продуктивність і щільність, низькі затримки й виняткову енергоефективність. Ці комутатори працюють у режимі ПЗ Cisco NX-OS або ACI (інфраструктури, орієнтованої на

застосунки) і підтримують передову технологію Cloud Scale ASIC. Вони ідеально підходять для традиційних або повністю автоматизованих центрів обробки даних.

Продуктивність і масштабованість

Мультишвидкістні порти 1/10/25/50/100/400G забезпечують масштабованості й захист інвестицій.

Підвищений рівень контролю й інформаційної безпеки

Кращий у галузі рівень контролю й інформаційної безпеки завдяки потоковій телеметрії, що попереджає аналізу й шифруванню на лінійній швидкості передачі (MACsec).

Зниження сукупної вартості володіння

Ви одержуєте уніфіковані порти, що підтримують 10/25 Gb і Fiber Channel 8/16/32 G, RDMA поверх конвергованого Ethernet (RoCE) і зберігання IP.

Продуктивність застосунків

Завдяки інтелектуальним буферам і відсутності втрати пакетів час обробки застосунків скорочується на 50%.

Порівняння моделей комутаторів Nexus серії 9000

Спеціалізовані кристали ASIC технології Cloud Scale підтримують архітектуру ACI типу «розподілене ядро» і структури VxLAN системи експлуатації NX-OS при розмаїтості модульних і фіксованих моделей.

Модульні комутатори Nexus серії 9500:

- 4 слота, 8 слотів, 16 слотів.
- Лінійні плати технології Cloud Scale 1/10/25/40/100G серії EX/FX.
- Лінійні плати серії R зі збільшеним буфером.

Фіксовані комутатори Nexus серії 9300:

- Серія FX 1/10/25/40/100G з технологією Cloud Scale

Можливості й переваги

Технологія Cloud Scale ASIC

Захист інвестицій завдяки можливості масштабування за рахунок наявності портів з вибором швидкості 10/25/50/100 Гбіт/с і шифрування зі швидкістю лінії. Інтегрована й потокова аналітика забезпечує підвищену безпеку. Уніфіковані порти 10/25 Гбіт/с і оптоволоконний канал 8/16/32 забезпечують конвергенцію.

Підтримка програмування для розробки й експлуатації

Перший у галузі програмувальний комутатор з відкритими API-Інтерфейсами оптимально підходить для середовищ розробки й експлуатації. Відкриті засоби програмування комутаторів Nexus серії 9000 підтримують убудовані інструменти автоматизації розробки й експлуатації, такі як Puppet, Chef і Ansible.

Автоматизація

Технологія Cisco ACI ставить застосунок у центр інфраструктури. Вона дозволяє створити гнучку, відкриту й безпечну архітектуру. Ви можете знизити сукупну вартість володіння, автоматизувати IT-завдання й прискорити розгортання застосунків центрів обробки даних.

Гнучкість архітектури

Енергозберігаюче розгортання архітектури третього рівня або деревоподібної архітектури («стовбур і листи»). Гнучка конфігурація портів 1/10/25/40/50/100 GE з підтримкою мережевих пристроїв зберігання даних. Створює основу для ACI – нашого кращого в галузі рішення для автоматизації.

Масштабованість

До 172,8 Тбіт/с пропускної здатності, що не блокує, із затримкою менш 5 мкс. Ці комутатори забезпечують маршрутизацію, підтримку шлюзів, мостів і площини керування на основі протоколу граничного шлюзу для VXLAN. Сегментна маршрутизація спрощує віртуалізацію.

Контроль у реальному часі й телеметрія

Убудовані датчики підтримують платформу Cisco Tetration Analytics для телеметрії потоку трафіку й збору даних зі швидкістю лінії. Дані про використання буфери в реальному часі розраховуючи на порт і на чергу допомагають відслідковувати шаблони трафіку застосунків.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів моніторингу мережі підприємства на основі комутаторів Nexus 9000. В межах України в недостатній мірі представлені вітчизняні розробки в цій області. У роботі наведені теоретичне узагальнення й рішення наукового завдання дослідження методів моніторингу мережі підприємства на основі комутаторів Nexus 9000. Рішення даного завдання полягало у вирішенні наступних задач:Був проведений огляд існуючих систем моніторингу мережі підприємства на основі комутаторів Nexus 9000; Досліджена система моніторингу мережі підприємства на основі комутаторів Nexus 9000; На основі отриманих результатів досліджень створена програмна реалізація системи моніторингу мережі підприємства на основі комутаторів Nexus 9000. Розроблені під час виконання роботи алгоритми дозволяють успішно вирішувати завдання моніторингу мережі підприємства на основі комутаторів Nexus 9000. 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. Смирнов А.А. gert-модель технологии передачи данных в облачные антивирусные системы / А.А. Смирнов, В.В. Босько, Мохамад Гани Абу Таам // Збірник тез доповідей науково-практичної конференції «Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку». м. Харків. 12-13 березня 2014 р. – Харків. АВВ МВС. – 2014. – С. 18-19.
2. Смирнов А.А. 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 IT-індустрії". м. Харків. 17-18 квітня 2014 р. – Харків: ХНЕУ. – 2014. – С. 260.
3. Смирнов А.А. 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.
4. 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.
5. 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.
6. 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.
7. 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 IT-індустрії". м. Харків. 17-18 квітня 2015 р. – Харків: ХНЕУ. – 2015. – С. 14.
8. 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.
9. 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.
10. 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.

УДК 004

Е. Гребенюк, магістр гр. КІ-19М-1,4
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ ПРОГРАМНО-ВИЗНАЧАЄМИХ СХОВИЩ ДЛЯ NVME НА БАЗІ ТЕХНОЛОГІЇ RDDA

У статті розроблено програмне забезпечення, яке призначено для реалізації системи програмно-визначаємих сховищ для NVMe на базі технології RDDA. Об’єктом дослідження є процес програмно-визначаємих сховищ для NVMe на базі технології RDDA. Предметом дослідження є методи програмно-визначаємих сховищ для NVMe на базі технології RDDA. Методи дослідження базуються на методах теорії телетрафіку, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи програмно-визначаємих сховищ для NVMe на базі технології RDDA. 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, програмно-визначаємі сховища, NVMe, RDDA

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 визначаємі системи зберігання.

Що розуміється під програмно визначаємим сховищем (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 визначаємих 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.

З кожним роком запам'ятовуючі пристрої стають все більш досконалими. У наші дні технологія NVMe забезпечує найвищі показники швидкодії – найшвидші накопичувачі використовують цей стандарт. NVM Express (NVMe, NVMHCI – від англ. Non-Volatile Memory Host Controller Interface Specification) – новий стандарт взаємодії з накопичувачем по швидкісній шині PCI Express. SATA-інтерфейс, навіть у своїй останній генерації, не в змозі забезпечити таку швидкість передачі даних через внутрішні обмежень. Тобто за фактом

змінився тільки інтерфейс передачі даних, який зняв ті обмеження, в які «упирався» старіший стандарт (SATA). На даний момент основними є наступні форм-фактори:

– Плата розширення PCI-E 4x. Даний форм-фактор використовується в серверах і ПК. Є також перехідники PCI-E 16x, в які можна встановити 4 M.2-накопичувача, але вони менш поширені.

– U.2 – форм-фактор для серверів, який підтримує виконання гарячої заміни. Пристрої зовні мало відрізняються від звичайних SATA-накопичувачів (хіба що більш масивним радіатором охолодження), мають ту ж форму роз'єму, що і SATA / SAS. Це дозволяє працювати з ними звичним способом (установка в «старі» серверні кошика, монтаж-демонтаж).

– M.2 – форм-фактор, створений для мобільних ПК. Роз'єми M.2 також часто зустрічаються на серверних материнських платах і платах настільних ПК. У старіших материнських платах цей роз'єм призначений для установки тільки SATA-накопичувачів (або інших плат розширення, наприклад, бездротових мережевих карт). Але в більш свіжих платах в цей роз'єм можна підключити і SSD стандарту NVMe.

– Intel Ruler SSD – форм-фактор для серверів, який має функцію гарячої заміни.

– Samsung NGSFF – форм-фактор для серверів, також з можливістю гарячої заміни.

Основними перевагами використання накопичувача NVMe є:

– Затримка записи у SSD з підтримкою NVMe нижче, ніж у SATA SSD, що прискорює запис даних на диск.

– Швидке відкриття сторінки і створення резервної копії в порівнянні з SSD на інтерфейсі SATA.

– Велика швидкість обробки даних. NVMe працює по інтерфейсу PCIe, що забезпечує максимальну швидкість 3,2 ГБ / с, а це в 2-3 рази швидше, ніж у SATA SSD.

– Можливість обробки більшої кількості запитів за одиницю часу (IOPS), ніж у SATA-SSD.

Метод віддаленого прямого доступу до дисків (Remote Direct Drive Access, RDDA), розроблений компанією Excelero, дозволяє звертатися до віддалених носіїв, які не задіюючи ресурси процесора

Як видно з назви, RDDA відтворює метод віддаленого прямого доступу до пам'яті (Remote Direct Memory Access, RDMA): клієнти отримують дистанційний доступ до дисків NVMe, а процесорні ресурси на віддаленій стороні не задіюються. Переклад підтримки сервісів зберігання з цільового пристрою на клієнта дозволяє, як стверджують в компанії, забезпечити детерміновану продуктивність для додатків і лінійне масштабування розподіленого сховища.

Пропоноване рішення є повністю програмним, проте на всіх клієнтах (в якості яких виступають сервери додатків) і серверах зберігання повинні бути мережеві плати з підтримкою RDMA (R-NIC) (точніше, RoCE v2). Це обмежує потенційну можливість застосування NVMesh в гіпермасштабіруемих інсталяціях, на які ця дія спрямована, так як передбачає заміну великої кількості обладнання. (Не випадково Facebook разом з іншими учасниками ринку стимулювала розробку NVMe поверх TCP.)

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи програмно-визначаємих сховищ для NVMe на базі технології RDDA.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи програмно-визначаємих сховищ для NVMe на базі технології RDDA.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем програмно-визначаємих сховищ для NVMe на базі технології RDDA.

– Дослідження системи програмно-визначаємих сховищ для NVMe на базі технології RDDA.

– Програмна реалізація системи програмно-визначаємих сховищ для NVMe на базі технології RDDA.

Об'єктом дослідження є процес програмно-визначаємих сховищ для NVMe на базі технології RDDA.

Предметом дослідження є методи програмно-визначаємих сховищ для NVMe на базі технології RDDA.

Методи дослідження базуються на методах теорії телетрафіку, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. У той час як Wi-Fi 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 визначаєме 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 програмно-визначаємих сховищ для NVMe на базі технології RDDA, а « SDS-сховище» спочатку формує всі дані в SSD-Журналі, а потім у фоновому режимі відправляє їх на жорсткий диск системи програмно-визначаємих сховищ для NVMe на базі технології RDDA.

Програмно визначаєме зберігання зручно саме по собі, однак найбільшу цінність воно здобуває в рамках повністю програмно визначаємого центра обробки даних. Одним з важливих етапів для досягнення цієї мети є розгортання гіперконвергентної інфраструктури (Hyperconverged Infrastructure, HCI).

Найбільші вигоди реалізація програмно визначаємого 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 визначаєме 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 визначаємими ЦОДами. І до цього майбутнього треба бути готовим.

Налаштування 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 налаштування продуктивності, у цьому випадку на рівні екземпляра бази даних: швидкість запису після налаштування 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 налаштуванні 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 налаштування 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 визначаємих 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 визначаємими 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.

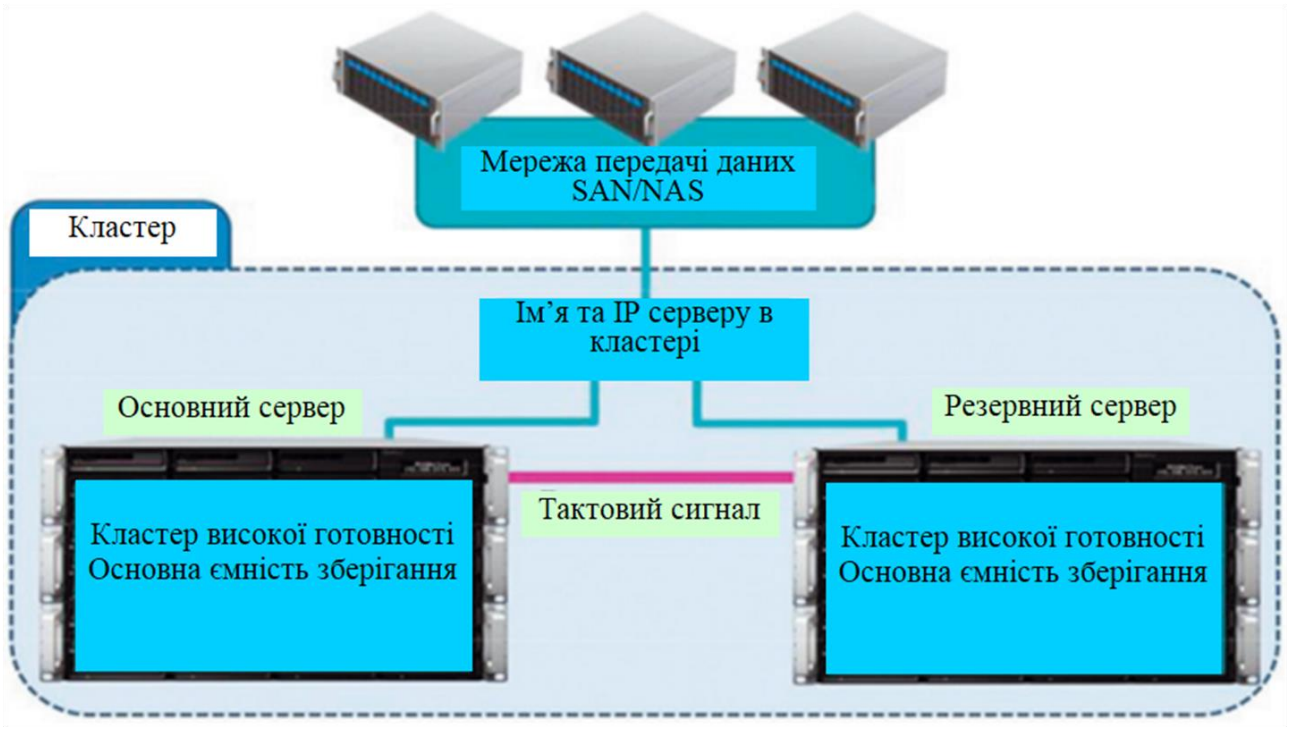


Рисунок 1 – Структурна схема системи

Програмно визначаєме 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 визначаємі 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.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів програмно-визначаємих сховищ для NVMe на базі технології RDDA. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем програмно-визначаємих сховищ для NVMe на базі технології RDDA; Досліджена система програмно-визначаємих сховищ для NVMe на базі технології RDDA; На основі отриманих результатів досліджень створена програмна реалізація системи програмно-визначаємих сховищ для NVMe на базі технології RDDA. Розроблені під час виконання роботи алгоритми дозволяють успішно вирішувати завдання програмно-визначаємих сховищ для NVMe на базі технології RDDA. 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. 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.

УДК 004

І. Іванова, магістр гр. КН-19МЗ
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ УНІФІКОВАНИХ КОМУНІКАЦІЙ НА БАЗІ ПРОТОКОЛУ AOIP

У статті розроблено програмне забезпечення, яке призначено для системи уніфікованих комунікацій на базі протоколу AoIP. Метою розробки є дослідження та програмна реалізація системи уніфікованих комунікацій на базі протоколу AoIP. б'єктом дослідження є процес уніфікованих комунікацій на базі протоколу AoIP. Предметом дослідження є методи уніфікованих комунікацій на базі протоколу AoIP. Методи дослідження базуються на методах теорії телетрафіку, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи уніфікованих комунікацій на базі протоколу AoIP.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, уніфіковані комунікації, AoIP

Постановка проблеми. З початком ери комп'ютеризації стали бурхливо розвиватися системи передачі даних (СПД) на базі IP [1-3]. Організувавши високошвидкісний доступ до СПД по наземних каналах або з використанням доступної бездротової технології, оператор може надати клієнтові й послуги телефонного зв'язку – досить лише підключити телефонні апарати

або персональну автоматичну телефону мережу (ПАТМ) клієнта через мережу IP до платформи AoIP оператора. Аналогічні підходи застосовні й при побудові корпоративної мережі зв'язку (КМЗ) [5]. Шлях побудови корпоративної мережі зв'язку на базі AoIP припускає відмову від традиційної комутації (тобто від комутації каналів) за допомогою ПАТМ і впровадження IP-PBX (IP-ПАТМ), які є новим поколінням систем зв'язку, орієнтованим на AoIP [1-10]. Замість IP-ПАТМ у КМЗ для комутації трафіку AoIP можна скористатися послугами операторів зв'язку Hosted IP-PBX (віртуальна IP-ПАТМ) або IP-Centrex (оренда комутаційної ємності). Більша частина середніх і великих підприємств має офіси в декількох районах і містах. Організація зв'язку із центральним офісом коштує чималих грошей. Тим часом діяльність всіх перерахованих компаній і підприємств не можна уявити без доступу співробітників до мережі Internet і/або корпоративної обчислювальної мережі. Однак однією з умов придатності приміщення для розміщення філії є найчастіше наявність мережі передачі даних і телефонної мережі. Тільки от чи не так уже необхідно сьогодні окреме підключення до Тфоп? Або, скажемо інакше, чи багато потрібно далеко не дешевих телефонних ліній і чи потрібна окрема ПАТМ, яку доводиться обслуговувати на місці? Використання у філіях електронної пошти, корпоративного електронного документообігу й внутрішніх ресурсів Web (Intranet), довідкових систем і баз даних, систем обліку товарно-фінансових потоків і керування ресурсами підприємства вимагають організації надійного доступу до корпоративної мережі по виділених каналах або через мережу передачі даних за допомогою VPN. Але якщо такий доступ реалізований, то ці ж канали придатні й для телефонного зв'язку – досить реалізувати підтримку технологій AoIP. Завдяки шлюзам AoIP сьогодні можна створювати налагоджену КМЗ з можливістю доступу до будь-якого співробітника без виходу до Тфоп. Для цього абоненти філій підключаються до ПАТМ центрального офісу (яка, як правило, уже є) за допомогою абонентських місць побудованих на основі шлюзів AoIP [9-10].

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи уніфікованих комунікацій на базі протоколу AoIP.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи уніфікованих комунікацій на базі протоколу AoIP.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем уніфікованих комунікацій на базі протоколу AoIP.
– Дослідження системи уніфікованих комунікацій на базі протоколу AoIP.
– Програмна реалізація системи уніфікованих комунікацій на базі протоколу AoIP.

Об'єктом дослідження є процес уніфікованих комунікацій на базі протоколу AoIP.

Предметом дослідження є методи уніфікованих комунікацій на базі протоколу AoIP.

Методи дослідження базуються на методах теорії телетрафіку, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Структура програмного забезпечення в першу чергу визначається тими функціями, які повинна виконувати програма. В даній роботі автоматизується система керування корпорацією, за рахунок впровадження IP-зв'язку. Для корпоративної мережі зв'язку можливо виділити наступні функції:

- реалізація IP-зв'язку між підрозділами корпорації;
- реалізація селективного зв'язку між підрозділами та структурами;
- реалізація режиму конференції;
- при наявності відповідного устаткування реалізація режиму відеоконференцій;
- реалізація можливості створення бази корпоративних номерів;
- можливість коригування інформації в базі корпоративних номерів.

Розроблюване програмне забезпечення повинне виконувати всі вказані вище функції, але в різному об'ємі. Головне призначення системи організації зв'язку в корпорації, в даному випадку – поліпшити оперативність прийняття рішень, підвищити продуктивність праці,

знизити кількість обчислювальних помилок за допомогою автоматизації процесу обробки інформації, сприяти ефективному і безпечному збереженню і доступу до інформації.

Метою корпоративної мережі зв'язку є створення єдиної мережі, що дозволяє ефективно здійснювати керування за рахунок застосування IP-телефонії.

Під IP-телефонією розуміється технологія, що дозволяє використовувати IP-мережу як засіб організації й ведення міжнародних і міжміських телефонних розмов і передачі факсів у режимі реального часу. Зараз в IP-телефонії існує два основних способи передачі голосових пакетів по IP-мережі: через публічний Інтернет і використовуючи виділені канали. У першому випадку смуга пропущення прямо залежить від завантаженості IP-мережі пакетами, що містять дані, голос, тощо, а значить затримки при проходженні пакетів можуть бути самими різними. При використанні виділених каналів винятково для голосових пакетів можна гарантувати фіксовану (або майже фіксовану) швидкість передачі. Виходячи зі схеми, реалізованої провайдером IP-телефонії, принцип роботи мережі IP-телефонії наступний (розглянутий найпоширеніший випадок – дзвінок з телефону на телефон або з факсимільного апарата на факсимільний апарат).

Необхідно зробити дзвінок на міський телефонний номер телефонного шлюзу, користуючись будь-яким телефонним апаратом або таксофоном, що переходить у тоновий режим. Дзвінок по цифрових або аналогових лініях приходить на телефонний шлюз. Шлюз звертається до сервера голосових повідомлень для видачі голосових підказок і повідомлення залишку на рахунку. Після ідентифікації й автентифікації, пропонується ввести код країни, міста й телефонний номер викликуваного абонента. Все спілкування з телефонним шлюзом відбувається в голосовому каналі. Далі телефонний шлюз встановлює зв'язок з віддаленим телефонним шлюзом по виділеному каналі. Віддалений шлюз робить таке ж з'єднання з викликуваним абонентом, але у зворотному порядку. Після установки з'єднання шлюзи починають обмін IP-Пакетами, у які впакований голос.

Апаратне забезпечення. У якості інтерфейсної плати ISDN використовуються плати для роботи з голосом, які з'єднані послідовно з інтерфейсною платою шиною SCBus. При використанні переривання відлуння одна плата підтримує до 8 ліній, а при використанні знищення ефекту відлуння до 4-х ліній. Зовні шлюз являє собою комп'ютер у промисловому виконанні, що монтується в 19-дюймову стійку. В одній мережі зі шлюзом розташовується голосовий сервер, що відповідає за голосові підказки й повідомлення про залишок на рахунку. Являє собою звичайний IBM-сумісний комп'ютер із ПЗ.

Програмне забезпечення. Для кодування використовується стандарт GSM. В IP-мережі голос займає 13,5 Кбіт/сек по протоколу UDP, що також значно зменшує затримки при передачі пакетів. При передачі факсу використовується та ж швидкість, причому використовується протокол гарантованої доставки TCP/IP. Таким чином, при використанні 30 ліній, потрібний канал із шириною пропущення не більше 512 Кбіт/сек, з яких тільки 405 Кбіт/сек будуть задіяні для IP-телефонії. Іншу ширину каналу можна використовувати під Інтернет, причому ніяк не погіршуючи якість передачі голосу. Шлюз підключається до мережі Ethernet, яка підключена до маршрутизатора. Максимально припустима затримка в каналі – 400 мс. При більших затримках недоцільне застосування функцій, що знищують ефект відлуння, тому на програмному рівні відлуння подавлення використовує буферізацію (за замовчуванням в 80 мс).

Рівні архітектури IP-телефонії

Архітектура технології AoIP може бути спрощено представлена у вигляді двох площин. Нижня площина – це базова мережа з маршрутизацією пакетів IP, верхня площина – це відкрита архітектура керування обслуговуванням викликів.

Нижня площина являє собою комбінацію відомих протоколів Інтернет: це – RTP, що функціонує поверх протоколу UDP, розташованого, у свою чергу, у стеці протоколів TCP/IP над протоколом IP. Таким чином, ієрархія RTP/UDP/IP являє собою свого роду транспортний механізм для мовного трафіку. У мережах з маршрутизацією пакетів IP для передачі даних завжди передбачаються механізми повторної передачі пакетів у випадку їхньої втрати. Рекомендації ITU-т допускають затримки в одному напрямку не перевищуючі 150 мс.

Розглянемо протокол TCP/IP. Transmission Control Protocol/Internet Protocol – це промисловий стандарт стеку протоколів, розроблений для глобальних мереж:

- це найбільш завершений стандартний і водночас популярний стек мережних протоколів, що має багаторічну історію.
- майже усі великі мережі передають основну частину свого трафіка за допомогою протоколу TCP/IP.
- це метод одержання доступу до мережі Internet.
- стек TCP/IP є основою для створення intranet-корпоративної мережі, що використовує транспортні послуги Internet і гіпертекстову технологію WWW, розроблену в Internet.
- усі сучасні операційні системи підтримують стек TCP/IP.
- це гнучка технологія для з'єднання різнорідних систем як на рівні транспортних підсистем, так і на рівні прикладних сервісів.
- це масштабована міжплатформенна середа для додатків клієнт-сервер.

Протоколи TCP/IP поділяються на 4 рівні.

Найнижчий IV рівень відповідає фізичному і канальному рівням моделі OSI. Цей рівень у протоколах TCP/IP підтримує всі популярні стандарти фізичного і канального рівня: для локальних мереж це Ethernet, Token Ring, FDDI, Fast Ethernet, 100VG-AnyLAN, для глобальних мереж – протоколи з'єднань "точка-точка" SLIP і PPP, протоколи територіальних мереж із комутацією пакетів X. 25, frame relay. Звичайно тільки з'являється нова технологія локальних або глобальних мереж вона швидко включається в стек TCP/IP за рахунок розробки відповідного стандарту, що визначає метод інкапсуляції пакетів IP у її кадри.

Наступний III рівень – це рівень міжмережної взаємодії, що займається передачею пакетів із використанням різноманітних транспортних технологій локальних мереж, територіальних мереж, ліній спеціального зв'язку тощо. У якості основного протоколу мережного рівня використовується протокол IP.

Наступний II рівень називається основним. На цьому рівні функціонує протокол керування передачею TCP і протокол дейтаграм користувача UDP. Протокол TCP забезпечує надійну передачу повідомлень між віддаленими прикладними процесами за рахунок утворення віртуальних з'єднань. Протокол UDP забезпечує передачу прикладних пакетів дейтаграмним засобом, як і IP, і виконує тільки функції сполучного ланка між мережним протоколом і численними прикладними процесами.

Верхній I рівень називається прикладним. За довгі роки використання в мережах різноманітних країн і організацій стек TCP/IP накопичив велику кількість протоколів і сервісів прикладного рівня. До них відносять такі широко використовувані протоколи, як протокол копіювання файлів FTP, протокол емуляції термінала telnet, поштовий протокол SMTP, використовуваний в електронній пошті мережі Internet, гіпертекстові сервіси доступу до віддаленої інформації, такі як WWW і багато інших.

Основу транспортних засобів стека протоколів TCP/IP складає протокол міжмережної взаємодії – Internet Protocol (IP). Основні функцій протоколу IP:

- перенос між мережами різноманітних типів адресної інформації в уніфікованій формі,
- складання і розбирання пакетів при передачі їх між мережами з різноманітним максимальним значенням довжини пакета.

Пакет IP складається з заголовка і поля даних. Максимальна довжина поля даних пакета обмежена розрядністю поля, що визначає цей розмір, і складає 65535 байтів, проте при передачі по мережах різноманітного типу довжина пакета вибирається з урахуванням максимальної довжини пакета протоколу нижнього рівня, що несе IP-пакети. Якщо це кадри Ethernet, то вибираються пакети з максимальною довжиною в 1500 байтів, що поміщаються в поле даних кадру.

Задачею протоколу транспортного рівня UDP є передача даних між прикладними процесами без гарантій доставки, тому його пакети можуть бути загублені, продубльовані або прийти не в тому порядку, у якому відправлені.

У стеку протоколів TCP/IP протокол TCP працює так само, як і протокол UDP, на транспортному рівні. Він забезпечує надійне транспортування даних між прикладними процесами шляхом установлення логічного з'єднання.

У протоколі TCP для зв'язку з прикладними процесами використовуються порти. Номера портам присвоюються. Є стандартні, зарезервовані номера (наприклад, номер 21 закріплений за сервісом FTP, 23 – за telnet), а менше відомі додатки користуються довільно обраними локальними номерами.

Перейдемо до верхньої площини керування обслуговуванням запитів зв'язку. Керування обслуговуванням виклику передбачає прийняття рішень про те, куди виклик повинен бути спрямований, і яким образом повинне бути встановлене з'єднання між абонентами. Інструмент такого керування – телефонні системи сигналізації, починаючи із систем, підтримуваних декадно-кроковими АТС і функцій, що передбачають об'єднання, маршрутизації й функцій створення розмовного каналу, що комутирується, у тих самих декадно-крокових шукачах. Далі принципи сигналізації еволюціонували до систем сигналізації по виділених сигнальних каналах, до багаточастотної сигналізації, до протоколів загальканальної сигналізації [6, 7] і до передачі функцій маршрутизації у відповідні вузли обробки послуг мережі [8].

У мережах з комутацією пакетів ситуація більше складна. Мережа з маршрутизацією пакетів IP принципово підтримує одночасно цілий ряд різноманітних протоколів маршрутизації. Такими протоколами на сьогодні є: RIP, IGRP, EIGRP, IS-IS, OSPF, BGP і ін. Точно так само й для IP-телефонії розроблений цілий ряд протоколів

Найпоширенішим є протокол H.323, зокрема, тому, що він став застосовуватися раніше інших протоколів. Інший протокол площини керування обслуговуванням виклику -SIP – орієнтований на те, щоб зробити кінцеві пристрої й шлюзи більш інтелектуальними й підтримувати додаткові послуги для користувачів. Ще один протокол – SGCP – розроблявся, для того, щоб зменшити вартість шлюзів за рахунок реалізації функцій інтелектуальної обробки виклику в централізованому встаткуванні. Протокол IPDC дуже схожий на SGCP, але має більше, ніж SGCP, механізмів експлуатаційного керування (OAM&P). Існує більш функціональний, ніж MGCP, протокол MEGACO. Його адаптований до H.323 варіант в рекомендації H.248.

Щоб стало зрозуміло, чим конкретно відрізняються один від одного перераховані в попередньому параграфі протоколи, розглянемо архітектуру мереж, побудованих на базі цих протоколів, і процедури встановлення й завершення з'єднання з їхнім використанням.

Мережі на базі протоколів H.323 орієнтовані на інтеграцію з телефонними мережами й можуть розглядатися як мережі ISDN, накладені на мережі передачі даних. Рекомендація H.323 передбачає досить складний набір протоколів, що призначений не просто для передачі мовної інформації з IP-мереж з комутацією пакетів. Його мета – забезпечити роботу мультимедійних додатків у мережах з негарантованою якістю обслуговування. Мовний трафік – це тільки один з додатків H.323, поряд з відеоінформацією й даними. Варіант побудови мереж IP-телефонії в рекомендації H.323, добре підходить тим операторам місцевих телефонних мереж, які зацікавлені у використанні мережі з комутацією пакетів (IP-мережі) для надання послуг міжміського й міжнародного зв'язку.

Основними пристроями мережі є: термінал (Terminal), шлюз (Gateway), воротар (Gatekeeper) і пристрій керування конференціями (MCU).

У сценарії встановлення з'єднання між двома користувачами передбачається, що кінцеві користувачі вже знають IP-адреси один одного. У звичайному випадку етапів буває більше, оскільки у встановленні з'єднання беруть участь gatekeeper і й шлюзи.

Розглянемо крок за кроком цей спрощений сценарій.

1. Кінцевий пристрій користувача А надсилає запит з'єднання – повідомлення SETUP – до кінцевого пристрою користувача В.

2. Кінцевий пристрій викликуваного користувача В відповідає на повідомлення SETUP повідомленням ALERTING, що означає, що пристрій вільний, а викликуваному користувачеві подається сигнал про вхідний виклик.

3. Після того, як користувач У приймає виклик, до зухвалої сторони А передається повідомлення CONNECT з номером Тср-порту каналу Н.245.

4. Кінцеві пристрої обмінюються по каналі Н.245 інформацією про типи використовуваних мовних кодеків та про інші функціональні можливості встаткування, і сповіщають один одного про номери портів RTP, на які варто передавати інформацію.

5. Відкриваються логічні канали для передачі мовної інформації.

6. Мовна інформація передається в обидва боки в повідомленнях протоколу RTP; крім того, ведеться контроль передачі інформації за допомогою RTCP.

Наведена процедура обслуговування виклику базується на протоколі Н.323 версії 1. Версія 2 протоколи Н.323 дозволяє передавати інформацію, необхідну для створення логічних каналів, безпосередньо в повідомленні SETUP протоколу Н.225.0 без використання протоколу Н.245. Така процедура називається «швидкий старт» (Fast Start) і дозволяє скоротити кількість циклів обміну інформацією при встановленні з'єднання. Крім організації базового з'єднання, у мережах Н.323 передбачене надання додаткових послуг відповідно до рекомендацій ITU Н.450.X. Моніторинг якості обслуговування забезпечується протоколом RTCP, однак обмін інформацією RTCP відбувається тільки між кінцевими пристроями, що беруть участь у з'єднанні.

Другий підхід до побудови мереж IP-телефонії заснований на використанні протоколу SIP – Session Initiation Protocol. SIP являє собою текст – орієнтований протокол, що є частиною глобальної архітектури мультимедіа. Ця архітектура також містить у собі протокол резервування ресурсів (RSVP, RFC 2205), транспортний протокол реального часу (RTP, RFC 1889), протокол передачі потоків у реальному часі (RTSP, RFC 2326), протокол опису параметрів зв'язку (SDP, RFC 2327), протокол повідомлення про зв'язок (SAP). Однак функції протоколу SIP не залежать від кожного із цих протоколів.

Третій підхід до побудови мереж IP-телефонії, заснована на використанні протоколу MGCP. При розробці цього протоколу робоча група MEGACO опиралася на мережну архітектуру, що містить основні функціональні блоки трьох видів:

– шлюз – Media Gateway (MG), що виконує функції перетворення мовної інформації, що надходить із боку ТфОП з постійною швидкістю передачі, у вид, придатний для передачі по мережах з маршрутизацією пакетів IP (кодування й упакування мовної інформації в пакети RTP/UDP/IP, та зворотнє перетворення);

– контролер шлюзів – Call Agent, що виконує функції керування шлюзами;

– шлюз сигналізації – Signaling Gateway (SG), що забезпечує доставку сигнальної інформації, що надходить із боку ТфОП, до контролера шлюзів і перенос сигнальної інформації у зворотному напрямку.

Таким чином, весь інтелект функціонально розподіленого шлюзу зосереджений у контролері, функції якого можуть бути розподілені між декількома комп'ютерними платформами.

Для побудови добре функціонуючих і сумісних із ТфОП мереж IP-телефонії підходять протоколи Н.323 і MGCP. Як вже відзначалось, протокол SIP трохи гірше взаємодіє із системами сигналізації, використовуваними в ТфОП. Підхід, заснований на використанні протоколу MGCP, має досить важливу перевагу перед підходом Н.323: підтримка контролером шлюзів сигналізації ОКС7 і інших видів сигналізації, а також прозора трансляція сигнальної інформації з мережі IP-телефонії. У мережі, побудованої на базі рекомендації Н.323, сигналізація ОКС7, як і будь-яка інша сигналізація, конвертується шлюзом у сигнальні повідомлення Н.225.0 (Q.931). Основним недоліком третього з наведених у даному параграфі підходів є незакінченість стандартів. До недоліків можна віднести також відсутність стандартизованого протоколу взаємодії між контролерами. Крім того, протокол MGCP є протоколом керування шлюзами, але не призначений для керування з'єднаннями за участю термінального встаткування користувачів (IP-телефонів). Це означає, що в мережі, побудованої на базі протоколу MGCP, для керування термінальним устаткуванням повинен бути присутнім gatekeeper або сервер SIP. Варто також відзначити, що в існуючих додатках IP-телефонії, таких як надання послуг міжнародного й

міжміського зв'язку, використовувати протокол MGCP (також, як і протокол SIP) недоцільно у зв'язку з тим, що основна кількість мереж IP-телефонії сьогодні побудована на базі протоколу H.323. В останньому зі згаданих підходів (у проекті версії 4 рекомендації H.323) введено принцип декомпозиції шлюзів, використаний у третьому підході. Керування функціональними блоками розподіленого шлюзу буде здійснюватися контролером шлюзу – MGC (Media Gateway Controller) за допомогою протоколу MEGACO/H.248.

Розробка структурної схеми

Для перевірки коректності реалізації даної задачі було виконано багато розрахунків та експериментальних матеріалів. Цьому питанню приділялась особлива увага тому, що помилка при розрахунку привела б до ряду негативних наслідків. Відлагодження та перевірка, що підтверджує вірність програмних рішень відбувалась за декількаами етапами:

- математична перевірка окремих модулів;
- математична перевірка всієї системи (з допомогою математичної логіки будується логічна схема всієї системи);
- практична перевірка підпрограм (перевіряється процедурна частина кожної підпрограми окремо);
- практична перевірка всієї системи у дії (перевіряється ситема в цілому за допомогою вводу різних даних у програму, потім на виході з програми перевіряємо отриману інформацію з очікуваною).

Для підтвердження правильності розрахунку програми були використані експеременталні дані різних аудіо форматів, були проведені консультації з даного питання зі спеціалістами.

Простота мови проектування та маніпулювання даними, зручність спілкування користувача з системою до мінімума вивчення цієї програми. Користувач програми – це людина, яка повинна володіти азами програмування. При написанні програми я намагалася, щоб програма відповідала наступним параметрам:

- Швидкодія. Програма працює постійно з великою кількістю кінцевих абонентів (селективний зв’язок).
- Захист. Забезпечити надійний захишенний канал зв`язку.
- Відсутність проблеми дороговизни сучасних персональних комп’ютерів. Система, що написана може встановлюватись на будь-якому персональному комп’ютері – використовувати відносно швидкі алгоритми захисту зв'язку.
- Можливість зручно і швидко формувати приклади і теорію для користувача.
- Можливість звертання до системних ресурсів. Користувача системи цікавить її інформаційний та сенсовий зміст. Подробиці організації фізичного зберігання даних його не цікавлять.

Перш за все перед розробкою системи слід одержати уявлення на наступні моменти:

- на які частини можна розбити систему;
- одержати уявлення про кожну частину (фрагмент);
- яка інформація і з якою детальністю необхідна користувачу кожного фрагменту;
- які процеси передачі і обробки даних знаходяться в кожному фрагменті;
- технологія накопичування і обробки аудіо інформації системи;
- на якому обладнанні планується реалізувати систему;
- технологія функціюваня системи;
- чи необхідна адаптація і настройка системи при змінах деяких умов.

Для розробки програми були попередньо збудовані функціональна схема, структурна схеми, структурна схема системи керування, схема процесів, а також блок-схеми алгоритму програми, розглянемо їх детально.

В процесі практичної реалізації теоретичних принципів розробки системи, додатково розглянутих вище, була розроблена структурна схема системи, яка зображена на рисунку 1.

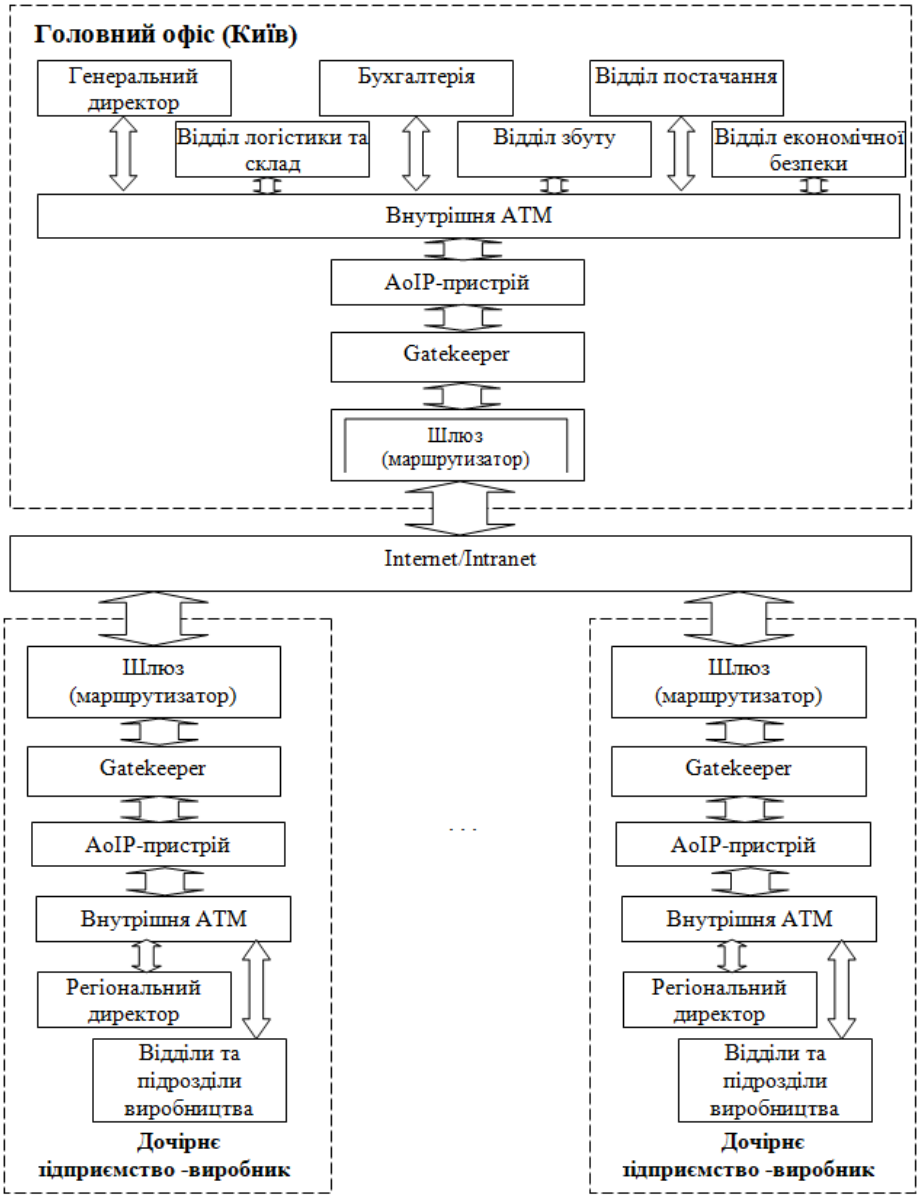


Рисунок 1 – Структурна схема системи

Завдяки структурній схемі можна чітко побачити основні структурні блоки системи та взаємозв'язки між ними. При розробці структурної схеми основний упор робився на існуючи розробки ПЗ і їх модулі допомоги. Аналіз рисунка 1 дозволяє чітко прослідити як працює програма. Розглянемо схему зверху вниз, в напрямку від пристрою до кінцевої програми – за допомогою внутрішнього пула доступу що забезпечує закриті канали зв'язку абоненти генеральний директор, відділи бухгалтерії, логістики, складу, збуту, економічної безпеки – можуть взаємодіяти з дочірніми виробниками з використанням внутрішньої АТМ. і чітко налагодженої технічної системи взаємодії. Технічна частина взаємодії забезпечується AoIP та воротарем з використанням маршрутизатора.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів уніфікованих комунікацій на базі протоколу AoIP. В межах України в недостатній мірі представлені вітчизняні розробки в цій області. У роботі наведені теоретичне узагальнення й рішення наукового завдання дослідження методів уніфікованих комунікацій на базі протоколу AoIP. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем уніфікованих комунікацій на базі протоколу AoIP; Досліджена система уніфікованих комунікацій на базі протоколу AoIP; На основі отриманих результатів досліджень створена програмна реалізація системи уніфікованих комунікацій на базі

протоколу AoIP. Розроблені під час виконання роботи алгоритми дозволяють успішно вирішувати завдання уніфікованих комунікацій на базі протоколу AoIP. 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. Іванова І.С. Дослідження та програмна реалізація системи уніфікованих комунікацій на базі протоколу AoIP // Збірник праць молодих науковців ЦНТУ. – Вип. 11. – Кропивницький: ЦНТУ, 2021.
2. Бакланов И.Г. ISDN и IP-телефония / Вестник связи, 1999, №4.
3. Будников В.Ю., Пономарев Б.А. Технологии обеспечения качества обслуживания в мультисервисных сетях / Вестник связи, 2000. №9.
4. Варламова Е. IP-телефония в России / Connect! Мир связи, 1999, №9.
5. Гольдштейн Б.С. Сигнализация в сетях связи. Том 1. М.: Радио и связь, 1998.
6. Гольдштейн Б.С. Протоколы сети доступа. Том 2. М.: Радио и связь, 1999.
7. Гольдштейн Б.С., Ехриель И.М., Рерле Р.Д. Интеллектуальные сети. М.: Радио и связь, 2000.
8. Кузнецов А.Е., Пинчук А. В., Суховицкий А.Л. Построение сетей IP-телефонии / Компьютерная телефония, 2000, №6.
9. Кульгин М. Технологии корпоративных сетей. Изд. «Питер», 1999.
10. Ломакин Д. Технические решения IP-телефонии / Мобильные системы, 1999 №8.
11. 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

УДК 004

Б. Клименко, магістр гр. КІ-19М-1,4
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ РЕАЛІЗАЦІЇ DLP-АГЕНТУ

У статті розроблено програмне забезпечення, яке призначено для реалізації системи реалізації DLP-агенту. Об’єктом дослідження є процес реалізації DLP-агенту. Предметом дослідження є методи реалізації DLP-агенту. Методи дослідження базуються на методах захисту інформації, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи реалізації DLP-агенту. 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, захисту інформації, DLP

Постановка проблеми. Сьогодні ринок DLP-систем є одним із самих швидкоростучих серед всіх засобів забезпечення інформаційної безпеки. Втім, вітчизняна ІБ-сфера поки не зовсім устигає за світовими тенденціями, у зв'язку із ніж у ринку DLP-систем у нашій країні є свої особливості.

Перш ніж говорити про ринок DLP-систем, необхідно визначитися з тим, що, власне кажучи, мається на увазі, коли мова йде про подібні рішення. Під DLP-системами прийнято розуміти програмні продукти, що захищають організації від витоків конфіденційної інформації. Сама абревіатура DLP розшифровується як Data Leak Prevention, тобто, запобігання витоків даних.

Подібного роду системи створюють захищений цифровий «периметр» навколо організації, аналізуючи всю вихідну, а в ряді випадків і вхідну інформацію. Контрольованою інформацією повинен бути не тільки інтернет-трафік, але й ряд інших інформаційних потоків: документи, які виносяться за межі контуру безпеки, що захищається, на зовнішніх носіях, що роздруковуються на принтері, що відправляються на мобільні носії через Bluetooth і т.д.

Оскільки DLP-система повинна перешкоджати витокам конфіденційної інформації, то вона в обов'язковому порядку має убудовані механізми визначення ступеня конфіденційності документа, виявленого в перехопленому трафіку. Як правило, найпоширеніші два способи: шляхом аналізу спеціальних маркерів документа й шляхом аналізу вмісту документа. У цей час більше розповсюджений другий варіант, оскільки він стійкий перед модифікаціями, внесеними в документ перед його відправленням, а також дозволяє легко розширювати число конфіденційних документів, з якими може працювати система.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи реалізації DLP-агенту.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи реалізації DLP-агенту.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

- Огляд існуючих систем реалізації DLP-агенту.
- Дослідження системи реалізації DLP-агенту.
- Програмна реалізація системи реалізації DLP-агенту.

Об'єктом дослідження є процес реалізації DLP-агенту.

Предметом дослідження є методи реалізації DLP-агенту.

Методи дослідження базуються на методах захисту інформації, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. DLP-систему використовують, коли необхідно забезпечити захист конфіденційних даних від внутрішніх погроз. І якщо фахівці з інформаційної безпеки в достатній мері освоїли й застосовують інструменти захисту від зовнішніх порушників, то із внутрішніми справу відбувається не так гладко.

Використання в структурі інформаційної безпеки DLP-системи припускає, що ІБ-фахівець розуміє:

- як співробітники компанії можуть організувати витік конфіденційних даних;
- яку інформацію варто захищати від погрози порушення конфіденційності.

Всебічні знання допоможуть фахівцеві краще зрозуміти принципи роботи технології DLP і настроїти захист від витоків коректним образом.

DLP-система повинна вміти відрізняти конфіденційну інформацію від неконфіденційної. Якщо аналізувати всі дані усередині інформаційної системи організації, виникає проблема надлишкового навантаження на IT-ресурси й персонал. DLP працює в основному «у зв'язуванні» з відповідальним фахівцем, що не тільки «учить» систему коректно працювати, вносить нові й видаляє неактуальні правила, але й проводить моніторинг поточних, заблокованих або підозрілих подій в інформаційній системі.

Функціональність DLP-системи будується навколо «ядра» – програмного алгоритму, що відповідає за виявлення й категоризацію інформації, що бідує в захисті від витоків. У ядрі більшості DLP-рішень закладені дві технології: лінгвістичного аналізу й технологія, заснована на статистичних методах. Також у ядрі можуть використовуватися менш розповсюджені техніки, наприклад, застосування міток або формальні методи аналізу.

Розроблювачі систем протидії витокам доповнюють унікальний програмний алгоритм системними агентами, механізмами керування інцидентами, парсерами, аналізаторами протоколів, перехоплювачами й іншими інструментами.

Ранні DLP-системи базувалися на одному методі в ядрі: або лінгвістичному, або статистичному аналізі. На практиці недоліки двох технологій компенсувалися сильними сторонами один одного, і еволюція DLP привела до створення систем, універсальних у плані «ядра».

Лінгвістичний метод аналізу працює прямо зі змістом файлу й документа. Це дозволяє ігнорувати такі параметри, як ім'я файлу, наявність або відсутність у документі грифа, хто й коли створив документа. Технологія лінгвістичної аналітики включає:

– морфологічний аналіз – пошук по всіх можливих словоформах інформації, яку необхідно захистити від витоку;

– семантичний аналіз – пошук входжень важливої (ключовий) інформації у вмісті файлу, вплив входжень на якісні характеристики файлу, оцінка контексту використання.

Лінгвістичний аналіз показує висока якість роботи з більшим обсягом інформації. Для об'ємного тексту DLP-система з алгоритмом лінгвістичного аналізу більш точно вибере коректний клас, віднесе до потрібної категорії й запустить налаштоване правило. Для документів невеликого обсягу краще використовувати методику стоп-слів, що ефективно зарекомендувала себе в боротьбі зі спамом.

Навченість у системах з лінгвістичним алгоритмом аналізу реалізована на високому рівні. У ранніх DLP-комплексів були складності із завданням категорій і інших етапів «навчання», однак у сучасних системах закладені налагоджені алгоритми самонавчання: виявлення ознак категорій, можливості самостійно формувати й змінювати правила реагування. Для налаштування в інформаційних системах подібних програмних комплексів захисту даних уже не потрібно залучати лінгвістів.

До недоліків лінгвістичного аналізу зараховують прив'язку до конкретної мови, коли не можна використовувати DLP-систему з «англійським» ядром для аналізу україномовних потоків інформації й навпаки. Інший недолік зв'язаний зі складністю чіткої категоризації з використанням імовірнісного підходу, що втримує точність спрацьовування в межах 95%, тоді як для компанії критичної може виявитися витік будь-якого обсягу конфіденційної інформації.

Статистичні методи аналізу, навпроти, демонструють точність, близьку до 100-процентного. Недолік статистичного ядра пов'язаний з алгоритмом самого аналізу.

На першому етапі документ (текст) ділиться на фрагменти прийнятної величини (не посимвольно, але досить, щоб забезпечити точність спрацьовування). Із фрагментів знімається ґеш (в DLP-системах зустрічається як термін Digital Fingerprint – «цифровий відбиток»). Потім ґеш рівняється з ґешем еталонного фрагмента, узятого з документа. При збігу система позначає документ як конфіденційний і діє відповідно до політиків безпеки.

Недолік статистичного методу в тому, що алгоритм не здатний самостійно навчатися, формувати категорії й типізувати. Як наслідок – залежність від компетенцій фахівця й імовірність завдання ґешу такого розміру, при якому аналіз буде давати надлишкова кількість помилкових спрацьовувань. Усунути недолік нескладно, якщо дотримуватися рекомендацій розроблювача по налаштуванню системи.

З формуванням ґешів зв'язаний і інший недолік. У розвинених IT-системах, які генерують більші обсяги даних, база відбитків може досягати такого розміру, що перевірка трафіку на збіги з еталоном серйозно сповільнить роботу всієї інформаційної системи.

Перевага рішень полягає в тому, що результативність статистичного аналізу не залежить від мови й наявності в документі нетекстової інформації. Ґеш однаково добре знімається й з англійської фрази, і із зображення, і з відеофрагмента.

Лінгвістичні й статистичні методи не підходять для виявлення даних певного формату для будь-якого документа, наприклад, номера рахунків або паспорта. Для виявлення в масиві інформації подібних типових структур у ядро DLP-системи впроваджують технології аналізу формальних структур.

У якісному DLP-рішенні використовуються всі засоби аналізу, які працюють послідовно, доповнюючи один одного.

Визначити, які технології присутні в ядрі, можна по описі можливостей конкретного DLP-комплексу.

Не менше значення, ніж функціональність ядра, мають рівні контролю, на яких працює DLP-система. Їх два:

- рівень мережі, коли контролюється мережний трафік в інформаційній системі;
- рівень хосту, коли контролюється інформація на робочих станціях.

Розроблювачі сучасних DLP-продуктів відмовилися від відособленої реалізації захисту рівнів, оскільки від витоку потрібно захищати й кінцеві пристрої, і мережа.

Мережний рівень контролю при цьому повинен забезпечувати максимально можливий охват мережних протоколів і сервісів. Мова йде не тільки про «традиційні» канали (поштові протоколи, FTP, HTTP-трафік), але й про більше нові системи мережного обміну (Instant Messengers, хмарні сховища). На жаль, на мережному рівні неможливо контролювати шифрований трафік, але дана проблема в DLP-системах вирішена на рівні хосту.

Контроль на хостовому рівні дозволяє вирішувати більше завдань по моніторингу й аналізу. Фактично ІБ-служба одержує інструмент повного контролю за діями користувача на робочій станції. DLP з хостовою архітектурою дозволяє відслідковувати, що копіюється на знімний носій, які документи відправляються на печатку, що набирається на клавіатурі, записувати аудіоматеріали, робити знімки екрана. На рівні кінцевої робочої станції перехоплюється шифрований трафік (наприклад, Skype), а для перевірки відкриті дані, які обробляються в сучасний момент і які тривалий час зберігаються на ПК користувача.

Крім рішення звичайних завдань, DLP-системи з контролем на хостовому рівні забезпечують додаткові заходи по забезпеченню інформаційної безпеки: контроль установки й зміни ПЗ, блокування портів уведення-виводу й т.п.

Мінуси хостової реалізації в тому, що системи з великим набором функцій складніше адмініструвати, вони більше вимогливі до ресурсів самої робочої станції. Керуючий сервер регулярно звертається до модуля-«агента» на кінцевому пристрої, щоб перевірити доступність і актуальність налаштувань. Крім того, частина ресурсів користувальницької робочої станції буде неминуче «з'їдатися» модулем DLP. Тому ще на етапі підбора рішення для запобігання витоку важливо звернути увагу на апаратні вимоги.

Принцип поділу технологій в DLP-системах залишився в минулому. Сучасні програмні рішення для запобігання витоків задіють методи, які компенсують недоліки один одного. Завдяки комплексному підходу конфіденційні дані усередині периметра інформаційної безпеки стає більше стійкими до погроз.

Відсіяти невідповідні системи на попередньому етапі допоможе грамотне технічне завдання. Критерії вибору, які варто враховувати при складанні документа, включають:

- кількість контрольованих каналів;
- надійність і швидкість роботи системи;
- аналітичні можливості;
- експертиза, досвід і надійність розроблювача;
- наявність, якість і швидкість реакції техпідтримки;
- ціна й вартість володіння системою.

Основна вимога до DLP-системи – уміння запобігти витоку конфіденційних даних по кожному з каналів, які використовуються в компанії. Якщо рішення не «закриває» хоча б один, варто пильно вивчити інші можливості системи й зрозуміти, чи компенсують вони відсутність контролю потрібного каналу передачі даних.

Базові функції DLP включають також контроль зберігання, використання й переміщення критично важливих документів усередині корпоративної інфраструктури. Частина DLP-рішень, представлених на українському ІБ-ринку, дозволяють при необхідності блокувати конфіденційну інформацію й робити резервування (зберігати тіньові копії). Ряд DLP-систем здатні шифрувати дані, щоб їх неможливо було прочитати за периметром компанії.

Традиційна класифікація має на увазі дві групи DLP-систем:

– активні, здатні блокувати конфіденційну інформацію при виявленні порушень;

– пасивні, здатні тільки «спостерігати» за потоками даних без можливості втрутитися й вплинути на процеси.

Сучасні рішення для запобігання витоків – це комплекси «два в одному», здатні працювати й в активному, і в пасивному режимі.

Сполучення двох режимів в DLP-системі дає перевага вже на етапі тестування. Впровадження DLP активного типу супроводжується ризиком припинення налагоджених бізнес-процесів через некоректні налаштування або неналагоджену реакцію на події. Установка DLP-комплексу в пасивному тестовому режимі дає можливість спокійно переконатися, що правила моніторингу й реакції налаштовані коректно, канали руху інформації – під безперервним спостереженням, а системи логування й архівування не перевантажують мережну інфраструктуру.

Інший критерій класифікації DLP-рішень – по методах архітектурної реалізації.

Хостові DLP припускають установку програм-«агентів» на комп'ютери користувачів. Агенти стежать за дотриманням політик безпеки й не дають робити потенційно небезпечні дії, наприклад, запускати ПЗ зі знімних пристроїв. Одночасно агенти реєструє всі дії користувачів і передають інформацію в єдину базу. У такий спосіб ІБ-фахівець одержує повне подання про те, що відбувається в корпоративній мережі.

Основна перевага хостових рішень полягає в більше повному контролі каналів передачі інформації й дій користувача на робочому місці. Агенти фіксують всі операції за комп'ютером, плюс DLP-рішення нового покоління дозволяють записувати переговори співробітників або, наприклад, підключаються до веб-камери. Недолік хостових систем у тім, що контроль поширюється тільки на пристрої, які підключаються прямо й безпосередньо взаємодіють із робочою станцією.

При виборі хостових DLP-систем варто звернути увагу, яким способом установлюються агенти на комп'ютери користувачів. Функція вилученої установки й адміністрування позбавить ІБ-фахівців від необхідності вручну ставити агента на кожну робочу станцію.

Інша важлива вимога до агентських компонентів хостових DLP – схований режим роботи й захист від видалення. Якщо в користувача є права локального адміністратора й рівень IT-Грамотності вище за середнє, він потенційно може припинити роботу агентів і вивести комп'ютер з-під «поля зору» DLP-системи.

Мережні DLP засновані на застосуванні централізованих серверів, куди перенаправляється копія вхідні й вихідного трафіку для перевірки на відповідність політикам безпеки. Мережні рішення забезпечують високий рівень захисту від несанкціонованого впливу, тому що дозволяють обмежити доступ до виділеного шлюзу й надати права адміністрування вузькому колу співробітників.

Область застосування мережних DLP-систем обмежена, відповідно, мережними протоколами й каналами: SMTP, POP3, HTTP(S), IMAP, MAPI, NNTP, ICQ, XMPP, MMP, MSN, SIP, FTP і т.д. Вагомим аргументом на користь мережного DLP-рішення буде, відповідно, здатність контролювати всі протоколи передачі даних, затребувані в компанії. З погляду адміністратора безпеки привабливості мережному DLP-комплексу додасть легкість впровадження й налаштування.

Хостові й мережні DLP-системи контролюють різні канали передачі інформації, і логічним кроком розроблювачів стала інтеграція можливостей різнотипних рішень. Практично всі сучасні інструменти запобігання витоків на ІБ-ринку – універсальні комплекси.

Крім архітектурних варто враховувати також особливості адміністрування DLP-систем. У порівнянні потрібно врахувати алгоритми розгортання компонентів системи, методи розподілу ролей, реалізацію консолі керування. Адміністраторові безпеки треба

попередньо оцінити інформативність інтерфейсу, складність налаштування правил і інші параметри, від яких залежить зручність керування комплексом захисту інформації.

Незважаючи на те, що закордонні виробники приділяють серйозну увагу локалізації продуктів, за інших рівних умов краще вибрати систему з «рідними» лінгвістичними алгоритмами.

Для державних організацій і установ у Україні вибір на користь вітчизняних DLP-рішень продиктований законом про імпортозаміщення. У державному секторі при проведенні тендерів українські рішення користуються преференціями. Криємо того, у системах забезпечення інформаційної безпеки рекомендується використовувати продукти, сертифіковані регуляторами, наприклад. Для державних установ використання несертифікованих DLP-систем неприпустимо, а при впровадженні ІБ-рішень потрібні сертифікати «внутрішніх» регуляторів.

Аналітичні можливості DLP-систем

Формування звітності залежить від можливостей DLP-системи не тільки вести моніторинг, але й архівувати перехоплену інформацію. Тіньова копія може включати різні типи даних: веб-трафік; поштові відправлення; активність на принтерах; файли, записувані на USB-носії; інформацію, що проходить по мережних протоколах. Тіньове копіювання є ефективним засобом розслідування інцидентів, однак можливість зберігати «резервну копію» закладена не у всіх DLP-системах. Причина – додаткове навантаження на мережні ресурси й робітники станції кінцевих користувачів.

Скільки коштує DLP?

Важливий критерій, що звузить коло підходящих рішень на етапі формування вимог до DLP-системи, – ціна продукту. Хостові й мережні системи коштують дешевше універсальних. Загальний принцип ціноутворення зводиться до простої формули: ніж більше додаткових опцій, тим вище кінцева вартість рішення.

Ціна DLP-системи прямо пропорційна наявності розширеного інструментарію, включаючи механізм розпізнавання тексту в зображенні, модулі лінгвістичного аналізу, технології самонавчання й інші функції. Ніж вище вимоги до захисту корпоративної інформації й ніж солідніше бюджет на інформаційну безпеку, тим більше «просунутої» буде DLP-система. До «просунутих» функцій, наприклад, відносять:

- здатність визначати транслітерацію;
- аналіз тексту по методу Байєса;
- застосування сигнатур і регулярних виражень;
- технологію «цифрових відбитків» для аналізу документів з мало змінюваною структурою й змістом;
- модулі OCR (Optical Character Recognition – оптичного розпізнавання символів) і інші високотехнологичні засоби контентного аналізу.

Витрати на DLP-систему включають не тільки вартість самого продукту. Остаточна сума формується по декількох статтях витрат.

Один з варіантів знизити вартість рішення – з'ясувати, є чи можливість купити окремі модулі DLP, щоб не переплачувати за непотрібні канали перехоплення.

Заключний етап

Перед тим, як вибрати єдино вірне DLP-рішення, варто провести випробування під реальним навантаженням. Для тестування необхідно вибрати 2-3 системи відповідно до технічного завдання й бюджетом. Тестуванню DLP-системи передує складання програми й методики випробувань. Щоб виявити всі нюанси й перевірити надійність ПЗ, буде потрібно від двох тижнів до місяця. За підсумками залишиться тільки зрівняти результати й вибрати DLP, що відповідає всім критеріям.

Розробка структурної схеми

Якщо бути досить послідовним у визначеннях, то можна сказати, що інформаційна безпека почалася саме з появи DLP-систем. До цього всі продукти, які займалися

«інформаційною безпекою», насправді захищали не інформацію, а інфраструктуру – місця зберігання, передачі й обробки даних. Комп'ютер, додаток або канал, у яких перебуває, обробляється або передається конфіденційна інформація, захищаються цими продуктами точно так само, як і інфраструктура, у якій звертається зовсім необразлива інформація. Тобто саме з появою DLP-продуктів інформаційні системи навчилися нарешті-те відрізняти конфіденційну інформацію від неконфіденційної. Можливо, із вбудовуванням DLP-технологій в інформаційну інфраструктуру компанії зможуть сильно заощадити на захисті інформації – наприклад, використовувати шифрування тільки в тих випадках, коли зберігається або передається конфіденційна інформація, і не шифрувати інформацію в інших випадках.

Однак ця справа майбутнього, а в сьогоденні дані технології використовуються в основному для захисту інформації від витоків. Технології категоризації інформації становлять ядро DLP-систем. Кожний виробник уважає свої методи детектування конфіденційної інформації унікальними, захищає їхніми патентами й придумує для них спеціальні торговельні марки. Адже інші, відмінні від цих технологій, елементи архітектури (перехоплювачі протоколів, парсери форматів, керування інцидентами й сховища даних) у більшості виробників ідентичні, а у великих компаній навіть інтегровані з іншими продуктами безпеки інформаційної інфраструктури. В основному для категоризації даних у продуктах по захисту корпоративної інформації від витоків використовуються дві основних групи технологій – лінгвістичний (морфологічний, семантичний) аналіз і статистичні методи (Digital Fingerprints, Document DNA, антиплагіат). Кожна технологія має свої сильні й слабкі сторони, які визначають область їхнього застосування.

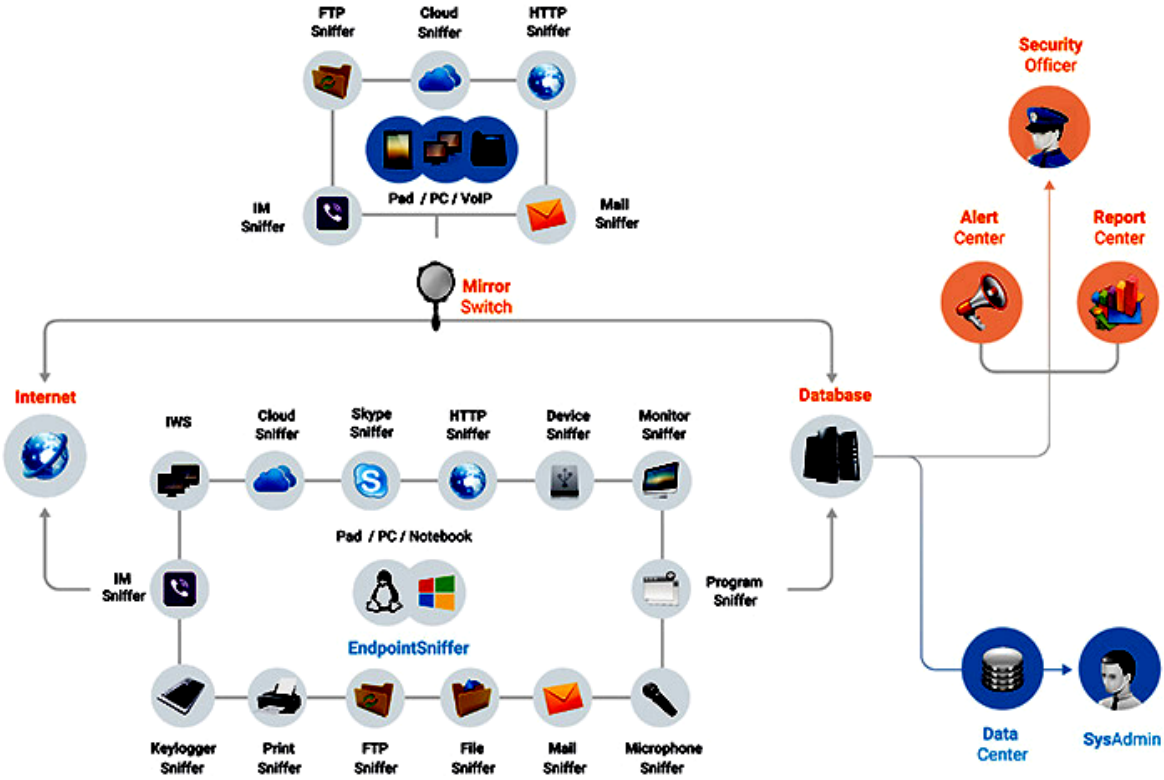


Рисунок 1 – Структурна схема системи

Лінгвістичний аналіз

Використання стоп-слів («секретно», «конфіденційно» і тому подібних) для блокування вихідних електронних повідомлень у поштових серверах можна вважати прабатьком сучасних DLP-систем. Звичайно, від зловмисників це не захищає – видалити стоп-слово, найчастіше винесене в окремого грифа документа, не становить праці, при цьому зміст тексту анітрошки не зміниться.

Поштовх у розробці лінгвістичних технологій був зроблений на початку цього століття творцями email-фільтрів. Насамперед, для захисту електронної пошти від спаму. Це зараз в антиспамовських технологіях переважають репутаційні методи, а на початку століття йшла справжня лінгвістична війна між снарядом і бронею – спамерами й антиспамерами. Пам'ятаєте найпростіші методи для обману фільтрів, що базуються на стоп-словах? Заміна букв на схожі букви з інших кодувань або цифри, трансліт, випадковим образом розставлені пробіли, підкреслення або переходи рядків у тексті. Антиспамери досить швидко навчилися боротися з такими хитростями, але тоді з'явилися графічний спам та інші хитрі різновиди небажаної кореспонденції.

Однак використовувати антиспамерські технології в DLP-продуктах без серйозної доробки неможливо. Адже для боротьби зі спамом досить ділити інформаційний потік на дві категорії: спам і не спам. Метод Байєса, що використовується при детектуванні спаму, дає тільки бінарний результат: «так» або «ні». Для захисту корпоративних даних від витоків цього недостатньо – не можна просто ділити інформацію на конфіденційну й неконфіденційну. Потрібно вміти класифікувати інформацію з функціональної приналежності (фінансова, виробнича, технологічна, комерційна, маркетингова), а усередині класів – категоризувати її за рівнем доступу (для вільного поширення, для обмеженого доступу, для службового використання, секретна, зовсім секретна й так далі).

Більшість сучасних систем лінгвістичного аналізу використовують не тільки контекстний аналіз (тобто в якому контексті, у сполученні з якими іншими словами використовується конкретний термін), але й семантичний аналіз тексту. Ці технології працюють тим ефективніше, ніж більше аналізований фрагмент. На великому фрагменті тексту точніше проводиться аналіз, з більшою ймовірністю визначається категорія й клас документа. При аналізі ж коротких повідомлень (SMS, інтернет-пейджери) нічого кращого, ніж стоп-слова, дотепер не придумано.

Переваги технології

Переваги лінгвістичних технологій у тім, що вони працюють прямо зі змістом документів, тобто їм не важливо, де і як був створений документ, який на ньому гриф і як називається файл – документи захищаються негайно. Це важливо, наприклад, при обробці чернеток конфіденційних документів або для захисту вхідної документації. Якщо документи, створені й використовуються усередині компанії, ще якось можна специфічним образом іменувати, надавати гриф або мітити, то вхідні документи можуть мати не прийняті в організації грифи й мітки. Чернетки (якщо вони, звичайно, не створюються в системі захищеного документообігу) теж можуть уже містити конфіденційну інформацію, але ще не містити необхідних грифів і міток.

Ще одна перевага лінгвістичних технологій – їхня навченість. Якщо ти хоч раз у житті натискав у поштовому клієнті кнопку «Не спам», то вже представляєш клієнтську частину системи навчання лінгвістичного движка. Помічу, що тобі зовсім не потрібно бути дипломованим лінгвістом і знати, що саме зміниться в базі категорій – досить указати системі помилкове спрацьовування, все інше вона зробить сама.

Третім перевагам лінгвістичних технологій є їхня масштабованість. Швидкість обробки інформації пропорційна її кількості й абсолютно не залежить від кількості категорій. Донедавна побудова ієрархічної бази категорій (історично неї називають БКФ – база контентної фільтрації, але ця назва вже не відбиває справжнього змісту) виглядало якимсь шаманством професійних лінгвістів, тому налаштування БКФ можна було сміло віднести до недоліків. Але з виходом в 2010 відразу декількох продуктів-«автолінгвистів» побудова первинної бази категорій стало гранично простим – системі вказуються місця, де зберігаються документи певної категорії, і вона сама визначає лінгвістичні ознаки цієї категорії, а при помилкових спрацьовуваннях – самостійно навчається. Так що тепер до достоїнств лінгвістичних технологій додалася простота налаштування.

І ще одне перевага лінгвістичних технологій, що хочеться відзначити в розділі – можливість детектувати в інформаційних потоках категорії, не пов'язані з документами, що

перебувають усередині компанії. Інструмент для контролю вмісту інформаційних потоків може визначати такі категорії, як протиправна діяльність (піратство, поширення заборонених товарів), використання інфраструктури компанії у власних цілях, нанесення шкоди іміджу компанії (наприклад, поширення слухів, що ганьблять) і так далі.

Недоліки технологій

Основним недоліком лінгвістичних технологій є їхня залежність від мови. Неможливо використовувати лінгвістичний движок, розроблений для однієї мови, з метою аналізу іншого. Це було особливо помітно при виході на український ринок американських виробників – вони були не готові зштовхнутися з українським словотвором і наявністю шести кодувань. Недостатньо було перекласти на українську мову категорії й ключові слова – в англійській мові словотвір досить простої, а відмінки виносяться в приводи, тобто при зміні падежу міняється привід, а не саме слово. Більшість іменників в англійській мові стають дієсловами без змін слова. І так далі. В українському всі не так – один корінь може породити десятки слів у різних частинах мови.

У Німеччині американських виробників лінгвістичних технологій зустріла інша проблема – так звані «компаунди», складені слова. У німецькій мові прийнято приєднувати визначення до головного слова, у результаті чого виходять слова, що іноді складаються з десятка корінь. В англійській мові такого немає, там слово – послідовність букв між двома пробілами, відповідно англійська лінгвістичний движок виявилася нездатний обробити незнайомі довгі слова.

Справедливості заради варто сказати, що зараз ці проблеми багато в чому американськими виробниками вирішені. Довелося досить сильно переробити (а іноді й писати заново) мовний движок, але великі ринки Україні й Німеччини напевно того коштують. Також складно обробляти лінгвістичними технологіями мультимовні тексти. Однак із двома мовами більшість движків все-таки справляються, звичайно це національна мова + англійська – для більшості бізнес-завдань цього цілком достатньо. Хоча авторові зустрічалися конфіденційні тексти, що містять, наприклад, одночасно казахський, українське й англійська, але це скоріше виключення, ніж правило.

Ще одним недоліком лінгвістичних технологій для контролю всього спектра корпоративної конфіденційної інформації є те, що не вся конфіденційна інформація перебуває у вигляді зв'язних текстів. Хоча в базах даних інформація й зберігається в текстовому виді, і немає ніяких проблем витягти текст із СУБД, отримана інформація найчастіше містить власні імена – ПІБ, адреси, назви компаній, а також цифрову інформацію – номера рахунків, кредитних карт, їхній баланс та інше. Обробка подібних даних за допомогою лінгвістики багато користі не принесе. Те ж саме можна сказати про формати CAD/CAM, тобто кресленнях, у яких найчастіше втримується інтелектуальна власність, програмних кодах і медійних (відео/аудіо) форматах – якісь тексти з них можна витягти, але їхня обробка також неефективна. Ще року три назад це стосувалося й відсканованих текстів, але лідируючі виробники DLP-систем оперативно додали оптичне розпізнавання й упоралися із цією проблемою.

Але самим більшим і найбільше часто критикуємим недоліком лінгвістичних технологій є все-таки імовірнісний підхід до категоризації. Якщо ти коли-небудь читав лист із категорією «Probably SPAM», то зрозумієш, про що я. Якщо таке діється зі спамом, де всього дві категорії (спам/не спам), можна собі представити, що буде, коли в систему завантажать кілька десятків категорій і класів конфіденційності. Хоча навчанням системи можна досягти 92-95% точності, для більшості користувачів це означає, що кожне десяте або двадцяте переміщення інформації буде помилково приписано не до того класу з усіма наслідками, що випливають для бізнесу (витік або переривання легітимного процесу).

Звичайно не прийнято відносити до недоліків складність розробки технології, але не згадати про ній не можна. Розробка серйозного лінгвістичного движка з категоризацією текстів більш ніж по двох категоріях – наукомісткий і досить складний технологічно процес. Прикладна лінгвістика – швидко, що розвивається наука, що одержала сильний поштовх у

розвитку з поширенням інтернет-пошуку, але сьогодні на ринку присутні одиниці працездатних движків категоризації: для української мови їх усього два, а для деяких мов їх просто ще не розробили. Тому на DLP-ринку існує лише пари компаній, які здатні повною мірою категоризувати інформацію «на льоту». Можна припустити, що коли ринок DLP збільшиться до багатомільярдних розмірів, на нього з легкістю вийде Google. Із власним лінгвістичним движком, відтестованим на трильйонах пошукових запитів по тисячах категорій, йому не важко буде відразу відрізати серйозний шматок цього ринку.

Статистичні методи

Завдання комп'ютерного пошуку значимих цитат (чому саме «значимих» – небагато пізніше) зацікавили лінгвістів ще в 70-х роках минулого століття, якщо не раніше. Текст розбивався на шматки певного розміру, з кожного з яких знімався ґеш. Якщо деяка послідовність ґешів зустрічалася у двох текстах одночасно, то з великою ймовірністю тексти в цих областях збігалися.

Побічним продуктом досліджень у цій області є, наприклад, «альтернативна хронологія» Анатолія Фоменко, шановного вченого, що займався «кореляціями текстів» і один раз зрівняв українські літописи різних історичних періодів. Зачудувавшись, наскільки збігаються літописи різних століть (більш ніж на 60%), наприкінці 70-х він висунув теорію, що наша хронологія на кілька століть коротше. Тому, коли якась вихідна на ринок DLP-компанія пропонує «революційну технологію пошуку цитат», можна з великою ймовірністю затверджувати, що нічого, крім нової торговельної марки, компанія не створила.

Статистичні технології відносяться до текстів не як до зв'язної послідовності слів, а як до довільної послідовності символів, тому однаково добре працюють із текстами на будь-яких мовах. Оскільки будь-який цифровий об'єкт – хоч картинка, хоч програма – теж послідовність символів, те ті ж методи можуть застосовуватися для аналізу не тільки текстової інформації, але й будь-яких цифрових об'єктів. І якщо збігаються ґеши у двох аудіофайлах – напевно в одному з них утримується цитата з іншого, тому статистичні методи є ефективними засобами захисту від витоку аудіо й відео, що активно застосовуються в музичних студіях і кінокомпаніях.

Самий час повернутися до поняття «значима цитата». Ключовою характеристикою складного ґешу, що знімається з об'єкта, що захищається, (який у різних продуктах називається те Digital Fingerprint, те Document DNA), є крок, з яким знімається ґеш. Як можна зрозуміти з опису, такий «відбиток» є унікальною характеристикою об'єкта й при цьому має свій розмір. Це важливо, оскільки якщо зняти відбитки з мільйонів документів (а це обсяг сховища середнього банку), те для зберігання всіх відбитків знадобиться достатня кількість дискового простору. Від кроку ґешу залежить розмір такого відбитка – ніж менше крок, тим більше відбиток. Якщо знімати ґеш із кроком в один символ, то розмір відбитка перевищить розмір самого зразка. Якщо для зменшення «ваги» відбитка збільшити крок (наприклад, 10 000 символів), то разом із цим збільшується ймовірність того, що документ, що містить цитату зі зразка довжиною в 9 900 символів, буде конфіденційним, але при цьому проскочить непомітно.

З іншого боку, якщо для збільшення точності виявлення брати дуже дрібний крок, кілька символів, то можна збільшити кількість помилкових спрацьовувань до неприйнятної величини. У термінах тексту це означає, що не варто знімати ґеш із кожної букви – всі слова складаються з букв, і система буде приймати наявність букв у тексті за зміст цитати з тексту-зразка. Звичайно виробники самі рекомендують деякий оптимальний крок зняття ґешів, щоб розмір цитати був достатній і при цьому вага самого відбитка була невеликою – від 3% (текст) до 15% (стисле відео). У деяких продуктах виробники дозволяють міняти розмір значимості цитати, тобто збільшувати або зменшувати крок ґешу.

Переваги технології

Як можна зрозуміти з опису, для детектування цитати потрібний об'єкт-зразок. І статистичні методи можуть із гарною точністю (до 100%) сказати, є в перевіряється файле, що, значима цитата із чи зразка ні. Тобто система не бере на себе відповідальність за

категоризацію документів – така робота повністю лежить на совісті того, хто категорував файли перед зняттям відбитків. Це сильно полегшує захист інформації у випадку, якщо на підприємстві в деякому місці (місцях) зберігаються нечасто змінюються й уже категоровані файли. Тоді досить із кожного із цих файлів зняти відбиток, і система буде, відповідно до налаштувань, блокувати пересилання або копіювання файлів, що містять значимі цитати зі зразків.

Незалежність статистичних методів від мови тексту й нетекстової інформації – теж незаперечна перевага. Вони гарні при захисті статичних цифрових об'єктів будь-якого типу – картинок, аудіо/відео, баз даних. Про захист динамічних об'єктів я розповім у розділі «недоліки».

Недоліки технології

Як і у випадку з лінгвістикою, недоліки технології – зворотна сторона достоїнств. Простота навчання системи (указав системі файл, і він уже захищений) перекладає на користувача відповідальність за навчання системи. Якщо раптом конфіденційний файл виявився не в тому місці або не був проіндексований по недбалості або злому намірі, то система його захищати не буде. Відповідно, компанії, що піклуються про захист конфіденційної інформації від витоку, повинні передбачити процедуру контролю того, як індексуються DLP-системою конфіденційні файли.

Ще один недолік – фізичний розмір відбитка. Автор неодноразово бачив вражаючі пілотні проекти на відбитках, коли DLP-система з 100% імовірністю блокує пересилання документів, що містять значимі цитати із трьохсот документів-зразків. Однак через рік експлуатації системи в бойовому режимі відбиток кожного вихідного листа рівняється вже не із трьома сотнями, а з мільйонами відбитків-зразків, що істотно сповільнює роботу поштової системи, викликаючи затримки в десятки хвилин.

Як я й обіцяв вище, опишу свій досвід по захисту динамічних об'єктів за допомогою статистичних методів. Час зняття відбитка прямо залежить від розміру файлу і його формату. Для текстового документа типу цієї розділу це займає частки секунди, для півторагодинного MP 4-фільми – десятки секунд. Для рідкозмінюємих файлів це не критично, але якщо об'єкт міняється щохвилини або навіть секунду, то виникає проблема: після кожної зміни об'єкта з його потрібно зняти новий відбиток…Код, над яким працює програміст, ще не сама більша складність, набагато гірше з базами даних, використовуваними в біллінгу, АБС або call-центрах. Якщо час зняття відбитка більше, ніж час незмінності об'єкта, то завдання рішення не має. Це не такий вуж і екзотичний випадок – наприклад, відбиток бази даних, що зберігає номера телефонів клієнтів федерального стільникового оператора, знімається кілька днів, а міняється щомиті. Тому, коли DLP-вендор затверджує, що його продукт може захистити вашу базу даних, подумки додавайте слово «квазистатичну».

Єдність і боротьба протилежностей

Як видно з попереднього розділу розділу, сила однієї технології проявляється там, де слабка інша. Лінгвістиці не потрібні зразки, вона категорує дані на льоту й може захищати інформацію, з якої випадково або навмисне не був знятий відбиток. Відбиток дає кращу точність і тому переважніше для використання в автоматичному режимі. Лінгвістика відмінно працює з текстами, відбитки – з іншими форматами зберігання інформації.

Тому більшість компаній-лідерів використовують у своїх розробках обидві технології, при цьому одна з них є основний, а інша – додаткової. Це пов'язане з тим, що споконвічно продукти компанії використовували тільки одну технологію, у якій компанія просунулася далі, а потім, на вимогу ринку, була підключена друга. Так, наприклад, раніше InfoWatch використовував тільки ліцензовану лінгвістичну технологію Morph-OLogic, а Websense – технологію PreciseID, що відноситься до категорії Digital Fingerprint, але зараз компанії використовують обидва методи. В ідеалі використовувати дві ці технології потрібно не паралельно, а послідовно. Наприклад, відбитки краще впораються з визначенням типу документа – договір це або балансова відомість, наприклад. Потім можна підключати вже

лінгвістичну базу, створену спеціально для цієї категорії. Це сильно заощаджує обчислювальні ресурси.

За межами розділу залишилися ще кілька типів технологій, використовуваних в DLP-продуктах. До таким відносяться, наприклад, аналізатор структур, що дозволяє знаходити в об'єктах формальні структури (номера кредитних карт, паспортів, ІПН і так далі), які неможливо детектувати ні за допомогою лінгвістики, ні за допомогою відбитків. Також не розкрита тема різного типу міток – від записів в атрибутних полях файлу або просто спеціального найменування файлів до спеціальних криптоконтейнерів. Остання технологія відживає своє, оскільки більшість виробників воліє не винаходити велосипед самостійно, а інтегруватися з виробниками DRM-систем, такими як Oracle IRM або Microsoft RMS.

DLP-продукти – галузь інформаційної безпеки, яка швидко розвивається, у деяких виробників нові версії виходять дуже часто, більше одного разу в рік. З нетерпінням чекаємо появи нових технологій аналізу корпоративного інформаційного поля для збільшення ефективності захисту конфіденційної інформації.

DLP працює за принципом data-centric security. Він має на увазі не захист серверів, програмного забезпечення або мереж, а контроль безпеки даних, які обробляються в системі. Відповідно до цього принципу, всі потоки інформації розділяють на три категорії:

- Data-in-use – вся інформація, з якої працюють користувачі (створення й редагування документів, медіа-контенту).
- Data-at-rest – інформація, що статично зберігається на кінцевих пристроях користувачів і в місцях загального доступу.
- Data-in-motion – дані в процесі руху, передані інформаційні потоки (транзакції, інформація про авторизації, запити « сервер-клієнт» і інші).

Для забезпечення максимально можливого захисту інформації в процесі впровадження DLP варто виконувати всі рекомендації й використовувати відразу кілька блоків захисту. Це дозволить створити економічно вигідний, робітник захисний контур. Впровадження DLP-системи повинне виконуватися поетапно від підготовки до проектування й налаштування компонентів для роботи під навантаженням у компанії.

Крок 1. Підготовка

На першому етапі впровадження DLP важливо провести підготовчі процедури. Процес підготовки компанії до установки системи захисту включає:

- аудит захищеності інформації;
- оцінка ризику;
- створення схеми розмежування доступу до даних;
- урегулювання юридичних питань.

Аудит має на увазі оцінку реального ступеня захисту інформації. На цьому підготовчому відрізку йде пошук всіх можливих каналів витоку даних і уразливостей в IT-«екосистемі». Як правило, підготовку й впровадження системи супроводжує фахівець компанії, що робить DLP, хоча в цій ролі може виступати й посередник – фірма, що надає послуги інтегрування DLP.

У кожному разі обстеження інформаційних потоків компанії включає:

1. Оцінку рівня безпеки при роботі із внутрішніми документами компанії.

2. Детальне вивчення всіх технічних ресурсів компанії, від серверів до мережних потоків.

3. Створення переліку даних, які відносяться до групи інформації з обмеженим доступом.

4. Розробка правил розмежування доступу.

5. Вивчення й опис процесів обробки, створення, передачі й зберігання інформації в рамках компанії.

Оцінка ризику й створення правил розмежування доступу – обов'язкові кроки на етапі впровадження економічно ефективної DLP-системи. Ризики оцінюються поряд з

обстеженням потенційних каналів витоку. Залежно від імовірний збиток приймається рішення про необхідність захисту каналу витоку.

Виконавець становить схему або детальний опис інформаційних потоків компанії й способів обробки даних. Далі виконавець і фахівці департаменту інформаційної безпеки компанії спільними зусиллями створюють правила розмежування доступу – набір прав, які одержує користувач системи залежно від займаної посади. Якщо в організації немає ІБ-відділу, що займається питаннями захисту, виконавець погоджує правила розмежування доступу з уповноваженою особою компанії. У процесі створення враховують режим комерційної таємниці й регламент роботи з конфіденційною інформацією.

Найчастіше, як показує практика, у замовників немає заздалегідь підготовленого опису бізнес-процесів, тому перший етап впровадження DLP-системи займає найбільше часу.

Сигналом завершення першого етапу служить перелік нормативних документів, без яких неможливо подальше впровадження системи. Список містить документи, де втримуються ймовірні сценарії й канали витоку інформації; перерахування типів і видів даних з обмеженим доступом; схема потоків інформації, доступ до якої обмежений; опис взаємодії користувачів і технічних компонентів з інформацією, доступ до якої обмежений.

Задокументовані особливості життєвого циклу конфіденційної інформації в копанні дозволяють зрозуміти, як відбувається робота з потоками даних і яких систем необхідні для їхнього захисту від несанкціонованого доступу або витоку.

При впровадженні DLP-системи важливо дотримуватися не тільки принципів захисту інформації, але й норм законодавства. Контроль за дотриманням правил роботи з конфіденційною інформацією не повинен порушувати особисті права користувачів, тому варто відмовитися від дії, які можуть бути розцінені як стеження. Додатково варто передбачити механізми контролю адміністраторів системи, у яких є доступ до всіх типів даних.

Щоб уникнути невдоволення й збурювання в колективі, у загальні відомості про роботу системи рекомендується включити пункти, де чітко позначити мети впровадження DLP-контролю й описати, як використання системи захисту інформації сприяє фінансовому благополуччю компанії. Окремо варто підкреслити, що керівник має право на захист комерційної таємниці організації, а комп'ютери й інша техніка, що надає працівникові, є власністю компанії, і для захисту власності може застосовуватися будь-яка система захисту.

Крок 2. Вибір DLP

Грамотний вибір системи DLP вимагає попереднього аналізу цінності даних, що бідують у захисті. Захист повинна бути вигідна з економічної точки зору. Інакше кажучи, вартість імовірного фінансового збитку від витоку інформації не повинна перевищувати вартості впровадження й експлуатації DLP-системи.

Після завершення першого кроку впровадження DLP-системи виконавець має чітке подання про те, які функції повинна виконувати система захисту. Попередньо слід домовитися про не тільки максимальну ціну самої системи в потрібній комплектації, але й вартість робіт з установки, налаштуванню, тестуванню й технічній підтримці.

При виборі DLP-рішення, варто з'ясувати в розроблювача:

– Складність установки й підтримки працездатності системи. Важливо врахувати наявність необхідних програмних оболонок для роботи з базами даних і фахівців, які здатні обслуговувати ПЗ: виконувати резервне копіювання, відновлення, відновлення й інші операції.

– Сценарії взаємодії зі сформованої в компанії комп'ютерною системою. DLP не повинна навантажувати існуючі обчислювальні процеси.

– Навички, які будуть потрібні ІБ-фахівцям і аналітикам, щоб виконувати посадові обов'язки по захисту від витоків даних.

Якщо обрана або рекомендована розроблювачем DLP-система не відповідає бюджету замовника, можна вибрати спрощені версії системи. Приміром, системи класу Channel DLP, які блокують канали передачі інформації без аналізу контенту або поставляються з обмеженим набором функцій для аналізу.

Крок 3. Проектування системи

Основні параметри архітектури технічних каналів і інформаційних процесів компанії окреслюються на першому етапі впровадження системи DLP. На етапі проектування відбувається більш детальне обстеження існуючої інфраструктури з упором на канали, обрані для захисту. Ця вимога є обов'язковим і дозволяє звести до мінімуму неполадки або збої в процесі установки й початкової експлуатації.

Для створення коректної схеми взаємодії модуля захисту й всіх серверів, баз даних, проксі в процес установки DLP утягують технічних фахівців компанії-замовника.

Крок 4. Установка й налаштування DLP

Для налаштування DLP не існує єдиного алгоритму дій, оскільки більше результативний підхід полягає в постійній підтримці роботи системи й тонке переналаштування протягом усього строку використання.

Важливо встановити систему таким чином, щоб при необхідності без проблем делегувати права доступу одного користувача іншому. Також варто створити набір функцій для можливого розширення системи технічного забезпечення компанії без порушення цілісності DLP-продуктів.

Налаштування DLP – це, по суті, перевірка роботи й тестування встановлених компонентів модуля захисту під реальним навантаженням. Необхідно в першу чергу перевірити коректність обробки запитів сервера й принципів розмежування доступу.

Для компанії, де безпека даних входить до числа бізнес-пріоритетів, впровадження DLP – оптимальний вибір. Успішна інтеграція DLP дозволить контролювати всі потоки інформації, а також вчасно виявляти й усувати погрози безпеки.

З установкою DLP-системи впорається навіть починаючий системний адміністратор. А от тонке налаштування DLP вимагає деяких навичок і досвіду.

Фундамент стабільної роботи продуктів класу DLP заставляється на етапі впровадження, що включає:

- визначення критичної інформації, що підлягає захисту;
- розробку політики конфіденційності;
- налаштування бізнес-процесів для рішення питань інформаційної безпеки.

Виконання подібних завдань вимагає вузької спеціалізації й поглибленого вивчання DLP-системи.

Класифікація систем захисту

Вибір DLP-системи залежить від завдань, які потрібно вирішити конкретної компанії. У самому загальному виді завдання діляться на кілька груп, включаючи контроль руху конфіденційної інформації, нагляд за активністю співробітників протягом дня, моніторинг мережної (аналіз шлюзів) і комплексний (мережі й кінцеві робочі станції).

Для цілей більшості компаній оптимальним буде вибір комплексного DLP-рішення. Для малих і середніх підприємств підійдуть хостові системи. Плюси хостових DLP – задовільна функціональність і невисока вартість. Серед мінусів – низькі продуктивність, масштабованість, стійкість відмов.

У мережних DLP подібних недоліків немає. Вони легко інтегруються й взаємодіють із рішеннями інших вендорів. Це важливий аспект, оскільки DLP-система повинна злагоджено працювати в тандемі із продуктами, уже встановленими в корпоративній мережі. Не менш важлива й сумісність DLP з базами даних і використовуваним програмним забезпеченням.

При виборі DLP ураховуються канали передачі даних, які використовуються в компанії й мають потребу в захисті. Найчастіше це протоколи електронної пошти, IP-

телефонії, HTTP; бездротові мережі, Bluetooth, знімні носії, печатка на принтерах, мережних або працюючих автономно.

Функції моніторингу й аналізу – важливі складові коректної роботи DLP-системи. Мінімальні вимоги до аналітичних інструментів включають морфологічного й лінгвістичного аналізу, здатність співвідносити контрольовані дані зі словниками або збереженими файлами-«еталонами».

З технічної точки зору сучасні DLP-рішення багато в чому збігаються. Результативність роботи системи залежить від грамотного налаштування автоматизації пошукових алгоритмів. Тому перевагою продукту буде простий і зрозумілий процес налагодження DLP, що не зажадає регулярних консультацій у технічних фахівців вендору.

Підходи до впровадження й налаштування

Установка DLP-системи в компанії найчастіше йде по одному із двох сценаріїв.

– **Класичний підхід** означає, що компанія-замовник самостійно встановлює перелік відомостей, що бідують у захисті, особливості їхньої обробки й передачі, а система контролює інформаційний потік.

– **Аналітичний підхід** полягає в тому, що система спочатку аналізує інформаційні потоки, щоб вичленувати відомості, що бідують у захисті, а потім відбувається тонке налаштування для більше точного моніторингу й забезпечення захисту інформаційних потоків.

Таблиця 1 – Етапи впровадження DLP

За класичною схемою	За аналітичною схемою
Аналіз базових бізнес-процесів і оформлення переліку конфіденційних даних	Створення проекту DLP-захисту
«Інвентаризація» носіїв і маршрутів руху даних, яким загрожують несанкціоновані дії	Установка мінімальних дозволів конфіденційної політики
Оформлення процедури роботи з інформаційним сервісами, включаючи інтернет-ресурси, з'ємні пристрої, ПК, ноутбуки, планшети, принтери, копіювальну техніку, друковані носії	Ознайомлення відповідальних за роботу DLP фахівців з базовими принципами функціонування системи
Ознайомлення співробітників з вимогами до оберту інформації в компанії	Запуск системи в дослідному режимі
Створення проекту DLP із вказівкою способів реагування системи на виявлені інциденти, а також способів зовнішнього керування	Аналіз результатів дослідного запуску
Запуск дослідної системи в режимі спостереження	Внесення змін у налаштування системи
Навчання фахівців, відповідальних за роботу DLP	Запуск системи в «промислову» експлуатацію
Аналіз дослідного запуску DLP-системи, при необхідності – додаткове налаштування	Регулярний аналіз роботи системи, коректування параметрів.
Запуск системи в «промислову» експлуатацію	
Регулярний аналіз роботи системи, коректування параметрів	

Проблеми в процесі експлуатації DLP

Практика показує: найчастіше проблеми функціонування DLP-систем криються не в технічних особливостях роботи, а в завищених очікуваннях користувачів. Тому набагато краще спрацьовує аналітичний підхід до впровадження захисту, його ще називають консалтинговим. «Зрілі» у питаннях ІБ компанії, які вже зіштовхувалися із впровадженням інструментів захисту конфіденційних відомостей і знають, що і яким способом краще

захищати, підвищують шанси побудувати налагоджену ефективну систему захисту на базі DLP.

Розповсюджені помилки при налагодженні DLP:

– Реалізація шаблонових правил. Нерідко ІБ-підрозділу приділяється роль сервісної служби для інших підрозділів компанії, що робить «клієнтам» послуги із запобігання витоків інформації. Тоді як для результативної роботи ІБ-фахівцям потрібні доскональні знання операційної діяльності компанії, щоб «заточити» DLP-систему з обліком індивідуальних бізнес-процесів.

– Охват не всіх можливих каналів витоку конфіденційних даних. Контроль електронної пошти й HTTP-протоколів засобами DLP-системи при безконтрольному використанні FTP або USB-портів навряд чи забезпечить надійний захист конфіденційних даних. У подібній ситуації можливо встановити співробітників, пересилаючих корпоративні документи на особисту пошту, щоб попрацювати з будинку, або ледарів, що просиджують робочі годинники на сайтах знайомств або в соціальних мережах. Але проти навмисного «зливу» даних такий механізм марний.

– Помилкові інциденти, які ІБ-адміністратор не встигає обробити вручну. Збереження налаштованих за замовчуванням на практиці обертається лавиною помилкових оповіщень. Наприклад, по запиті «банківські реквізити» на ІБ-фахівця обрушується інформація про всі транзакції в компанії, включаючи оплату канцелярських приналежностей і доставки води. Адекватно обробити велику кількість фіктивних тривог система не може, тому доводиться відключати деякі правила, що послабляє захист і збільшує ризик пропустити інцидент.

– Нездатність попередити витік даних. Стандартні налаштування DLP дозволяють виявити співробітників, які займаються особистими справами на робочому місці. Щоб система зіставляла події в корпоративній мережі й указувала на підозрілу активність, знадобиться тонке налаштування.

– Погіршення ефективності DLP у зв'язку з вибудовуванням інформаційних потоків навколо системи. Систему захисту інформації треба «набудовувати» поверх бізнес-процесів і прийнятих регламентів роботи з конфіденційної інформації, а не навпаки – підганяти роботу компанії під можливості DLP.

Як вирішити проблеми?

Щоб система захисту заробила як годинники, потрібно пройти все без винятку стадії впровадження й налаштування DLP, а саме: планування, реалізація, перевірка й коректування.

Планування

Полягає в точному визначенні програми захисту даних. Відповідь на простій, здавалося б, питання: «Що будемо захищати?» – є не в кожного замовника. Розробити план допоможе чек-аркуш, складений з відповідей на більше деталізовані питання:

– Хто буде використовувати DLP-систему?
– Хто буде адмініструвати дані?
– Які перспективи застосування програми протягом трьох років?
– Які мети переслідує керівництво, впроваджуючи DLP-систему?
– Із ніж зв'язані нетипові вимоги до запобігання витоків даних у компанії?

Важлива частина планування – уточнити об'єкт захисту, або інакше кажучи, конкретизувати інформаційні активи, які передаються конкретними співробітниками. Конкретизація включає розподіл по категоріях і облік корпоративних даних. Виконання завдання звичайно виділяють в окремий проект з захисту даних.

Наступний крок – визначення реальних каналів витоку інформації, звичайно це складова аудита інформаційної безпеки в компанії. Якщо виявлені потенційно небезпечні канали не «закривають» DLP-комплексом, варто прийняти додаткові технічні міри захисту або вибрати DLP-рішення з більше повним охватом. Важливо розуміти, що DLP – діючий

способів запобігти витоку з доведеною ефективністю, але не може замінити всі сучасні інструменти захисту даних.

Реалізація

Налагодження програми відповідно до індивідуальних запитів конкретного підприємства базується на контролі конфіденційних відомостей:

- відповідно до ознак особливої документації, прийнятої в компанії;
- відповідно до ознак типової документації, загальної для всіх організацій галузі;
- с використанням правил, спрямованих на виявлення інцидентів (нетипових дій співробітників).

Триступінчастий контроль допомагає виявити навмисну крадіжку й несанкціоновану передачу інформації.

Перевірка

DLP-комплекс входить до складу системи ІБ підприємства, а не заміняє її. І ефективність роботи DLP-рішення прямо пов'язана з коректністю роботи кожного елемента. Тому перед зміною «заводської» конфігурації під приватні потреби компанії проводять докладний моніторинг і аналіз. На цьому етапі зручно прорахувати людський ресурс, необхідний для забезпечення стабільної роботи DLP-програми.

Коректування

Проаналізувавши інформацію, зібрану на етапі тестової експлуатації DLP-рішення, приступають до переналаштування ресурсу. Цей крок включає уточнення існуючих і встановлення нових правил; зміна тактики забезпечення безпеки інформаційних процесів; комплектація штату для роботи з DLP-системою, технічне вдосконаленню програми (нерідко – за участю розроблювача).

Сучасні DLP-комплекси вирішують велика кількість завдань. Однак потенціал DLP повністю реалізується тільки на основі циклічного процесу, де аналіз результатів роботи системи переміняється уточненням налаштування DLP.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів реалізації DLP-агенту. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем реалізації DLP-агенту; Досліджена система реалізації DLP-агенту; На основі отриманих результатів досліджень створена програмна реалізація системи реалізації DLP-агенту. Розроблені під час виконання роботи алгоритми дозволяють успішно вирішувати завдання реалізації DLP-агенту.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. Розробка методів підвищення оперативності передачі та захисту інформації у телекомунікаційних системах: звіт про НДР (проміжний) / Наук. кер. О.А. Смірнов. – К.:КНТУ, 2013 № ДР 0113U003086
2. Даниленко Д.О. Дисперсійний аналіз мережного трафіку для забезпечення інформаційної безпеки телекомунікаційних систем / О.О. Кузнецов, О.А. Смірнов, Д.О. Даниленко // Інформаційна та економічна безпека: сучасний стан та тенденції розвитку : монографія за заг. ред. – Х.: ХІБС УБС НБУ – 2014 – С. 82-100.
3. Даниленко Д.О. Дослідження методів виявлення вторгнень в телекомунікаційні системи та мережі / Д.О. Даниленко, О.А. Смірнов, Є.В. Мелешко // Системи озброєння і військова техніка. – Випуск 1(29) – Х.: ХУПС – 2012. – С. 92-100.
4. Даниленко Д.А. Метод обнаружения вредоносного программного обеспечения. Часть 1. Корреляционный анализ сетевого трафика // А.А.Смирнов, Д.А. Даниленко, Е.В.Мелешко // Науково-технічний журнал «Інформаційно-керуючі системи на залізничному транспорті» – Випуск 4(95). – Х.: УкрДАЗТ – 2012. – С. 8-14.
5. Даниленко Д.А. Методы обнаружения вредоносного программного обеспечения в телекоммуникационных системах и сетях / Д.А. Даниленко // Збірник наукових праць "Системи обробки інформації". – Випуск 3(101) том 2. – Х.: ХУПС – 2012. – С. 152-155.

6. Даниленко Д.А. Системы обнаружения и предотвращения вторжений для защиты телекоммуникационных сетей от вредоносного программного обеспечения / Д.А. Даниленко, А.А. Смирнов, А.В. Коваленко // Системи управління, навігації та зв'язку. – Випуск 1 (21) том 2. – Київ: ДП «ЦНДІНУ». – 2012. – С. 183-186.
7. Даниленко Д.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.
8. Даниленко Д.О. 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.
9. Клименко Б.С. Дослідження та програмна реалізація системи реалізації DLP-агенту // Збірник праць молодих науковців ЦНТУ. – Вип. 11. – Кропивницький: ЦНТУ, 2021.
10. Даниленко Д.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.

УДК 004

М. Кобець, магістр гр. КІ-19М-1,4
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ НАЛАШТУВАННЯ, КОНФІГУРУВАННЯ ТА ВІДЛАГОДЖЕННЯ МЕРЕЖЕВОГО ОБЛАДНАННЯ НА БАЗІ ТЕХНОЛОГІЇ SOFTWARE-DEFINED ACCESS

У статті розроблено програмне забезпечення, яке призначено для налаштування, конфігурування та відлагодження мережевого обладнання на базі технології Software-Defined Access. Об'єктом дослідження є процес налаштування, конфігурування та відлагодження мережевого обладнання на базі технології Software-Defined Access. Предметом дослідження є методи налаштування, конфігурування та відлагодження мережевого обладнання на базі технології Software-Defined Access. Методи дослідження базуються на методах теорії телетрафіку, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи налаштування, конфігурування та відлагодження мережевого обладнання на базі технології Software-Defined Access. 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, Software-Defined Access

Постановка проблеми. Cisco представила новий підхід до побудови мереж і відповідні рішення, що дозволяють його реалізувати. Цей підхід дозволяє будувати інтуїтивні мережі, здатні самостійно навчатися, аналізуючи переданий трафік, і адаптуватися до змін, у тому числі відбивати атаки зловмисників. Це відповідь на нові вимоги до мережевих інфраструктур, висунуті у зв'язку із процесом цифрової трансформації, що набирає оберти, стрімким зростанням числа підключених пристроїв, у тому числі розумних речей (IoT), а також з новими погрозами безпеки. Cisco уперше в галузі представила рішення для програмно обумовленого доступу (Software-Defined Access, SD-Access). Технологія SD-Access дозволяє автоматизувати такі повсякденні рутинні операції, як налаштування,

конфігурування й налагодження мережевого устаткування, що кардинально скорочує час, необхідне для адаптації мережі до нових завдань, і строки усунення проблем (з декількох тижнів і місяців до декількох годин), а також істотно послабляє наслідки злому систем безпеки. Перші пилотні проекти, виконані поруч замовників, показали наступні результати використання нової технології: час конфігурування мережі скоротилося на 67%, а експлуатаційні витрати – на 61%. Ще однією вражаючою новою можливістю представлених Cisco рішень став аналіз зашифрованого трафіку (без його дешифрації) на предмет виявлення потенційних погроз. За даними, які приводять фахівці Cisco, біля половини кібератак сьогодні маскується в зашифрованому трафіку, і їхнє число постійно росте. Використовуючи для аналізу потоків даних інтелектуальні засоби Cisco Talos і машинне навчання, мережа здатна визначати сигнатури відомих атак навіть у зашифрованому трафіку, не розшифровуючи його й зберігаючи конфіденційність даних..

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи налаштування, конфігурування та відлагодження мережевого обладнання на базі технології Software-Defined Access.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи налаштування, конфігурування та відлагодження мережевого обладнання на базі технології Software-Defined Access.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

1. Огляд існуючих систем налаштування, конфігурування та відлагодження мережевого обладнання на базі технології Software-Defined Access.
2. Дослідження системи налаштування, конфігурування та відлагодження мережевого обладнання на базі технології Software-Defined Access.
3. Програмна реалізація системи налаштування, конфігурування та відлагодження мережевого обладнання на базі технології Software-Defined Access.

Об'єктом дослідження є процес налаштування, конфігурування та відлагодження мережевого обладнання на базі технології Software-Defined Access.

Предметом дослідження є методи налаштування, конфігурування та відлагодження мережевого обладнання на базі технології Software-Defined Access.

Методи дослідження базуються на методах теорії телетрафіку, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Основними елементами інтуїтивних мереж стануть нові комутатори Catalyst 9000 і централізована система керування DNA Center. Комутатори створені на основі нових високопродуктивних програмувальних інтегральних схем (IC) (ASIC) і мають убудований комплекс обчислювальних засобів на базі процесорів x86, які дозволяють виконувати різні застосунки, у тому числі контейнерні. Таким чином, вони можуть застосовуватися як вузли «прикордонних обчислень», здійснюючи обробку даних максимально близько до кінцевих пристроїв. Це особливо важливо для застосунків Інтернету речей, коли необхідно мінімальний час реакції, а затримки, пов'язані з передачею даних у центральний ЦОД, стають неприпустимими.

Саме на комутаторах Catalyst 9000 будуть виконуватися застосунки для аналізу зашифрованого трафіку. Також слід зазначити використовувану цими пристроями модульну мережеву ОС IOS XE з функцією hot patching, що дозволяє обновляти частина коду без заміни ОС цілком. Ця функція Cisco уже використовується на маршрутизаторах операторського класу, тепер вона стала доступна й у кампусних комутаторах Catalyst 9000. На цих пристроях можливе розміщення контролера бездротового зв'язку, у тому числі з підтримкою таких нових стандартів, як IEEE 802.11ax.

Система керування DNA Center охоплює процеси, пов'язані із проектуванням, конфігуруванням і забезпеченням виконання політик безпеки. Через неї реалізується максимально автоматизований процес налаштування, налагодження й адаптації до змін у

рамках технології SD-Access. Одержуючи від DNA Center контекстну інформацію про всю мережу, IT-фахівці можуть централізовано управляти всіма мережевими функціями. Крім того, DNA Center одержує з комутаторів різні телеметричні дані, що дозволяє прогнозувати подальший розвиток мережі й превентивно усувати потенційні проблеми.

Поставки комутаторів Catalyst 9000 і ПЗ керування DNA Center почнуться вже в червні-серпні поточного року. Трохи пізніше, під кінець року, стане доступна платформа Network Data Platform and Assurance. Ця аналітична система дозволить оперативно виконувати класифікацію й кореляцію більших обсягів переданих по мережі даних і за допомогою машинного навчання трансформувати їх у проактивну аналітику, бізнес-інформацію й оперативну інформацію, видаючи результати за допомогою сервісу DNA Center Assurance.

Cisco Catalyst 9000

Комутатори Cisco Catalyst 9000 відносяться до нової серії пристроїв від компанії Cisco, які орієнтовані на те, щоб одержати нові можливості при роботі в сучасному інформаційному середовищі. Запропоноване устаткування відрізняється оптимізованою апаратною платформою, що відрізняється гнучкою комутаційною конфігурацією. У нових пристроях розроблювачі основна увага приділили програмній частині комутаторів. Завдяки цьому рішенню вдалося одержати унікальні показники продуктивності й гнучкості робочої конфігурації.

Область застосування

Комутатори Cisco Catalyst 9000 відрізняються широким практичним застосуванням. Серед основних напрямків, для яких застосовується ця техніка слід зазначити:

- підтримка хмарних технологій;
- робота з віртуалізованими системами;
- підтримка технології Інтернету речей;
- робота з мобільними сервісами інформаційних послуг та інше.

Важливо відзначити, що забезпечуючи доступ до інформації при рішенні будь-яких завдань, пристрої серії Cisco Catalyst 9000 відрізняються високим рівнем безпеки оброблюваних даних.

Моделі комутаторів серії Cisco Catalyst 9000

У цій серії лінійка продукції від компанії Cisco представлена трьома комутаційними платформами.

- Catalyst 9300. Ці пристрої стануть оптимальним варіантом для підтримки Інтернету речей, вони відрізняються кращими у своєму класі показниками масштабованості. Платформа цих пристроїв може забезпечувати 384 комутаційних портів із загальною потужністю для UPOE до 60 Вт. Також комутаторами може підтримуватися PoE+, протоколи AVB і стандарти IEEE 1588.
- Catalyst 9400. Пристрої є модульними комутаторами, які створені для підтримки технології інтернету речей, а також для хмарних сервісів і забезпечення високого рівня безпеки переданої інформації. Ці комутаційні платформи здатні підтримувати швидкість обміну трафіком на рівні 8 ТБ/сек.
- Catalyst 9500. Це пристрої з 40Gb портами, які спеціально призначені для використання в структурі корпоративних мереж. Вони використовуються для підтримки інтернету речей, хмарних сервісів і підтримки безпеки потоків, що комутируються.

Комутатори Cisco Catalyst серії 9300

Комутатори Cisco Catalyst серії 9300 – це нове покоління самої популярної в галузі стекуємої платформи комутації. Ці мережеві комутатори створені для Інтернету речей, хмарних технологій, забезпечення безпеки і є основою нашої інноваційної архітектури рівня підприємства – Cisco SD-Access.

Створені для Інтернету речей

Ця серія комутаторів реалізує конвергенцію Інтернету речей з ведучим в індустрії

рівнем масштабованості. Комутатори забезпечують до 384 портів з потужністю до 60Вт для UPOE, а також POE+ і PoE, високу безпеку, підтримку протоколу AVB і стандарту IEEE 1588, аналіз сервісів і класифікацію для застосунків Інтернету речей.

Сумісні із хмарними інфраструктурами

Перетворите, спростите й захистите Вашу хмарну інфраструктуру. Cisco забезпечує готовий до хмарного середовища підхід, що охоплює всю мережу, від додатка в ЦОД до користувача на границі мережі.

Оптимізовані для мобільності

Комутатори Catalyst серії 9300 забезпечують інтелектуальний, простий і максимально безпечний доступ за допомогою інтегрованого контролера бездротової мережі. Вони можуть працювати в умовах високої щільності по стандарті 802.11ac другої хвилі (48 точок доступу) і при цьому відрізняються компактністю (форм-фактор 1 RU).

Послуги для проактивного керування мережами

Вирішуйте проблеми швидше, підвищуйте ефективність експлуатації й знижуйте ризик простою.

У серію Catalyst 9300 входять 18 моделей.

Мультигігабітні комутатори з 24 портами:

- 24 порту – 1 Гбіт, 2,5 Гбіт, 5 Гбіт, 10 Гбіт.
- Multigigabit Ethernet, 1 Гбіт SFP, 10 Гбіт SFP+.
- До 384 портів PoE, PoE+, Cisco UPOE потужністю 60 Вт.
- SD-Access, Cisco StackWise, контейнери.

Комутатори з 48 портами по 1 Гбіт:

- 48 портів 1 Гбіт SFP для даних, PoE+, Cisco UPOE.
- До 384 портів PoE, PoE+, Cisco UPOE потужністю 60 Вт.
- SD-Access, Cisco StackWise, контейнери.

Комутатори з 24 портами 1 Гбіт:

- 24 порту 1 Гбіт SFP для даних, PoE+, Cisco UPOE.
- До 384 портів PoE, PoE+, Cisco UPOE потужністю 60 Вт.
- SD-Access, Cisco StackWise, контейнери.

Комутатори Cisco Catalyst серії 9400

Комутатори Cisco Catalyst серії 9400 – це нове покоління самої популярної в галузі корпоративної платформи комутації. Ці модульні комутатори доступу спеціально розроблені для Інтернету речей, хмарних послуг і забезпечення безпеки. Вони надають найвищий ступінь надійності, підтримують швидкість передачі даних до 8 Тбіт/с і є ключовим елементом SD-Access, інноваційної архітектури Cisco для мереж рівня підприємства.

Захист на всьому протязі атаки

Унікальні можливості комутаторів Catalyst 9400 забезпечують захист вашої організації до, під час і після атаки. Зменшите можливу область атаки за допомогою надійних систем Cisco і шифрування MACSEC256. Удоскональте виявлення шкідливого ПЗ й стримування погроз.

Готові до Інтернету речей

Ця серія комутаторів забезпечує впровадження Інтернету речей з ведучим в індустрії рівнем масштабованості. Комутатори забезпечують до 384 портів з потужністю до 60Вт для UPOE, а також POE+ і PoE, високу безпеку, підтримку протоколу AVB і стандарту IEEE 1588, аналіз сервісів і класифікацію для застосунків Інтернету речей.

Готові до хмарного середовища

Перетворите, спростите й захистите Вашу хмарну інфраструктуру. Cisco забезпечує готовий до хмарного середовища підхід, що охоплює всю мережу, від додатка в ЦОД до користувача на границі мережі.

Унікальна надійність

Ці комутатори доступу забезпечують високу доступність на основі часткових

відновлень, технологію GIR для безпечної установки й видалення ПЗ й устаткування, використовують механізми NSF/SSO, а також використовують високоефективні резервуємі модулі вентиляторів і блоків живлення. Крім того, вони підтримують розширені можливості для маршрутизації й надання мережевих сервісів.

Послуги, що знижують ризик

Ми допоможемо вам знизити операційні ризики, поки ви плануєте й впроваджуєте перехід на наші послуги.

Catalyst 9410R:

- 384 порту, кожний слот – до 480 Гбіт/с.
- 1 Гбіт SFP, 10 Гбіт SFP+, Cisco UPOE і PoE+ потужністю до 60Вт.
- MPLS VPN 2 і 3 рівнів, MVPN, трансляція мережевих адрес (NAT).
- SD-Access, Cisco StackWise, резервування за типом N+N або N+1.

Catalyst 9407R:

- 240 портів, кожний слот – 480 Гбіт/с.
- 1 Гбіт SFP, 10 Гбіт SFP+, Cisco UPOE і PoE+ потужністю до 60Вт.
- MPLS VPN 2 і 3 рівнів, MVPN, трансляція мережевих адрес (NAT).
- SD-Access, Cisco StackWise, резервування за типом N+N або N+1.

Комутатори Cisco Catalyst серії 9500

Серія Catalyst 9500 – це перші 40-гігабітні комутатори, розроблені спеціально для корпоративної мережі. Комутатори Cisco Catalyst серії 9500 створені для Інтернету речей, хмарних технологій і забезпечення безпеки і є новим поколінням найпоширенішої платформи комутації. Комутатори Catalyst 9500 у ролі фіксованого ядра є ключовим елементом SD-Access, інноваційної архітектури Cisco рівня підприємства.

Захист на всьому протязі атаки

Унікальні можливості комутаторів Catalyst 9500 забезпечують захист вашої організації до, під час і після атаки. Зменшіть можливу область атаки за допомогою надійних систем Cisco і шифрування MACSEC256. Удоскональте виявлення шкідливого ПЗ й стримування погроз.

Готові до Інтернету речей

Ця серія комутаторів забезпечує впровадження Інтернету речей з ведучим в індустрії рівнем масштабованості. Комутатори забезпечують до 384 портів з потужністю до 60Вт для UPOE, а також POE+ і PoE, високу безпеку, підтримку протоколу AVB і стандарту IEEE 1588, аналіз сервісів і класифікацію для застосунків Інтернету речей.

Готові до хмарного середовища

Перетворите, спростите й захистите Вашу хмарну інфраструктуру. Cisco забезпечує готовий до хмарного середовища підхід, що охоплює всю мережу, від додатка в ЦОД до користувача на границі мережі.

Основна технологія

Ці комутатори доступу забезпечують високу доступність на основі часткових відновлень, технологію GIR для безпечної установки й видалення ПЗ й устаткування, використовують механізми NSF/SSO, а також використовують високоефективні резервуємі модулі вентиляторів і блоків живлення. Крім того, вони підтримують розширені можливості для маршрутизації й надання мережевих сервісів.

Послуги оптимізації бізнес-архітектури

Управляйте своєю мережею з розумом і використовуйте максимум її можливостей, аналізуючи продуктивність, показники, якість впровадження й виникаючі інциденти.

Catalyst 9500-24Q-A7:

- 4-ядерний ЦП 2,4 ГГц x86.
- 16 Гбайт оперативної пам'яті DDR4, убудована пам'ять 16 Гбайт.
- MPLS VPN 2 і 3 рівнів, MVPN, трансляція мережевих адрес (NAT).

- SD-Access, StackWise, висока доступність.
- Передплата на технічну підтримку високого рівня – 7 років.

Catalyst 9500-24Q-A:

- 4-ядерний ЦП 2,4 ГГц x86.
- 16 Гбайт оперативної пам'яті DDR4, убудована пам'ять 16 Гбайт.
- MPLS VPN 2 і 3 рівнів, MVPN, трансляція мережевих адрес (NAT).
- SD-Access, StackWise, висока доступність.
- Передплата на технічну підтримку високого рівня – 5 років.

Catalyst 9500-24Q-A3:

- 4-ядерний ЦП 2,4 ГГц x86.
- 16 Гбайт оперативної пам'яті DDR4, убудована пам'ять 16 Гбайт.
- MPLS VPN 2 і 3 рівнів, MVPN, трансляція мережевих адрес (NAT).
- SD-Access, StackWise, висока доступність.
- Передплата на технічну підтримку високого рівня – 3 роки.

Catalyst 9500-24Q-E:

- 4-ядерний ЦП 2,4 ГГц x86.
- 16 Гбайт оперативної пам'яті DDR4, убудована пам'ять 16 Гбайт.
- MPLS VPN 2 і 3 рівнів, MVPN, трансляція мережевих адрес (NAT).
- StackWise, висока доступність.
- Передплата на базову технічну підтримку – 5 років.

Розробка структурної схеми

Корпоративна служба IT перебуває «між молотом і ковадлом». З одного боку, бізнес вимагає забезпечити високу доступність мережі й очікує, що мережа повинна працювати завжди – у режимі 24x7, без виключень. Це очевидно. В IT важко знайти те, що турбує бізнес більше, ніж неприступність бізнес-процесів. Але ж з розвитком цифрових технологій залежність бізнес-процесів від мережі тільки росте.

З іншого боку, користувачі (а по суті, той же бізнес) вимагають підтримку нових сервісів, нових типів пристроїв, нових типів користувачів (у тому числі гостей, партнерів) і т.д. Усім їм потрібно забезпечити належну підтримку з боку мережі, причому швидко. Крім того, необхідно врахувати й вимоги служби ІБ.

Але вимоги впровадження нових сервісів і забезпечення високої доступності, як правило, суперечать один одному. Адже висока доступність припускає насамперед стабільність мережі, що відомо як зі спеціалізованої літератури (наприклад Piedad, Floyd, and Michael Hawkins. High availability: design, techniques, and processes. Upper Saddle River, N.J: Prentice Hall PTR, 2001. Print), так і із загальних принципів, наприклад KISS (Keep it Simple Stupid), «працює – не займай! і т.п.

А впровадження нових сервісів мережі по визначенню порушує її стабільність, тому що привносить у мережу щось нове, вимагає внесення змін. Ці зміни нерідко виявляються складне й великими – наприклад, впровадження рішень для спільної мультимедійної роботи й механізмів QoS, технологій безпеки й сегментації. Навіть рішення «транспортних» завдань може виявитися непростим, наприклад забезпечення зв’язності на Рівні 2 між точками А и Б у різних частинах кампусної мережі.

У результаті впровадження сервісів ускладнює мережа й вимагає багато часу, а іноді взагалі відбувається не в повному обсязі.

Є й інша сторона протиріччя між забезпеченням високої доступності й рішенням повсякденних бізнес-завдань. Бізнес-завдання звичайно жадають від мережі не просто передачу пакетів із точки А в точку Б, а реалізацію різного роду політик. Політики транслюються в конкретні вимоги, наприклад – як забезпечити безпека, по яких шляхах направити трафік різних застосунків, як його обробляти й т.п. Будь-яка нетривіальна політика підвищує складність впровадження й експлуатації мережі.

Крім того, політики недостатньо впровадити. Необхідно також підтримувати їх в актуальному стані, вносити в них зміни. Подібні зміни в масштабах корпоративної мережі, особливо виконувані вручну – як правило, ресурсномісткі, довгі й досить уразливі до помилок. У результаті доступність мережі знову має тенденцію до зниження, а операційні витрати – до підвищення.

Таким чином, у типовий, «класичної» корпоративної мережі:

– вимоги підвищення доступності й впровадження сервісів суперечать один одному;

– реалізація політик утруднений;

– завдання впровадження політик і підтримки їх в актуальному стані заважають забезпечити високу доступність мережі.

Із цими труднощами служби IT зіштовхуються повсюдно. Але бізнес не цікавлять труднощі IT. Бізнес цікавить, щоб бізнес-процеси працювали надійно, а впроваджувалися – швидко.

Мережева фабрика: сполучаючи що не сполучиться

Як же вирішити ці суперечні один одному складні завдання, що коштують перед IT? Добре, що зарекомендував сЪебе, спосіб рішення складних завдань – розбити одне завдання на трохи більше простих, а далі вирішувати вже їх. Широко відомі приклади – семирівнева модель OSI або чотирьохрівнева модель DoS у рішенні завдання мережевої взаємодії.

У нашім випадку на допомогу приходить концепція мережевої фабрики, або оверлея (overlay). Оверлей – це логічна топологія, побудована поверх деякої нижчележачої топології (underlay), опорної мережі. Оверлей використовує який-небудь вид інкапсуляції трафіку для передачі поверх опорний мережі. Поняття оверлея добре знайомо мережевим адміністраторам. Прокладаючи будь-який тунель у мережі, адміністратор створює оверлей. Типові приклади – IPSec, GRE, CAPWAP, VXLAN, OTV і т.д.

Чому ж мережева фабрика допомагає перебороти вищезгадані труднощі, які не виходить вирішити в «класичній мережі»?

В «класичній мережі» ці труднощі не вирішуються із принципової причини – тому що суперечливі вимоги пред'являються до тому самому об'єкта.

У випадку ж мережевої фабрики об'єкт, до якого пред'являються вимоги, розділяється на два. Одна мережева топологія розділяється на дві.

Перша, нижчележача топологія забезпечує надійний транспорт на основі маршрутизуємої мережі. Це її єдине завдання. Вона не реалізує сервіси й політики – вона не призначена для цього.

Завдання реалізації сервісів і політик вирішує друга, оверлейна мережева топологія. Вона відділена від нижчележачої топології, як, наприклад, відділений друг від друга протоколи різних рівнів моделі OSI.

Поява двох мережевих топологій і дає розв'язку суперечних один одному вимог. У цьому й полягає принципова різниця між «класичною мережею» і мережевою фабрикою. Саме це й дозволяє мережевій фабриці перебороти труднощі, з якими не може впоратися «класична мережа».

Що таке Cisco SD-Access?

Реалізації концепції мережевої фабрики вже є в багатьох корпоративних мережах. Наприклад, ідея фабрики на основі тунелів CAPWAP давно реалізована в централізованій архітектурі корпоративних бездротових ЛОМ. Інший приклад – фабрика в мережах ЦОД у рішенні Cisco Application Centric Infrastructure (ACI). Фабрики одержують поширення й у територіально-розподілених мережах у вигляді технологій SD-WAN, зокрема, Cisco IWAN.

Наступає час для появи мережевої фабрики й у кампусних мережах (див. рисунок 1).

Cisco Software-Defined Access (SD-Access) – це реалізація Cisco концепції мережевої фабрики для кампусної мережі із централізованими засобами керування, автоматизації й оркестрації, а також моніторингу й аналітики.

Ці засоби надає контролер DNA Center – ключовий компонент рішення. DNA Center забезпечує веб-інтерфейс адміністратора й інтерфейси API. Крім того, DNA Center реалізує сервіси аналітики, одержуючи й аналізуючи службову інформацію й телеметрію від пристроїв фабрики. DNA Center вирішує завдання перетворення маси розрізнених даних у конкретні виводи й практичні рекомендації. Такі виводи й рекомендації стосуються поточного стану мережі, її сервісів і застосунків, що течуть інцидентів. На підставі аналізу даних з урахуванням знання контексту DNA Center надає аналітику про ймовірний вплив інцидентів на сервіси мережі, рекомендує конкретні міри для усунення інцидентів, аналізує тренди, дає рекомендації із планування ємності мережі. Це дуже важливий функціонал для моніторингу, швидкого пошуку й усунення несправностей. В остаточному підсумку він допомагає забезпечити високу доступність бізнес-процесів, що працюють поверх фабрики.

DNA Center працює разом із сервером контролю доступу Identity Service Engine (ISE). ISE надає фабриці сервіси автентифікації, авторизації й контролю доступу (AAA), забезпечує динамічне приміщення користувачів фабрики в групи й засоби керування політиками взаємодії між групами. ISE необхідний для реалізації у фабриці політики безпеки організації.

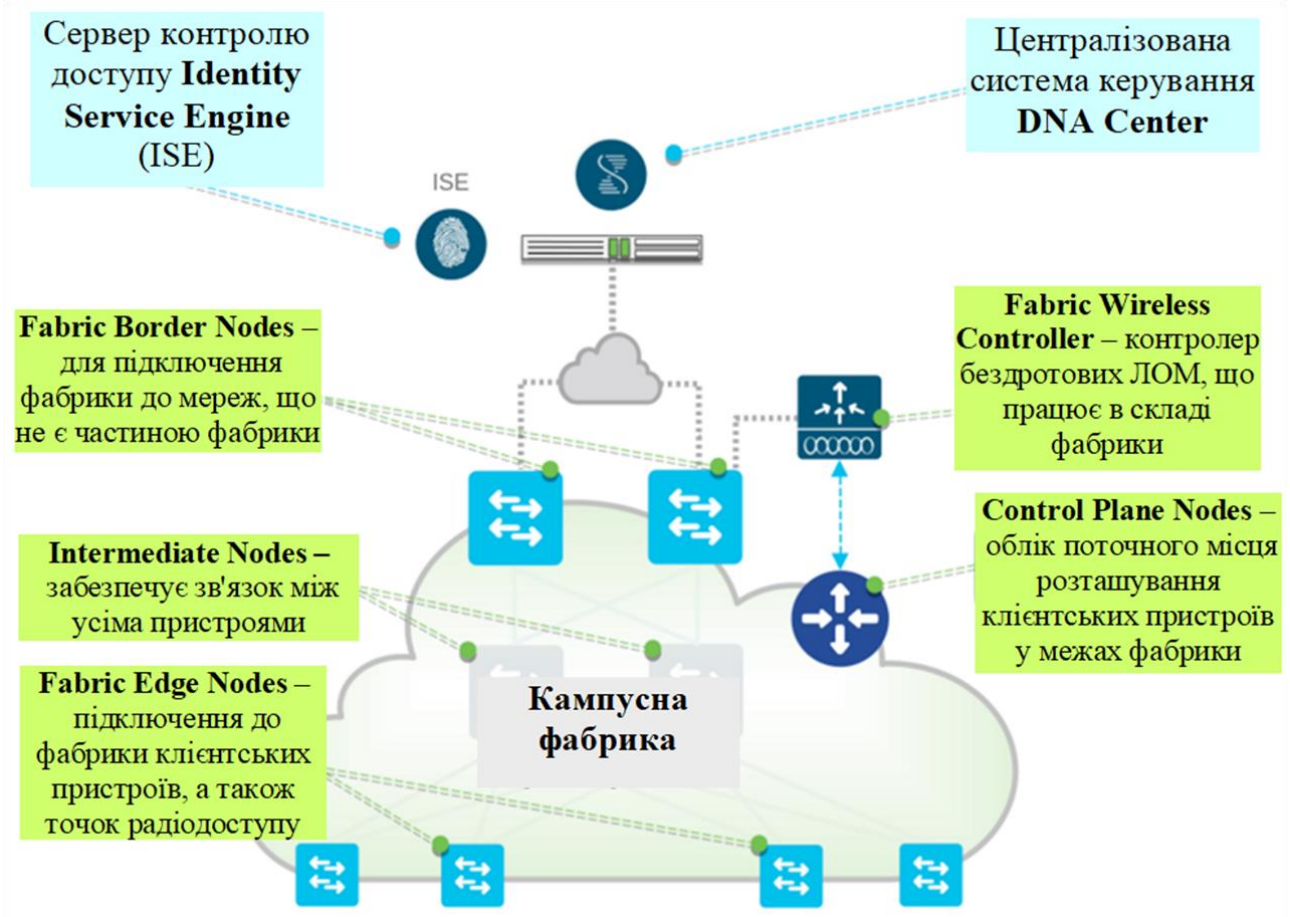


Рисунок 1 – Структурна схема мережі

З погляду мережевої інфраструктури фабрика складається із пристроїв, що виконують наступні ключові ролі:

– Control Plane Nodes ведуть облік поточного місця розташування клієнтських пристроїв у межах фабрики. Це необхідно для вільного переміщення користувачів у межах фабрики зі збереженням призначених користувачеві політик і забезпечення їхньої мобільності.

– Fabric Border Nodes необхідні для підключення фабрики до зовнішнього світу, тобто до мереж, що не є частиною фабрики. Наприклад, це можуть бути мережа ЦОД і інші частини корпоративної мережі, побудовані не на основі фабрики SD-Access, Інтернет і т.д.

Fabric Edge Nodes забезпечують підключення до фабрики клієнтських пристроїв, а також точок радіодоступу.

Fabric Wireless Controller являє собою контролер бездротових ЛОМ, що працює в складі фабрики.

Intermediate Nodes забезпечують зв'язок між перерахованими вище пристроями. Вони не виконують ніяких функцій оверлея, а тільки реалізують опорну, нижчележачу мережеву топологію.

З погляду технологій, data plane фабрики Cisco SD-Access реалізований на базі інкапсуляції Virtual Extensible LAN (VXLAN). Control plane оверлея використовує протокол Locator/ID Separation Protocol (LISP). Політики реалізуються на базі тегів Scalable Group Tag (SGT) технології Cisco TrustSec. Нарешті, оверлей працює поверх маршрутизуємої опорної мережі. Розглянемо ці технології докладніше.

Data plane оверлея: VXLAN

Data plane фабрики Cisco SD-Access побудований на базі інкапсуляції VXLAN з Group Policy Option(VXLAN-GPO). Важлива перевага VXLAN полягає в збереженні первісного Ethernet-Заголовка фрейму. У результаті забезпечується мобільність хостів фабрики не тільки на Рівні 3, але й на Рівні 2. Це дає гнучкий і універсальний транспорт. Які б не були вимоги застосунків, фабрика здатна надати їм будь-який вид транспорту – Рівнів 3 і 2 – незалежно від напрямку взаємодії хостів і їхнього розташування у фабриці.

Трафік data plane фабрики (фрейми Рівня 2) інкапсулюється в пакети VXLAN і відправляється по мережі поверх UDP і IP. З погляду проміжних пристроїв фабрики, це стандартні пакети IP із вкладеними сегментами UDP, адресованими на порт 4789. Номер source-порту UDP визначається гешем заголовків Рівнів 2, 3 і 4 вихідних пакетів і, таким чином, міняється динамічно. Це важливо для належного розподілу навантаження технологією Cisco Express Forwarding (CEF) в опорній мережі. При розподілі навантаження метод full технології CEF використовує значення геш-функції від адрес IP і портів транспортного рівня для вибору конкретного каналу зв'язку. Тому змінне значення source-портів UDP приводить до розподілу навантаження між різними каналами зв'язку навіть без застосування додаткових способів боротьби з поляризацією CEF.

VXLAN-тунелі не вимагають попереднього встановлення з'єднання, тобто є stateless тунелями.

Оверлей приводить до появи додаткових заголовків через використання опорної мережі (underlay) для транспорту. Це 8-байтний заголовок VXLAN, 8-байтний заголовок UDP, 20-байтний заголовок IP і 14-байтний заголовок MAC (з опціональними додатковими 4 байтами) – разом від 50 до 54 байт.

Інкапсуляцію трафіку в пакети VXLAN і назад у рішенні Cisco SD-Access виконують прикордонні пристрої фабрики. Для трафіку зовнішніх мереж це Fabric Border Nodes, для трафіку провідних клієнтів – Fabric Edge Nodes.

SD-Access також забезпечує інтеграцію бездротових мереж у фабрику. Такий режим роботи називається Fabric Enabled Wireless (FEW). На відміну від централізованої архітектури БЛОМ, у режимі FEW трафік користувачів БЛОМ тунелюється не на контролер БЛОМ у пакетах CAPWAP, а на комутатор доступу Edge Node у пакетах VXLAN. Таким чином, трафік і провідних, і бездротових клієнтів надходить безпосередньо на комутатори Edge Node.

У результаті забезпечується однакова обробка трафіку провідних і бездротових користувачів, оптимізація шляхів передачі трафіку БЛОМ, усунення потенційних «вузьких місць», характерних для стику контролера БЛОМ і провідної мережі.

Control & management plane бездротової ЛОМ у режимі FEW залишається централізованим на контролері Fabric Wireless. Контролер використовує протокол LISP для обміну даними з Control Plane Nodes про поточне місце розташування бездротових клієнтів у фабриці. Точки радіодоступу взаємодіють із контролером за протоколом CAPWAP.

Таким чином, архітектура бездротової мережі при інтеграції у фабрику одержує «краще із двох світів».

Control plane оверлея: LISP

Мобільність хостів на Рівнях 2 і 3 – невід'ємна властивість фабрики. З погляду data plane мобільність забезпечується технологією VXLAN, а в якості control plane використовується протокол Locator/ID Separation Protocol (LISP).

Щоб забезпечити можливість переміщення хостів у межах фабрики без зміни адрес, фабриці необхідно відслідковувати місце розташування кожного окремо взятого хосту. При рішенні цього завдання з використанням традиційних протоколів маршрутизації потрібна була б робота з host specific маршрутами із префіксами /32 або /128 (для IPv4 і IPv6 відповідно). Вимога роботи з host specific маршрутами по визначенню виключає агрегацію маршрутів, що привело б до підвищеної витрати пам'яті комутаторів фабрики. Крім того, кожне переміщення хосту між комутаторами фабрики породжувало б апдейт протоколу маршрутизації, створюючи додаткове навантаження на CPU всіх комутаторів незалежно від того, чи потрібний на даному комутаторі цей чи маршрут ні.

У результаті реалізація мобільності хостів приводила б до високих вимог до ресурсів control plane. І ці вимоги стосувалися б прикордонних комутаторів фабрики – комутаторів доступу, у яких, як правило, немає потужного control plane.

Для рішення цієї проблеми фабрика Cisco SD-Access використовує протокол LISP. Це дуже ефективний протокол, оптимізований для мобільності хостів. Фабрика містить централізовану базу даних користувачів Host Tracking Database (HTDB), що працює на пристроях ролі Control Plane Nodes. HTDB зберігає інформацію про відповідність клієнтського хосту (Endpoint ID) поточному місцю розташування в межах фабрики, а також ряд додаткових атрибутів.

Прикордонні пристрої фабрики, використовуючи протокол LISP, запитують базу HTDB, коли їм потрібно передати пакет на клієнтський хост із невідомим місцем розташування, і зберігають цю інформацію в локальному кеше.

Інформація надходить у базу від прикордонних пристроїв фабрики в міру підключення й переміщення клієнтських хостів.

Таким чином, Cisco SD-Access дозволяє хостам вільно переміщатися в межах фабрики без зміни адрес, забезпечує їхня мобільність.

Політики контролю доступу й сегментація: TrustSec

Фабрика пропонує гнучкі й масштабовані засоби для реалізації політик контролю доступу до ресурсів, а також сегментації й мікросегментації користувачів.

Історично для рішення завдання контролю доступу застосовувалися списки контролю доступу (ACL), засновані на IP-адресах. Відбувалося це тому, що заголовок IP-пакета не містить ніяких інших даних, які могли б використовуватися для встановлення логічного зв'язку між IP-пакетом і користувачем.

Подібне рішення вимагає широкомасштабного впровадження ACL у багатьох місцях мережі, а також підтримки їх в актуальному стані, внесення змін. А можливих причин для таких змін багато – наприклад, нові вимоги політики безпеки, зміни в складі користувачів, ресурсів, топології мережі, мобільність користувачів у провідних і бездротових мережах. Тому такий підхід вимагає значних витрат часу й сил обслуговуючого персоналу. Крім того, він досить уразливий до помилок. У результаті страждають безпека й масштабованість мережі, швидкість реакції IT на потребі бізнесу, доступність бізнес-процесів.

Сегментація користувачів довгий час реалізовувалася за допомогою віртуальних топологій, що збираються з VLAN'ов, VRF'ов, MPLS VPN'ов, тунелів і інших подібних засобів. Такий підхід також досить ресурсномісткий і працює тим гірше, чим більше динаміки в середовищі сегментації й чим гранулярніше така сегментація потрібна.

Тому віртуальні топології особливо погано підходять для мікросегментації користувачів, але ж саме вона потрібно всі частіше у зв'язку із цифровізацією сучасного

бізнесу й еволюцією погроз безпеки (у тому числі масового поширення мережевих хробаків-шифрувальників).

Для рішення завдань контролю доступу й сегментації користувачів Cisco розробила технологію TrustSec. TrustSec використовує мітку Scalable Group Tag (SGT) замість IP-адреси як критерій приналежності пакета тій або іншій групі користувачів. Такий підхід дозволяє відокремити адресацію від контролю доступу, використовувати спеціалізовані списки контролю доступу SGACL для реалізації політик контролю доступу, додати мережі гнучкість і автоматизацію застосування політик безпеки.

Базовий метод передачі міток усередині домену TrustSec (метод inline) полягає в інкапсуляції міток у заголовки фреймів або пакетів трафіку (у полі Cisco Meta Data). А у фабриці Cisco SD-Access значення мітки передається в складі заголовків VXLAN оверлея. Заголовок VXLAN містить поля VN ID і Segment ID (24- і 16-розрядні відповідно). Ці поля використовуються для переносу інформації про приналежність пакета певної віртуальної мережі VN (адресується понад 16 млн. VRF) і групі SGT технології TrustSec (адресується понад 64 тис. мітки). Таким чином, TrustSec споконвічно є невід'ємним функціоналом фабрики. Крім того, інкапсуляція мітки SGT у заголовок VXLAN полегшує впровадження TrustSec – адже від проміжних пристроїв опорної мережі не потрібна робота з мітками.

Фабрика Cisco SD-Access дозволяє реалізувати два рівні сегментації користувачів: VRF для грубої сегментації на високому рівні (наприклад, для поділу організацій або їхніх підрозділів) і групи SGT для тонкої сегментації (наприклад, на рівні від організації до невеликих робочих груп). У першому релізі фабрики SD-Access SGT унікальні в межах VN, але в принципі можливі й так звані VN-Agnostic групи, що є присутнім у різних VN, тому що SGT не залежить ні від IP-адрес, ні від VRF.

Окремого роз'яснення заслуговує й сам термін SGT. Він з'явився в процесі розробки технології TrustSec і споконвічно звався Source Group Tag. Зусиллями маркетологів згодом термін став означати Security Group Tag. У випадку TrustSec це було виправдано, адже SGT використовувалися для реалізації політик безпеки. І все-таки, SGT – це всього лише мітка, число, що дозволяє розрізняти пакети. І це число підходить для реалізації будь-яких політик, не тільки безпеки, що й робиться в Cisco SD-Access. У підсумку SGT тепер означає Scalable Group Tag.

Контроль доступу, налаштування й впровадження політик доступу виробляється на сервері Cisco ISE, інтегрованому в рішення Cisco SD-Access. У результаті SD-Access пропонує готові автоматизовані засоби реалізації політики контролю доступу організації, а також сегментації й мікросегментації користувачів.

Опорна мережа

Головне завдання опорної мережі з погляду фабрики – забезпечити передачу трафіку оверлея. Для оверлея опорна мережа прозора. Тому як опорна мережа може підійти будь-яка сучасна корпоративна мережа, що забезпечує адекватний рівень доступності й продуктивності. Вона повинна надати прикордонним пристроям фабрики, таким як Fabric Edge Node, Border Node, Control Plane Node, зв'язок за протоколом IP.

У загальному випадку опорна мережа може бути побудована на базі будь-якого сполучення технологій Рівнів 2 і 3, хоча Cisco рекомендує будувати повністю маршрутизуєму мережа (з маршрутизацією до комутаторів доступу) і каналами зв'язку, що мають конфігурацію point-to-point. Протокол маршрутизації теж може бути кожним, рекомендований варіант – IS-IS, що став стандартом де-факто в опорних мережах фабрик завдяки своїй незалежності від адрес Рівня 3, швидкій збіжності й наявності параметрів TLV.

У зв'язку з інкапсуляцією VXLAN оверлея Cisco рекомендує забезпечити передачу в опорній мережі jumbo-фреймів зі значенням MTU не менш 9,100 байт. Затримки передачі пакетів (RTT) усередині фабрики повинні не перевищувати 100 мс.

Як устаткування опорної мережі походить будь-яке устаткування, що відповідає цим вимогам, як від Cisco, так і від інших виробників. Можна використовувати вже наявну корпоративну мережу. Це забезпечує захист інвестицій в устаткування існуючої мережі,

навіть якщо воно не підтримується фабрикою. У цьому випадку опорна мережа буде являти собою Manual Underlay, тобто управлятися автономно від фабрики.

Також є можливість автоматизації керування опорної мережі за допомогою інструментарію фабрики у випадку використання відповідного устаткування Cisco (рішення Cisco SD-Access 1.0 забезпечує автоматизацію опорної мережі, побудованої на базі комутаторів Catalyst серій 3850/3650 і 9000). Це сценарій Automated Underlay. У цьому випадку провіженінг опорної мережі буде виконуватися функціоналом DNA Center. Контролер завантажить на пристрої опорної мережі попередньо протестовані конфігурації, побудовані на базі рекомендацій Cisco Validated Design. Ручне редагування конфігурацій пристроїв у режимі Automated Underlay на момент написання статті не допускається, але така можливість передбачається в майбутньому.

Крім захисту інвестицій, гнучкість вимог SD-Access до опорної мережі полегшує впровадження – можна почати з пілотного проекту, створення невеликої фабрики, що використовує як транспорт існуючу опорну мережу, і поступово провести міграцію на повномасштабне рішення.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів налаштування, конфігурування та відлагодження мережевого обладнання на базі технології Software-Defined Access. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем налаштування, конфігурування та відлагодження мережевого обладнання на базі технології Software-Defined Access; Досліджена система налаштування, конфігурування та відлагодження мережевого обладнання на базі технології Software-Defined Access; На основі отриманих результатів досліджень створена програмна реалізація системи налаштування, конфігурування та відлагодження мережевого обладнання на базі технології Software-Defined Access. Розроблені під час виконання роботи алгоритми дозволяють успішно вирішувати завдання налаштування, конфігурування та відлагодження мережевого обладнання на базі технології Software-Defined Access. 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. 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. 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

УДК 004

М. Крамський, магістр гр. КН-19М-1,4
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ SOFTWARE DEFINED STORAGE

У статті розроблено програмне забезпечення, яке призначено для системи Software Defined Storage. Метою розробки є дослідження та програмна реалізація системи Software Defined Storage. Об’єктом дослідження є процес Software Defined Storage. Предметом дослідження є методи Software Defined Storage. Методи дослідження базуються на методах зберігання даних, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи Software Defined Storage.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, Software Defined Storage

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 встаткування. 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. Так, по оцінці Markets and Markets, в 2018 році обсяг ринку програмно обумовлених систем зберігання склав 4,72

млрд доларів, а до 2021-му він виросте до 22,56 млрд доларів, тобто щорічний ріст складе 36,7%.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи Software Defined Storage.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи Software Defined Storage.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

- Огляд існуючих систем Software Defined Storage.
- Дослідження системи Software Defined Storage.
- Програмна реалізація системи Software Defined Storage.

Об'єктом дослідження є процес Software Defined Storage.

Предметом дослідження є методи Software Defined Storage.

Методи дослідження базуються на методах зберігання даних, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. У великих організаціях системи зберігання даних займають значну частку вартості IT-інфраструктури (по оцінках фахівців – до 25%). Ця цифра може істотно вирости. Причини – ріст обсягу даних і збільшення потреби в ємностях систем зберігання даних (СЗД), у тому числі через закони, які зобов'язують ці дані зберігати. У той же час компанії активно намагаються заощаджувати IT-бюджети, що змушує їх перебувати в постійному пошуку найбільш вигідних технологічних рішень, які б дозволили скоротити ці витрати не на шкоду якості сервісу. Це ж ставиться до зберігання й обробки даних.

Вимоги замовників до зниження вартості володіння IT-інфраструктурою змушують постачальників інвестувати в розробки й пропонувати нові технології. Одна з них – програмно-визначаємі системи зберігання даних (Software-Defined Storage, SDS). Компанії починають замислюватися про впровадження SDS, коли процедури роботи з даними стають неефективними і їхній пошук забирає багато часу.

Концепція SDS дозволяє одержати такі переваги, як:

- абстрагування від нижнього рівня (апаратної платформи);
- масштабованість;
- спрощена інфраструктура зберігання;
- низька вартість рішень.

Завдяки технологіям SDS можна значно знизити вартість СЗД і їхнього адміністрування. За прогнозами Gartner, до 2020 року 70–80% неструктурованих даних будуть зберігатися на недорогих системах, керованих за допомогою SDS, а вже до 2021 року 70% існуючих масивів зберігання стануть доступні в повністю програмній версії.

Коли й навіщо потрібна SDS

ПЗ керування СЗД повинне забезпечувати гнучку організацію зберігання даних, а також:

- дедуплікацію;
- реплікацію даних;
- динамічне виділення ємності;
- знімки даних;
- дотримання політик зберігання.

SDS визначають в Storage Networking Industry Association (SNIA, Асоціація виробників і споживачів систем зберігання) як віртуалізоване середовище зберігання даних з інтерфейсом керування сервісами, що повинна містити в собі:

- автоматизацію – спрощене керування, що знижує витрати на обслуговування інфраструктури зберігання даних;

– стандартні інтерфейси – API для керування, виділення й звільнення ресурсів, обслуговування сервісів і пристроїв зберігання;

– віртуалізацію шляхів доступу до даних – блоковий, об'єктний і файловий доступ відповідно до інтерфейсів застосунків;

– масштабованість – зміна інфраструктури зберігання без зниження необхідного рівня доступності або продуктивності;

– прозорість – моніторинг споживаних ресурсів зберігання, керування ними й контроль їхньої вартості.

Відзначу, що для SDS потрібний стандартизований інтерфейс керування – такий, як SNIA Storage Management Initiative Specification (SMI-S). Він є складовою частиною концепції програмно-визначаємих дата-центрів (SDDC). Ця програмна логіка хмарної інфраструктури зберігання й хмарних апаратних платформ може бути елементом і традиційних ЦОД. Сервіси зберігання й обробки даних можуть виконуватися на серверах, спеціалізованих пристроях зберігання (storage appliance) або на обох цих платформах, усуваючи традиційні границі.

Software-Defined Storage пропонують багато хто вендори:

–Dell EMC (рішення Dell Nexenta, EMC ScaleIO);

–HPE (рішення StoreVirtual VSA);

–IBM (рішення Spectrum Storage);

–NetApp (рішення ONTAP Select);

–VMware (рішення vSAN);

–Red Hat (рішення Red Hat Storage);

–StoneFly (рішення SCVM, SDUS);

–DataCore (рішення SANsymphony);

–SwiftStack;

–Pivot3 і ін.

Уточню, що рішення RedHat Storage представлене двома продуктами: RedHat Ceph Storage і RedHat Gluster Storage (RH Storage Server). Тут вони маються на увазі обоє, але в наведеному нижче порівнянні вони не брали участь, тому що значно відрізняються від інших згаданих рішень.

Ceph – не зовсім коробковий продукт. Його використання без штату розроблювачів досить важко, що зробило його нецікавим для нашої компанії. Тому цього рішення немає в порівняльній таблиці.

Умовно всі SDS-рішення можна розділити на три категорії:

– класичні (CEPH, Red Hat Storage Server, EMC ScaleIO);

– на основі традиційних систем зберігання (NetApp ONTAP Select, HPE StoreVirtual VSA);

– у складі обчислювальних комплексів (VMware vSAN).

Деякі виробники пропонують як комплексні рішення, так і програмну частину (Huawei, Dell EMC). Це дозволяє гнучко підходити до підбору продуктів і використовувати успадковане «обчислювальне» устаткування для рішення менш ресурсномістких завдань зберігання даних. Ще однією заслугою SDS стала можливість застосування в деяких класичних СЗД віртуалізації дискових масивів.

Рішення архітектурно будуються по двох принципах:

– слабко зв'язані;

– розподілені (без загальних елементів).

У першому випадку відказостійкість забезпечується за рахунок розподілених копій даних, але через надмірність комунікацій між вузлами (нодами) знижується швидкість запису. Критичним місцем є мережа передачі даних, тому такі рішення звичайно реалізовані на основі InfiniBand. По такому принципі побудовані рішення VMware vSAN, HPE StoreVirtual VSA, Dell EMC ScaleIO.

У системах без загальних елементів дані записуються на один вузол, а потім із заданою періодичністю копіюються на інші для забезпечення відказостійкості. При цьому записи не є транзакційними. Такий підхід найбільш дешевий. Найчастіше в якості інтерконекта в ньому використовується Ethernet. Дана архітектура зручна з погляду масштабованості. Яскравий її представник – CEPH.

Зараз багато компаній займаються розробкою як програмної SDS (наприклад, Atlantis Computing, Maxta, StarWind, DataCore Software, Sanbolic, Nexenta, CloudByte), так і випуском комплексних рішень (Dell EMC, IBM) або спеціалізованих пристроїв (Tintri, Nimble, Solidfire).

Розробка структурної схеми

По даним Gartner, в 2021 році близько 50% наявних систем зберігання даних стануть доступні у вигляді програмних аналогів (зараз тільки 15%). Крім того, в 2021 році близько 30% СЗД, застосовуваних у великих ЦОДах, будуть програмними (зараз 5%). Нарешті, в 2020 році близько 70% функцій по наданню сховищ і керуванню ними виявляться інтегровані в єдину програмну платформу підприємства (у цей час – 10%).

Тенденція абстрагування ПЗ від нижчележащого встаткування дає шанс розроблювачам запропонувати передові рішення й вийти на перспективний ринок, не маючи ресурси західних компаній. І вони намагаються цей шанс використовувати: цілий ряд вітчизняних компаній займаються розробками в області програмно обумовлених мереж і систем зберігання.

По своїй функціональності програмне забезпечення, що розробляється в даній роботі, не уступає закордонним конкурентам, а в багатьох випадках їх перевершує. П'ять-Десять років тому все остерігалися використовувати програмні СЗД, але зараз вони не уступають апаратним платформам ні по функціональності, ні по надійності. Як і інше програмні СЗД, програмне забезпечення, що розробляється в даній роботі, може бути встановлене на будь-яке встаткування x86, а компоненти можна використовувати стандартні, доступні на ринку: сервери x86 і диски оригінальних виробників.

Оскільки замовники усе ще консервативні й поки не готові відмовлятися від переваг, які дає покупка готового рішення в порівнянні із самостійною установкою програмного забезпечення на сервери, продукт поставляється й у вигляді апаратного комплексу. При виникненні яких-небудь збоїв замовники не хочуть з'ясовувати, хто винуватий – постачальник ПЗ або встаткування, а купуючи апаратно-програмний комплекс, вони одержують протестоване рішення, за надійну роботу якого повністю відповідає постачальник.

Одне з головних переваг SDS – простота й дешевина масштабування рішення, оскільки в традиційних СЗД використовуються дорогі специфічні контролери, плати й диски. Для програмного рішення можна придбати будь-які сучасні диски, дискові полки й сервери за прийнятною ціною й додати їх у систему. Якщо ж устаткування відробило свій строк і виводиться з експлуатації, ліцензія на ПЗ без проблем переноситься на нове «залізо».

Замовники хочуть зберегти свої інвестиції в інфраструктуру зберігання. Тому в програмному забезпеченні, що розробляється в даній роботі, передбачили можливість поступового й планомірного впровадження системи: почавши з невеликих некритичних завдань, ємність і продуктивність можна нарощувати по потребі. Оплата по факті використання, as-you-go, поширюється не тільки на програмне забезпечення, але й на апаратні платформи. Щоб спростити вбудовування системи в існуючий IT-ландшафт, використовується API у вигляді простого командного рядка, що підходить і для автоматизації операцій.

Пропоноване програмно обумовлене сховище даних масштабується до 8 Пбайт шляхом об'єднання дискового простору серверів у розподілене відказостійке й масштабоване сховище даних. Архітектура програмного забезпечення, що розробляється в даній роботі, 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. Програмне забезпечення, що розробляється в даній роботі, 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), рекомендується 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, програмне забезпечення, що розробляється в даній роботі, приблизно у два рази ефективніше Ceph, оскільки в ньому відсутній сервіс моніторингу (ця функціональність виконується сервісом MDS). У сценаріях випадкового запису програмне забезпечення, що розробляється в даній роботі, 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, а програмне забезпечення, що розробляється в даній роботі, спочатку формує всі дані в SSD-журналі, а потім у фоновому режимі відправляє їх на жорсткий диск.

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 настроїти кластер можна протягом години. Наше рішення легко масштабувати, причому в одному кластері без проблем може застосовуватися встаткування 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 за протоколом 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 гіпервізора. Вибір KVM був визначений тим, що за останні кілька років він став для багатьох синонімом гіпервізорної віртуалізації. На KVM перейшли такі гіганти, як Apple, Intel і PayPal.

Проте не рекомендується будувати рішення на базі відкритого гіпервізора 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 встаткування (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. У програмному забезпеченні, що розробляється в даній роботі, 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 встаткування, 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 все 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.

Налаштування продуктивності СЗД

Якщо компанія не хоче витратити гроші впусту, 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 їхні бізнес-застосунки 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 робітничому середовищі.

Питання вибору встаткування рано або пізно виникає в будь-якої компанії, наприклад, у зв'язку з незадоволеністю поточною продуктивністю застосунків. 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 проведене 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 трипотоковому 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 налаштування продуктивності, у цьому випадку на рівні екземпляра бази даних: швидкість запису після налаштування збільшилася більш ніж у два рази. Отже, якщо система перестала справлятися з підтримкою застосунків 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 налаштуванні 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 використання декількох інтерфейсів для доступу до конкретного СЗД. Як показало тестування, у випадку СЗД Huawei 5500 V3 швидкість запису 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.

Застосунки розрізняються вимогами до введення-виводу, а системи зберігання – архітектурою, тому дати які-небудь загальні рекомендації щодо налаштування 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 2018 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 виділяється – 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. Представлено 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 застосунок 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 стоїть питання надійності зберігання даних. На базі пропонованого рішення 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. Програмне забезпечення 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 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 за протоколом ONVIF. Крім цього, сервери можуть виконувати функції поштового сервера, Web-сервера, хмарного сховища, мультимедійного сервера, сервера друку, 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.

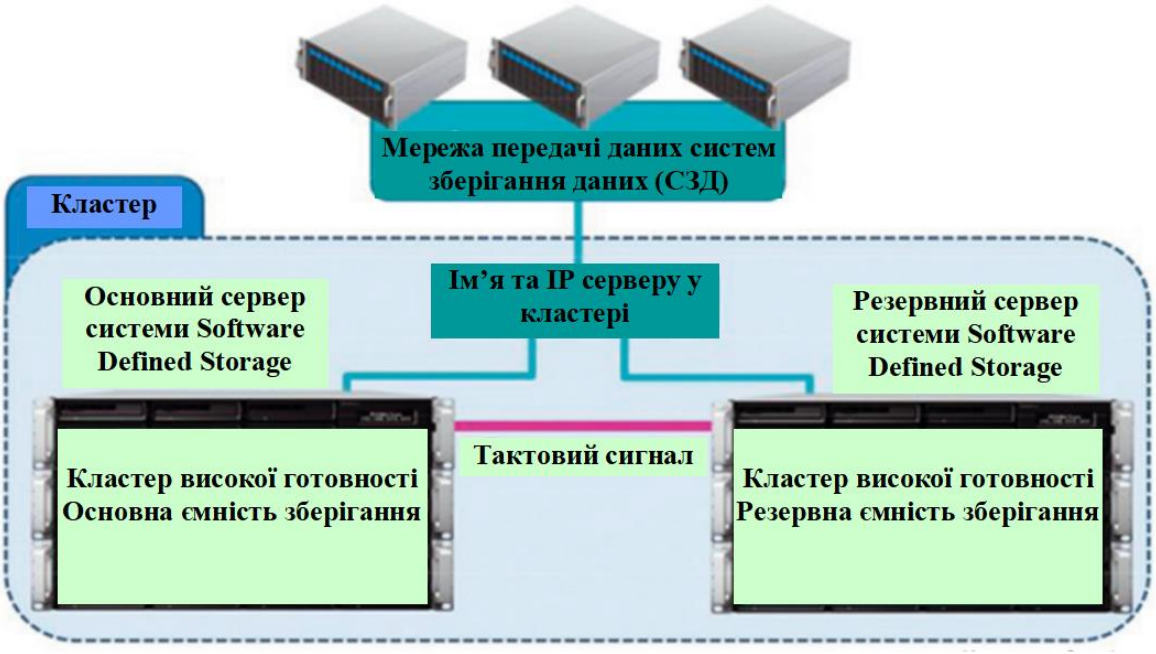


Рисунок 1 – Структурна схема системи

На базі рішення, що розроблено в даній роботі, можна побудувати інфраструктуру за принципом Active-Passive: при виході з ладу одного сервера, другий протягом 30 з візьме на себе всю роботу

Програмно обумовлене зберігання називають найбільшим просуванням в області рішень для зберігання даних із часів появи мережних сховищ. Перехід від монолітних пропрієтарних сховищ до гнучкого 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.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів Software Defined Storage. В межах України в недостатній мірі

представлені вітчизняні розробки в цій області. У роботі наведені теоретичне узагальнення й рішення наукового завдання дослідження методів Software Defined Storage. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем Software Defined Storage; Досліджена система Software Defined Storage; На основі отриманих результатів досліджень створена програмна реалізація системи Software Defined Storage. Розроблені під час виконання роботи алгоритми дозволяють успішно вирішувати завдання Software Defined Storage. 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. 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.
2. 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.
3. 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.
4. 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.
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. 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. 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.
8. 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.
9. 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.
10. 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.

УДК 004

О. Красноноженко, магістр гр. КІ-19М-1,4
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ ХМАРНОЇ СИСТЕМИ ПОБУДОВИ ТА КЕРУВАННЯ МЕРЕЖАМИ НА ОСНОВІ ВИКОРИСТАННЯ SD-WAN

У статті розроблено програмне забезпечення, яке призначено для хмарної системи побудови та керування мережами на основі використання SD-WAN. Метою розробки є дослідження та програмна реалізація хмарної системи побудови та керування мережами на основі використання SD-WAN. Об’єктом дослідження є процес побудови та керування мережами на основі використання SD-WAN. Предметом дослідження є методи побудови та керування мережами на основі використання SD-WAN. Методи дослідження базуються на методах побудови та керування мережами, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація хмарної системи побудови та керування мережами на основі використання SD-WAN.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, побудова та керування мережами, SD-WAN

Постановка проблеми. Коли ми говоримо про SD-WAN – програмно-визначаємі розподілені мережі – ми маємо на увазі рішення для керування мережею й передачі даних між центром і філіями. Що стосується основних характеристик і завдань, які звичайно ставляться перед SD-WAN, те це, як правило, інтелектуальне керування трафіком, що передається від центра до філії й назад. Також для програмно-визначаємих мереж характерна єдина точка керування всією інфраструктурою й моніторингу. Звичайно це виглядає так: є якась центральна площадка, є філії. Скрізь повинні бути встановлені пристрої, які будуть працювати з технологією програмно-визначаємих мереж. Вся конфігурація цього розподіленого устаткування походить із єдиної точки – контролера. При якихось змінах конфігурації контролер на вимогу адміністратора поширює відновлення на інші пристрої, які перебувають у філіях. У випадку з великою кількістю філій, будь-які типові процедури по зміні конфігурації звичайно займають досить велику кількість часу. У випадку з SD-WAN буде інакше: досить настроїти один пристрій, і все це передати по мережі далі. Звідси маємо зниження операційних витрат на керування інфраструктурою. Крім завдань керування конфігурацією, контролер також бере на себе роль точки моніторингу. Він стежить за розподіленою мережею. Адміністраторові не потрібно у випадку якихось змін у мережі заходити на кожній пристрій. Якщо при моніторингу виявляється проблема: падіння каналу зв'язку, погіршення характеристик каналу, ріст затримки сигналу та інше – це відразу відслідковується й відображається у відповідній панелі. Можна подивитися як поточну, так і історичне завантаження каналу, відстежити сплески навантаження тієї або іншої філії.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні хмарної системи побудови та керування мережами на основі використання SD-WAN.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація реалізація хмарної системи побудови та керування мережами на основі використання SD-WAN.

Для досягнення поставленої мети визначена програма дослідження, що складається з

наступних завдань:

1. Огляд існуючих систем побудови та керування мережами на основі використання SD-WAN
2. Дослідження хмарної системи побудови та керування мережами на основі використання SD-WAN.
3. Програмна реалізація хмарної системи побудови та керування мережами на основі використання SD-WAN.

Об'єктом дослідження є процес побудови та керування мережами на основі використання SD-WAN

Предметом дослідження є методи побудови та керування мережами на основі використання SD-WAN

Методи дослідження базуються на методах побудови та керування мережами, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Система, проектована в даній роботі буде побудована на використанні технології Cisco SD-WAN. Сучасні трудові ресурси стають усе більше мобільними, а важливі для бізнесу застосунки працюють через Інтернет з безліччю хмар. Глобальні мережі із традиційною архітектурою не поспівають за цими тенденціями через недолік доступної пропускної здатності, обмежених засобів захисту й підвищеної складності, що не дозволяє IT-відділу вчасно реагувати на потребі бізнесу.

Переваги Cisco SD-WAN

Передбачуване поводження додатків

Підвищте продуктивність роботи користувачів шляхом оптимізації характеристик хмарних і локальних додатків за допомогою аналітики, контролю й керування в реальному часі.

Спрощення на рівні підприємства

Централізуйте керування хмарами, щоб спростити розгортання мереж SD-WAN і засобів їхнього захисту, зберігши дію політик на тисячах об'єктів.

Надійній захист у потрібнім місці

Захистите користувачів, пристрої й застосунки, прискоривши розгортання убудованих або хмарних систем безпеки із кращими засобами аналітики погроз.

Максимальні можливості вибору й керування

Забезпечте гнучкість за рахунок використання хмарної архітектури для підключення будь-якого користувача до будь-якого застосунку через будь-яку хмару.

Як працює архітектура Cisco SD-WAN

Cisco SD-WAN – це архітектура, в основі якої лежить принцип пріоритетної реалізації хмарних рішень, що розділяє площини даних і керування, керовані через консоль Cisco vManage. Ви можете швидко створити оверлейну фабрику SD-WAN для підключення центра обробки даних, філій, комплексів будинків і центрів спільного розміщення ресурсів для підвищення швидкості, безпеці й ефективності мережі.

Впровадите SD-WAN на платформі за своїм вибором

Платформи для SD-WAN пройшли тестування в галузі й мають відповідні сертифікати, пропонують різні способи підключення до глобальних мереж і широкій спектр можливостей підвищення продуктивності для задоволення потреб вашого бізнесу. Тільки Cisco поєднує кращі у своєму класі мережні рішення й засоби захисту для підвищення продуктивності додатків і зниження ризиків – від філій до периметра хмари.

Фізичній рівень

Розгортайте високопродуктивні платформи для філій і комплексів будинків з убудованими мережними сервісами:

- Маршрутизатори ASR серії 1000.
- Маршрутизатори ISR серії 1000.
- Маршрутизатори ISR серії 4000.

- Маршрутизатори vEdge.
- Meraki SD-WAN.

Віртуальній рівень

Запустите віртуалізовані мережні сервіси на платформах, призначених для віртуалізації:

- Cisco ENCS.
- SD-Branch.

Хмарні технології

Підключитеся до будь-якої хмари й оптимізуйте застосунку SaaS:

- Хмарній маршрутизатор CSR 1000v.
- Cloud onRamp для Office 365.
- Інформаційній бюлетень vEdge Cloud.

Розробка структурної схеми

Перенос додатків у хмару вимагає більше високошвидкісних і надійних підключень, а Інтернет речей – більшої продуктивності, адже число підключених до нього споживчих прикінцевих пристроїв продовжує рости, збільшуючи навантаження на пропускну здатність і роблячи мережі уразливими для різних погроз. Одночасно із цим ваші співробітники усе більше мобільні, і їм необхідна оптимальна робота, де б вони не перебували. Компаніям непросто працювати з таким ландшафтом, але програмно-обумовлена WAN Cisco їм у цьому допоможе. Вона сполучить високу ефективність програмно-визначаємих систем з перевіреною надійністю платформ Cisco, забезпечуючи безпрецедентно широкі можливості моніторингу WAN, оптимальне підключення для кінцевих користувачів і самій повній набір функцій безпеки для зміцнення вашої мережі.

Фабрика програмно-визначаємої WAN Cisco

Консоль Cisco SD-WAN vManage дозволяє вам швидко створити оверлейну фабрику для програмно-визначаємої WAN, що зв'язує центри обробки даних, філії, кампуси й центри колокації й високу швидкість, що забезпечує, безпеку й ефективність роботи мережі. Призначивши шаблони й політики, ви зможете скористатися засобами аналітики для виявлення проблем з підключенням і контекстуальними проблемами, а потім підібрати оптимальні шляхи підключення користувачів до необхідних ресурсів, незалежно від типу з'єднань.

Платформи оркестрації й контролера Cisco vBond і vSmart, що підтримують як хмарне, так і локальне розміщення, реалізують автентифікацію й виділення ресурсів мережної інфраструктури, гарантуючи, що підключатися до вашої програмно-визначаємої WAN будуть тільки авторизовані пристрої. Після підключення ці платформи визначать оптимальній шлях надання користувачам необхідних додатків і візьмуть на себе оверлейну маршрутизацію, адаптацію в режимі реального часу до змін політик, а також ключові взаємодії, які будуть доставлятися через повнозв’язну мережу шифрування Cisco.

Крім того, програмно-визначаєма WAN Cisco підтримує стандартні протоколи маршрутизації, що є критично важливими для всіх корпоративних середовищ такого роду, такі як протокол граничного шлюзу (BGP), Open Shortest Path First (OSPF), Virtual Router Redundancy Protocol (VRRP) і протокол IPv6.

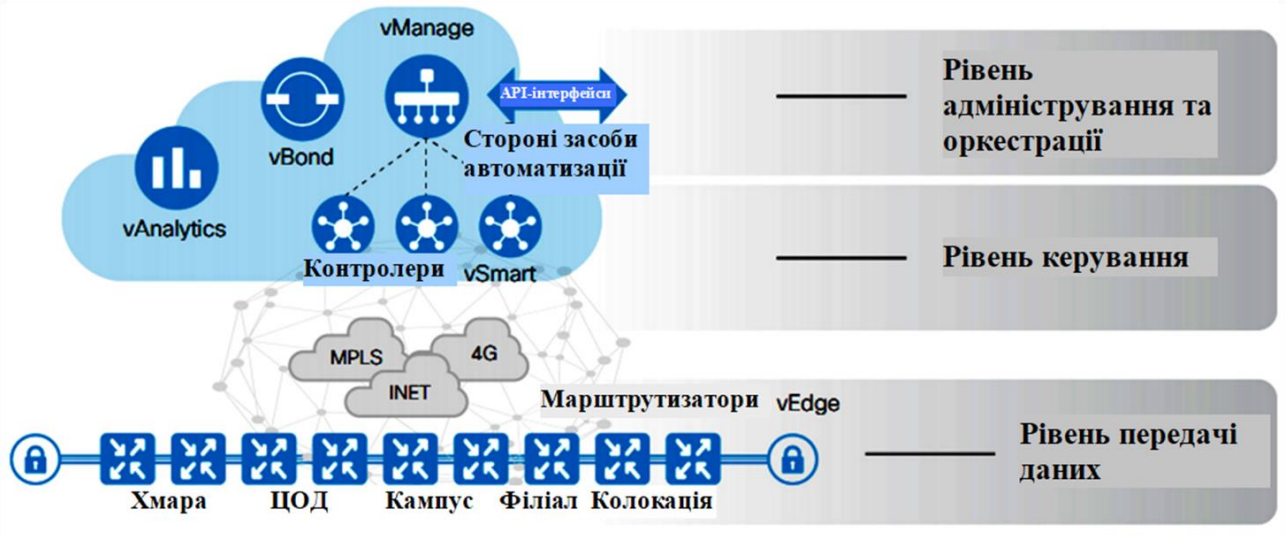


Рисунок 1 – Структурна схема системи

Програмно-визначаєма WAN Cisco дає вам наступні можливості:

– Незалежність транспортних каналів: можливість розгортати WAN з будь-якими підключеннями, наприклад MPLS, Інтернетом або 4G LTE.

– Мережні сервіси: набір багатофункціональних мережних сервісів і сервісів безпеки, що розгортаються по запиті, включаючи оптимізацію WAN, міжмережевої екран і систему запобігання вторгнень IPS.

– Гнучкій вибір прикінцевих пристроїв: програмно-обумовлена WAN може бути розгорнута в невеликих або великих філіях, кампусах, центрах обробки даних і хмарі як на фізичних, так і на віртуальних платформах.

Програмно-визначаєма WAN Cisco надає користувачам не тільки можливість керування WAN-з'єднаннями через єдину панель, але й більше швидке, надійне й ефективне підключення до хмарних платформ.

За допомогою консолі Cisco SD-WAN vManage ви можете легко автоматизувати розгортання віртуальних приватних шлюзів у середовищах IaaS і PaaS. А рішення Cisco SD-WAN OnRamp реалізує безпечну доставку додатків замовникам, адаптуючи маршрути IPsec для надання необхідних служб і забезпечення оптимальної продуктивності, при цьому контролюючи інфраструктуру розміщення на предмет аномалій.

Cisco SD-WAN OnRamp забезпечує поліпшене автоматизоване підключення до хмарних середовищ IaaS і PaaS, рятуючи вас від необхідності використовувати вже наявні багатокористувальницькі шлюзи або довго підключатися вручну. І завдяки програмно-визначаємой WAN Cisco ви одержуєте оперативне подання хмарного трафіку, контроль над розгортанням і зручне автоматичне керування.

Крім того, рішення Cisco SD-WAN OnRamp дозволяє автоматизувати SaaS-застосунки, необхідні вам і вашим партнерам у повсякденній роботі.

Cisco SD-WAN OnRamp здійснює постійній моніторинг роботи опорної мережі через панель керування vManage. У режимі реального часу рішення автоматично вибирає найшвидшій і надійній шлях доставки SaaS-Додатків вашим користувачам, незалежно від їхнього місцезнаходження. При не залежному від вас порушенні роботи сервісів рівня 3 система Cisco SD-WAN OnRamp вносить необхідні коректування, забезпечуючи зацікавленим особам гарантовану безперебійну роботу.

Тільки необхідній захист. Тільки там, де потрібно

Будучи провідної у світі компанією в сфері мережних технологій, Cisco задала стандарти в області маршрутизації. Як найбільшій постачальник рішень корпоративної каібербезпеки, Cisco надає комплексній захист тисячам замовників.

Вибираючи програмно-визначаєму WAN Cisco, ви одержуєте у своє розпорядження перевірені сертифіковані платформи з керуванням через загальну панель і можливістю миттєво розгортати необхідній захист там, де вам потрібно. Усього кілька клацань мишею в консолі Cisco vManage дозволяють оперативно зміцнити оборону всієї мережі, скоротити ризики, забезпечити відповідність бізнес-вимогам, гарантувати безперебійну роботу й привести організацію до успіху.

Наша програмно-визначаєма WAN може зробити з ваших маршрутизаторів Cisco витончені багаторівневі пристрої безпеки з орієнтованим на застосунки корпоративним міжмережевим екраном, системою запобігання вторгнень IPS, фільтрацією URL-адрес і безперервним моніторингом DNS. У результаті кінцеві користувачі із центрів обробки даних, філій, кампусів або віддалених об'єктів будуть надійно захищені від самих різних погроз безпеки. Крім того, рішення підтримує наскрізну сегментацію мережного трафіку, що захищає ваш бізнес від крадіжки даних і внутрішніх погроз.

Прогнозована робота додатків

Просунута аналітична система vAnalytics, доступна через консоль Cisco vManage, дозволяє швидко надавати зацікавленим особам дані моніторингу для виявлення проблем у глобальній мережі. vAnalytics включає наступні додаткові компоненти.

– Комплексній моніторинг додатків і інфраструктури в рамках всієї фабрики програмно-визначаємой WAN.

– Надавані в реальному часі відомості для кореляції даних про збої, порівняльного дослідження замовників і рейтингу продуктивності додатків.

– Прогнозування роботи зі сценаріїв «Що, якщо».

– Допомога в плануванні по виділенню застосункум ресурсів, збільшенню пропускної здатності й розширенню інфраструктури філій.

– Інтелектуальні рекомендації на основі існуючій політик, шаблонів і переваг.

– Категоризація якості обслуговування (QoS) додатків і зміни політик для забезпечення передбачуваної продуктивності.

Крім того, використовуваній в Cisco SD-WAN vAnalytics розширеній механізм кореляції подій усуває шум у неопрацьованих даних і застосовує контекстній аналіз, видаючи повідомлення, коли якесь переривання в роботі сервісів дійсно заслуговує вашої уваги. Це істотно скорочує число помилкових спрацьовувань і непотрібних ескалацій, заощаджуючи час вашого IT-відділу для рішення більше важливих завдань.

Програмно-визначаєма WAN Cisco підтримує розширену аналітику, моніторинг і автоматизацію для будь-яких підключень у вашій мережі (як MPLS, так і за межами хмари). З нею ви можете бути впевнені, що користувачі одержать оптимальну швидкість і продуктивність у застосункух, необхідних їм для успішної роботи. Ще більша ефективність і зручність за рахунок стабільного й захищеного доступу до бізнес-застосункум на перевіреному сертифікованому встаткуванні.

Платформи програмно-визначаємой WAN

І у своєму встаткуванні, і в програмному забезпеченні Cisco прагне створювати якісні інноваційні технології, які допоможуть вашому бізнесу досягти нових висот. Програмно-визначаєма WAN Cisco не виключення. Це рішення підтримує широкій вибір варіантів розгортання й дозволяє створити єдину фабрику WAN з можливостями масштабування в мультихмарних середовищах. Пристроі для програмно-визначаємоі WAN Cisco можна розгортати у філіях, кампусах, головних офісах, ЦОД і центрах колокації.

Філії й кампуси

Варіанти розгортання програмно-визначаємої WAN Cisco включають фізичну, віртуальну й хмарну маршрутизацію на базі маршрутизаторів Cisco vEdge, CSR 1000v, ISR 1000 і ISR 4000, а також з використанням архітектури віртуалізації мережних функцій (NFV) на базі рішень Cisco для програмно-визначаємих філій (SD-Branch), наприклад платформ ENCS 5000 і UCS серії E.

Головні офіси, ЦОД і центри колокації

Варіанти розгортання програмно-визначаємой WAN Cisco включають фізичну, віртуальну й хмарну маршрутизацію на базі маршрутизаторів Cisco CSR 1000v і ASR 1K або з використанням архітектури віртуалізації мережних функцій на базі рішень регіонального порталу (Regional Hub) на платформах CSP 5K.

Програмно-визначаєма WAN Cisco дозволяє вибрати оптимальну платформу для вашого середовища з будь-якими бізнес-потребами.

Приклади використання

Програмно-визначаєма WAN Cisco забезпечує великій ряд переваг при роботі з мережею, безпекою й хмарою. Оцініте її переваги для своєї галузі.

Роздрібна торгівля :

– Сегментація трафіку POS-терміналів для відповідності вимогам індустрії платіжних карткових систем (PCI) і забезпечення мережної безпеки.

– Забезпечення захищеного прямого доступу до Інтернету для замовників і персоналу.

– Підвищення пропускної здатності й значне скорочення витрат на ланцюзі.

– Реалізація в магазинах таких послуг, як гостьовій бездротової доступ, цифрова візуалізація, віддалені консультанти й Інтернет речей.

– Прискореній запуск нових філій і магазинів з автоматизованим розгортанням і функціями попереднього виділення ресурсів.

– Спрощення керування мережею й політиками безпеки по всій організації, включаючи філії.

Охорона здоров'я:

– Міграція на хмарні застосунки для охорони здоров'я (для електронних медичних карт і історій хвороби).

– Збільшення часу безперебійної роботи мережі для надання послуг пацієнтам і персоналу.

– Міграція IT-інфраструктури лікарні в хмару без участі IT-Персоналу.

– Швидке підключення гостьового доступу до Wi-Fi, хмарної VoIP-зв'язку, роздачі ліків і інших сервісів.

– Підвищення ефективності роботи філій будь-якого розміру: від невеликих клінік до великих лікарень.

– Дотримання вимог безпеки й законодавства в сфері охорони здоров'я; відділення внутрикорпоративної мережі від мережі телемедицини або медкарт.

Утворення:

– Оптимізація в режимі реального часу для офісних додатків і додатків SaaS для навчання.

– Забезпечення безпеки й відповідності вимогам; відділення студентської або викладацької мережі для досліджень від гостьової мережі.

– Економія при підключенні всієї глобальної мережі до хмари.

Фінанси:

– Виділення більшої пропускної здатності за меншою ціною завдяки великому пулу ресурсів « активній-активній».

– Політики додатків для оптимізації якості роботи й маршрутизація з урахуванням додатків для підтримки у філіях таких сервісів, як цифрова візуалізація й відеобанкінг із HD-якістю.

– Висока продуктивність і безпека при використанні хмарних трейдингових і фінансових додатків.

– Можливість розгортання топологій з урахуванням додатків, де буде використовуватися захищена фабрика й повсюдне шифрування, які дозволять розмежувати зв'язок між банкоматами й відео- або VoIP-зв'язок між філіями.

Промислове виробництво:

– Впровадження комплексної сегментації для розмежування бізнес-підрозділів і десятків ізольованих сегментів.

– Захищеній контрольованій доступ для ділових партнерів через зовнішню мережу.

– Єдина панель керування підключеннями й безпекою промислового Інтернету речей.

Постачальники послуг:

– Значне скорочення витрат на доступ до Інтернету у філіях (своїх або клієнтських) за рахунок використання власної мобільної або оверлейної інфраструктури без необхідності орендувати канал у конкурента.

– Сегментація трафіку POS-терміналів для відповідності вимогам індустрії платіжних карткових систем і забезпечення мережної безпеки.

– Реалізація в магазинах або філіях таких послуг, як гостьовій бездротової доступ, цифрова візуалізація, віддалені консультанти й Інтернет речей.

– Прискореній запуск нових філій і магазинів з автоматизованим розгортанням.

– Можливість запропонувати бізнес-клієнтам вигідну захищену програмно-визначаєму WAN як новій сервіс, здатній швидко принести прибуток.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів побудови та керування мережами на основі використання SD-WAN. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем побудови та керування мережами на основі використання SD-WAN; Досліджена система побудови та керування мережами на основі використання SD-WAN; На основі отриманих результатів досліджень створена програмна реалізація хмарної системи побудови та керування мережами на основі використання SD-WAN. Розроблені під час виконання роботи алгоритми дозволяють успішно вирішувати завдання побудови та керування мережами на основі використання SD-WAN . 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.

УДК 004

С. Кузнєцова, магістр гр. КН-19МЗ
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ ПРОЕКТУВАННЯ ЦОД З ВИКОРИСТАННЯМ ТЕХНОЛОГІЙ КАСТОМІЗАЦІЇ

У статті розроблено програмне забезпечення, яке призначено для системи проектування ЦОД з використанням технологій кастомізації. Метою розробки є дослідження та програмна реалізація системи проектування ЦОД з використанням технологій кастомізації. Об’єктом дослідження є процес проектування ЦОД з використанням технологій кастомізації. Предметом дослідження є методи проектування ЦОД з використанням технологій кастомізації. Методи дослідження базуються на методах Big Data, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи проектування ЦОД з використанням технологій кастомізації.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, ЦОД, кастомізація

Постановка проблеми. Існують наступні сучасні підходи до побудови мереж у центрах обробки даних (ЦОД), а саме технології побудови розподілених фабрик комутації – Transparent Interconnect a Lot of Links (TRILL) і Shortest Path Bridging (SPB).

З історичних причин зложилося так, що на ринку з'явилися дві дуже схожі технології маршрутизації на другому (L2) рівні – TRILL і SPB, суть яких полягає в тому, що на базі протоколу стану каналу (в обох випадках використовується IS-IS) розраховується топологія мережі комутації й потім на основі цих розрахунків передається трафік L2 між мережними пристроями (nodes). Отже, TRILL і SPB має сенс використовувати:

– при побудові більших, плоских L2-фабрик комутації, де переважають «горизонтальні» комунікації сервер – сервер, наприклад, для кластеризації, хмарних обчислень, підтримки vMotion і т.д.;

– з метою об'єднання декількох площадок в один загальний домен L2, особливо коли площадок більше трьох;

– при реалізації мультивендорних рішень, коли, наприклад, мережне встаткування декількох виробників потрібно якимось образом вмонтувати в загальну інфраструктуру.

В останньому випадку використання технологій організації стека на зразок IRF важко в силу ряду обмежень, тоді як TRILL і SPB є стандартами й тому повинні бути однаково реалізовані на встаткуванні всіх вендорів, що заявляють про їхню підтримку.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи проектування ЦОД з використанням технологій кастомізації.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи проектування ЦОД з використанням технологій кастомізації.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем проектування ЦОД з використанням технологій кастомізації.

– Дослідження системи проектування ЦОД з використанням технологій кастомізації.

– Програмна реалізація системи проектування ЦОД з використанням технологій кастомізації.

Об'єктом дослідження є процес проектування ЦОД з використанням технологій кастомізації.

Предметом дослідження є методи проектування ЦОД з використанням технологій кастомізації.

Методи дослідження базуються на методах Big Data, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Поряд з будівництвом нових дата-центрів на порядку денному стоїть проблема модернізації старих. Середній строк відновлення комп'ютерного встаткування в ЦОД – приблизно три роки. Інфраструктура ЦОД проектується з урахуванням строку експлуатації порядку 15 років.

Призначення й структура ЦОД

Залежно від призначення сучасні ЦОД можна розділити на корпоративні, які працюють у рамках конкретної компанії, і ЦОД, що надають сервіси стороннім користувачам.

Наприклад, банк може мати дата-центр, де зберігається інформація із транзакцій його користувачів, – звичайно він не робить послуг стороннім користувачам. Навіть якщо ЦОД не надає подібних послуг, він може бути виділений в окрему організаційну структуру компанії й робити їй послуги з доступу до інформаційних сервісів на базі SLA. Багато великих компаній мають ЦОД того або іншого виду, а міжнародні компанії можуть мати десятки ЦОД.

ЦОД може також використовуватися для надання послуг професійного IT-аутсорсингу IT-решений на комерційних умовах.

Всі системи ЦОД складаються із властиво IT-інфраструктури й інженерної інфраструктури, що відповідає за підтримку оптимальних умов для функціонування системи.

IT-інфраструктура

Сучасний центр обробки даних (ЦОД) включає серверний комплекс, систему зберігання даних, систему експлуатації й систему інформаційної безпеки, які інтегровані між собою й об'єднані високопродуктивної ЛОМ. Розглянемо організацію серверного комплексу й системи зберігання даних.

Серверний комплекс ЦОД

Найбільш перспективною моделлю серверного комплексу є модель із багаторівневою архітектурою, у якій виділяється кілька груп серверів:

– ресурсні сервери, або сервери інформаційних ресурсів, відповідають за збереження й надання даних серверам додатків; наприклад, файл-сервери;

– сервери додатків виконують обробку даних відповідно до бізнес-логікою системи; наприклад, сервери, що виконують модулі SAP R/3;

– сервери подання інформації здійснюють інтерфейс між користувачами й серверами додатків; наприклад, web-сервери;

– службові сервери забезпечують роботу інших підсистем ЦОД; наприклад, сервери керування системою резервного копіювання.

До серверів різних груп пред'являються різні вимоги залежно від умов їхньої експлуатації. Зокрема, для серверів подання інформації характерний великий потік

коротких запитів від користувачів, тому вони повинні добре горизонтально масштабуватися (збільшення кількості серверів) для забезпечення розподілу навантаження.

Для серверів додатків вимога по горизонтальній масштабованості залишається, але воно не є критичним. Для них обов'язкова достатня вертикальна масштабованість (можливість нарощування кількості процесорів, обсягів оперативної пам'яті й каналів уведення-виводу) для обробки мультиплексованих запитів від користувачів і виконання бізнес-логіки розв'язуваних завдань.

Системи зберігання даних

Найбільш перспективним рішенням організації системи зберігання даних (СЗД) є технологія SAN (Storage Area Network), що забезпечує відказостійкий доступ серверів до ресурсів зберігання й що дозволяє скоротити сукупну вартість володіння IT-інфраструктурою за рахунок можливості оптимального онлайнового управління доступу серверів до ресурсів зберігання. СЗД складається із пристроїв зберігання інформації, серверів, системи керування й комунікаційної інфраструктури, що забезпечує фізичний зв'язок між елементами мережі зберігання даних. Подібна архітектура дозволяє забезпечити безперебійне й безпечне зберігання даних і обмін даними між елементами мережі зберігання даних.

В основі концепції SAN лежить можливість з'єднання кожного із серверів з будь-яким пристроєм зберігання даних, що працюють по протоколі Fibre Channel (FC). Технічну основу мережі зберігання даних становлять волоконно-оптичні з'єднання, FC-HBA і FC-комутатори, у цей час передачі, що забезпечують швидкість, 200 Мбайт/с.

Застосування SAN як транспортна основа системи зберігання даних дає можливість динамічної реконфигурації (додавання нових пристроїв, зміна конфігурацій наявне і їхнє обслуговування) без зупинки системи, а також забезпечує швидке перегрупування пристроїв відповідно до вимог, які змінилися, і раціональне використання виробничих площ.

Висока швидкість передачі даних по SAN (200 Мбайт/с) дозволяє в реальному часі реплікувати дані, що змінюються, у резервний центр або у вилучене сховище. Зручні засоби адміністрування SAN дають можливість скоротити чисельність обслуговуючого персоналу, що знижує вартість змісту підсистеми зберігання даних.

Адаптивна інженерна інфраструктура ЦОД

Крім властиво апаратно-програмного комплексу, ЦОД повинен забезпечувати зовнішні умови для його функціонування. Розміщене в ЦОД устаткування повинне працювати в цілодобовому режимі при певних параметрах навколишнього середовища, для підтримки яких потрібен цілий ряд надійних систем забезпечення.

Сучасний ЦОД нараховує більше десятка різних підсистем, включаючи основне й резервне живлення, слабкострумовий, силову й інший види проводки, системи кліматичного контролю, забезпечення пожежної безпеки, фізичний безпеки та ін.

Досить складним є забезпечення оптимального кліматичного режиму встаткування. Необхідно відводити велику кількість тепла, виділюваного комп'ютерним устаткуванням, причому його обсяг наростає в міру збільшення потужності систем і щільності їхнього компонування. Все це вимагає оптимізації повітряних потоків, а також застосування охолодного встаткування. По даним IDC, уже цього року витрати на постачання центрів обробки даних електроенергією й забезпечення охолодження перевищать витрати на властиво комп'ютерне встаткування. Перераховані системи взаємозалежні, тому оптимальне рішення може бути знайдено тільки якщо при його побудові будуть розглядатися не окремі компоненти, а інфраструктура в цілому.

Проектування, будівництво й експлуатація ЦОД – досить складний і трудомісткий процес. Існує безліч компаній, що пропонують необхідне встаткування – як комп'ютерне, так і допоміжне, але для побудови індивідуального рішення без допомоги інтеграторів тут не обійтися.

ЦОД і IT-аутсорсинг

Найбільш комплексна послуга IT-аутсорсингу – це аутсорсинг інформаційних систем. Він надається за довгостроковою згодою, по якому постачальник послуг одержує в повне керування всю IT-інфраструктуру клієнта або її значну частину, у тому числі встаткування й установлене на ньому програмне забезпечення. Це проекти із широким залученням виконавця, які припускають відповідальність за системи, мережу й окремі додатки, що входять в IT-інфраструктуру. Звичайно аутсорсинг IT-інфраструктури оформляється довгостроковими контрактами, які тривають більше роки.

Для створення власної IT-інфраструктури з нуля компаніям необхідні більші засоби й високооплачувані фахівці. Оренда інфраструктури дата-центра дозволяє знизити ТСО за рахунок поділу ресурсів між клієнтами, забезпечує доступ до новітніх технологій, дає можливість швидкого розгортання офісів з можливостями нарощування ресурсів. Для багатьох компаній надійність безперебійного функціонування встаткування й мережної інфраструктури стає сьогодні критичним фактором для функціонування бізнесу. Аутсорсинг IT-інфраструктури дозволяє забезпечити високий рівень надійності даних при обмеженій вартості, надаючи клієнтам можливість оренди серверних стійок і місць у стійці для розміщення встаткування замовника (co-location), оренди виділеного сервера (dedicated server), ліцензійного ПЗ, каналів передачі даних, а також одержання технічної підтримки. Замовник звільняється від безлічі процедур: технічної підтримки й адміністрування встаткування, організації цілодобової охорони приміщень, моніторингу мережних з'єднань, резервного копіювання даних, антивірусного сканування ПЗ й т.д.

ЦОД також може робити послугу аутсорсингового керування додатками. Це дозволяє замовникам використовувати сертифікованих фахівців, що гарантує високий рівень обслуговування програмних продуктів і забезпечує легкий перехід з одного ПЗ на інше при мінімальних фінансових витратах.

У режимі аутсорсингу додатків клієнти ЦОД можуть одержати аутсорсинг поштових систем, інтернет-ресурсів, систем зберігання даних або баз даних.

Передаючи свої корпоративні системи на аутсорсинг для резервування, замовники знижують ризик втрати критичної інформації за рахунок використання професійних систем поновлення працездатності IT-систем, а у випадку аварії одержують можливість страхування інформаційних ризиків.

Звичайно клієнтам ЦОД пропонується кілька рівнів забезпечення безперервності бізнесу. У найпростішому випадку це розміщення резервних систем у дата-центрі із забезпеченням належного захисту. Крім того, може бути варіант, при якому клієнтові також надається оренда програмно-апаратних комплексів для резервування. Найбільш повний варіант послуги припускає розробку повномасштабного плану відновлення систем у випадку аварії (Disaster Recovery Plan, DRP), що має на увазі аудит інформаційних систем замовника, аналіз ризиків, розробку плану відновлення після аварії, створення й обслуговування резервної копії системи, а також надання обладнаного офісного приміщення для продовження роботи у випадку аварії в основному офісі.

Розробка структурної схеми

Тепер докладніше поговоримо про кожний протокол, і почнемо з SPB. Що ж таке SPB і як ця технологія працює? SPB Mac-in-Mac (SPBM) дозволяє здійснювати множинну маршрутизацію (multipath routing) у змішаних мережах Ethernet на основі топології, розрахованої протоколом IS-IS, причому на кожному комутаторі обчислюється своє власне дерево Shortest Path Tree, а трафік інкапсулюєся комутатором у стандартні кадри MAC-in-MAC у відповідності зі стандартом IEEE 802.1ah PBB.

Кожний Backbone Edge Bridge (BEB) за допомогою IS-IS з додатковим TLV (Type Length Value) анонсує нові сервіси у вигляді I-SID (свого роду ідентифікатор сервісу) і B-MAC (Backbone MAC) завжди, коли на комутаторі активується новий сервіс (інакше кажучи, створюється новий екземпляр віртуального сервісу – Virtual Service Instance, VSI –

с призначеної йому VLAN). Ця інформація розноситься за допомогою IS-IS, і про нову точку надання сервісу «довідаються» інші комутатори мережі.

Подивимося, як відбувається передача трафіку в SPB і як, зокрема, обробляється широкомовний трафік (broadcast).

Припустимо, віртуальна машина А повинна відправити трафік віртуальній машині В. Машина А надсилає запит ARP на адресу машини В. Комутатор B20 бачить цей пакет, інкапсулює його із вказівкою B-MAC, B-VLAN, I-SID і відправляє через своє дерево Shortest Path Tree на інші мости BEB з тим же самим I-SID. Комутатор B1 отриманий кадр уже не розбирає й у відповідності зі своєю локальною таблицею SPBM FIB відправляє його на комутатор B31. B31 розбирає кадр і розсилає його на інтерфейси, підключені до даного сервісу (VSI). У такий спосіб запит ARP доходить до віртуальної машини В.

MAC-адреса А вже відома, і У відправляє трафік машині А на певний VSI. Комутатор B31 інкапсулює цей трафік з відповідному даному сервісу I-SID, B-VLAN і B-MAC і передає його по своєму дереву SPT. B31 направляє кадр на B1 відповідно до локальної таблиці SPBM. B1, ґрунтуючись на своїй таблиці SPBM, передає кадр на B20. B20 знає MAC-адресу машини А, розбирає кадр і направляє його на локальний хост А. При цьому шляху для одне- і багатоадресного трафіку в SPB симетричні. Так передається трафік у мережі SPB.

TRILL

Тепер зрівняємо механізми роботи TRILL і SPB. Але спочатку небагато теорії. Основним пристроєм у мережі TRILL є так званий маршрутизуючий міст (Routing Bridge, RB), що виконує всі основні мережні функції. Як і у випадку з SPB, замість Spanning Tree на ньому виконується протокол IS-IS, що розраховує мережну топологію. При цьому комутатори з підтримкою TRILL сумісні з комутаторами, оснащеними традиційними мережними інтерфейсами. Пристрій з TRILL сприймає старі комутатори просто як з'єднання між двома маршрутизуючими мостами.

Формати пакетів TRILL відрізняються від пакетів SPB. Принципова відмінність полягає у відсутності поля для I-SID, що ідентифікує сервіс, тобто в пакеті TRILL не передається інформація про сервіс, для якого цей трафік призначений. В іншому формати пакетів TRILL і SPB схожі, тільки між зовнішнім і внутрішнім тегами додається ще один заголовок з EtherType = TRILL, у якому окремо виділяються імена вхідного (ingress) і вихідного (egress) комутаторів TRILL.

Як же мережа TRILL передає трафік. Допустимо, хосту S1 необхідно відправити пакет на хост D1. S1 формує пакет з MAC-адресою одержувача D1 і VLAN 10 і відправляє його на Routing Bridge 1. Routing Bridge 1 визначає, що MAC-адреса D1 перебуває за Routing Bridge 3, а потім з'ясовує, що RB3 доступний через RB2, а RB2 – через порт 2 по такому-те MAC-адресі. Він формує пакет із зовнішнім MAC-адресою RB2, опорною віртуальною мережею VLAN 200 і відправляє трафік з новим заголовком на RB2. RB2 розбирає зовнішній заголовок, переглядає таблиці й визначає порт, MAC-адреса й зовнішню VLAN, на яких для RB2 доступний RB3. Потім RB2 «перезбирає» зовнішній заголовок пакета TRILL (помітьте, номер опорної VLAN помінявся на 300) і відправляє пакет на RB3 через відповідний порт (у цьому випадку порт 4). Пакет доходить до RB3, що визначає, що цей MAC-адреса D1 перебуває за локальним інтерфейсом RB3 і, видаливши зовнішній заголовок, передає пакет на хост D1. Так одноадресний трафік передається по домену TRILL. При цьому, трафік передається через один транзитний вузол за іншим (hop-by-hop) і зовнішній заголовок «перезбирається» на кожному комутаторі заново.

Два слова про можливі типи портів. В TRILL, як і у звичайній мережі, виділяються три різновиди портів: порт доступу, до якого підключаються всі прикінцеві пристрою, магістральний (trunk) порт, через який проходить опорний (backbone) трафік, і гібридний – для зв'язку домена TRILL із традиційними сегментами мережі.

Як бачимо, контрольні пакети передаються по всіх типах з'єднань. Пакети даних без інкапсуляції TRILL – тільки через порти доступу й гібридні порти, але не магістральні. І

навпаки, пакети з інкапсуляцією TRILL – тільки через магістральні й гібридні порти, але не порти доступу.

Як згадано вище, як протокол контрольної площини й в TRILL, і в SPB використовується IS-IS. Він обраний тому, що, на відміну від інших протоколів, працює на канальному рівні (link), а також досить швидко сходиться й підтримує гнучке додавання нових TLV. При цьому TRILL визначає нові TLV в IS-IS для передачі топологічної інформації про мережу – VLAN ID, псевдоніми (Nickname), за яких ці VLAN розташовані, і т.д.

Крім того, як і в традиційних мережах, на основі пріоритету мостів вибирається виділений маршрутизуючий міст (Designated Routing Bridge). При рівності пріоритетів як додаткові критерії вибору використовується MAC-адреса, порт або SystemID. Після цього для кожної VLAN вибирається так званий призначений транспортний агент VLAN (Appointed VLAN Forwarder, AVF) – RB. Нарешті, визначається VLAN для контрольного трафіку TRILL, задається Circuit ID для LSP і потім поширюються CSNP. При цьому Designated RB є Appointed VLAN Forwarder для всі відкритих на ньому VLAN, а для інших RB AVF призначаються відповідно до SystemID, де в процесі вибору перемагає RB з найбільшим SystemID.

Що стосується завантаження каналів, то TRILL підтримує балансування на основі ECMP.

Для передачі багатоадресного/широкомовного/невідомого/одноадресного трафіку використовуються дерева. У принципі, щоб мережа працювала нормально, досить одного дерева, але з метою балансування навантаження дерев може бути кілька. Для даного кореня дерево обчислюється на основі інформації про з'єднання між комутаторами. Щоб «домовитися» про кількість дерев і параметри їхнього розрахунку, комутатори обмінюються відповідною інформацією в LSP.

При проектуванні мережі TRILL виникає багато принципових питань:

– Як приєднати мережа TRILL L2 до шлюзу L3?
– Як трафік потрапить в L2-мережа TRILL/SPB?
– Як здійснюється серверний доступ в TRILL RB або SPB BEB?
– Як успадкований комутатор L2 стане функціонувати у зв'язуванні з TRILL RB або SPB BEB?
– Чи буде використовуватися VRRP? Якщо так, то яким образом?
– Як застосовувати IRF?
– Які вимоги до HA?

Для відповіді на ці питання краще розглядати конкретні реалізації SPB/TRILL.

12900-е збирають за допомогою технології IRF у стек, що встановлюється в ядро мережі, на них же можна запустити й L3. Як комутатори доступу використовуються пристрої серії 5900, причому в цьому випадку LAGG не знадобиться, тому що за множинні шляхи L2 відповідає TRILL, хоча LAGG дозволяє скоротити кількість шляхів і весь домен буде сходитися швидше за рахунок спрощення загальної топології мережі.

З більших комутаторів TRILL підтримують пристрою серій 10500, 11900 і 12900; з комутаторів поменше, рівня ToS або ядра серверної, – серії 7900 і 5900. SPB підтримується на всіх перерахованих лінійках, крім 10500.

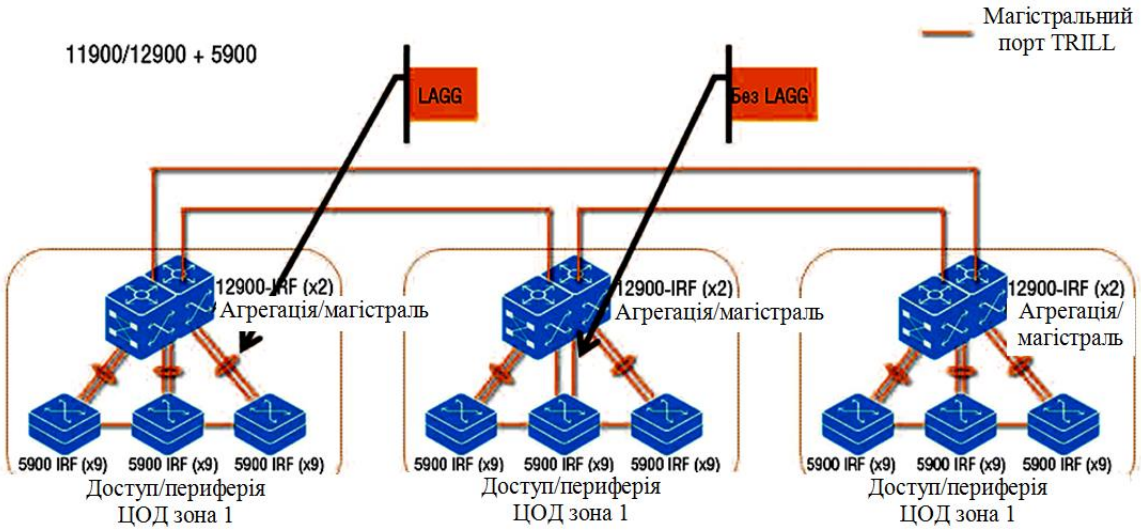


Рисунок 1 – Структурна схема системи

Одне із ключових питань, що виникає при проектуванні TRILL/SPB, складається в організації розвантаження L3 Offload – точки, у якій трафік L2 перетворюється в L3. Можливі три варіанти реалізації L3 Offload:

– організація зовнішньої петлі на пристрої;
– розвантаження усередині комутатора на мікросхемі, наприклад на 11900;
– використання Multitenant Device Context (MDC).

Перший спосіб – підключити зовнішню петлю й призначити TRILL Appointed Port, приєднаний до інтерфейсу L3. Щоб не виникло петлі L2 на порту доступу, використовується VLAN Mapping і включається захист від утворення петель (loopback protection). Такий варіант може бути налаштований для великої кількості різних VLAN. Важливий момент, на який варто звернути увагу при настроюванні, – порт доступу не повинен нести обидві VLAN (і Source VLAN, і Translated VLAN), інакше це може привести до формування петлі L2.

Інший спосіб полягає у використанні внутрішнього міжз'єднання, реалізованого на базі ASIC. Фактично це дозволяє домогтися тих же результатів, що й організація зовнішньої петлі. На жаль, дана опція доступна не на всіх моделях комутаторів, що підтримують TRILL/SPB.

Третій спосіб – організувати L3 Offload на окремому пристрої, виділеному для терминування L3, або робити це в окремому контексті MDC того ж комутатора.

У завершення поговоримо про те, як настроїти працюючу мережу, де використовується встаткування HP Networking. Почнемо з SPB.

Ядро мережі SPB з опорними мостами магістралі (Backbone Core Bridge, BCB) являє собою об'єднані в стек IRF комутатори серії 12504, до яких підключені граничні пристрої мережі SPB (Backbone Edge Bridge, BEB). У якості BEB даної мережі виступають комутатори серії 5900, а також стік із двох пристроїв серії 12504 (на схемі 1-з).

Якщо придивитися до конфігурації уважно, можна побачити, що конфігурації SPB і VPLS схожі.

У якості TRILL Spine у цій мережі використовуються комутатори 5900, 11900 і 12900, об'єднані в IRF, а 12900 ще й розділені на контексти. Периферійні комутатори – серії 5900. При цьому Spine 1, 2 і 3 перебувають в одній області OSPF Area; відносини суміжності OSPF (OSPF Adjacency) установлюються через канал L3 або інтерфейси VLAN між RB Spine і між кожним RB Spine і ядром L3. Балансування навантаження на основі VRRP використовуються для рівномірного розподілу трафіку з мережі TRILL назовні, BGP ECMP балансує трафік із зовнішніх мереж у домен TRILL.

Загальні виводи за результатами тестування TRILL/SPB можна коротко підсумувати наступними тезами:

– Балансування навантаження.

– Трафік локальних мереж від різних клієнтів може бути розподілений між декількома шляхами з рівною вартістю.

– Множинні маршрути L2 і L3 можуть функціонувати одночасно.

– Комбінування IRF і SPB/TRILL

– Оптимальний дизайн фабрики L2 і краща масштабованість.

– Висока доступність

– Збіжність менш 1 з (або близько до неї) у більшості сценаріїв збоїти.

– Потрібно звертати увагу на використання GR.

– Висока продуктивність

– Канали активний/активний на всій фабриці L2.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів проектування ЦОД з використанням 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 проектування ЦОД з використанням технологій кастомізації.Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем проектування ЦОД з використанням технологій кастомізації; Досліджена система проектування ЦОД з використанням технологій кастомізації; На основі отриманих результатів досліджень створена програмна реалізація системи проектування ЦОД з використанням технологій кастомізації. Розроблені під час виконання роботи алгоритми дозволяють успішно вирішувати завдання проектування ЦОД з використанням 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.

Список літератури

1. 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.
2. 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.
3. 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.
4. 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.
5. 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.
6. 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.
7. 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.
8. 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.

9. 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.
10. 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

С. Лазурський, магістр гр. КН-19МЗ
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ АВТОМАТИЗОВАНОЇ СИСТЕМИ ІНТЕЛЕКТУАЛЬНОГО МОНІТОРИНГУ СЕГМЕНТУ ВЕБ-СЕРЕДОВИЩА (СОЦІАЛЬНОЇ МЕРЕЖІ) НА БАЗІ МЕТОДІВ DATA MINING

У статті розроблено програмне забезпечення, яке призначено для інтелектуального моніторингу сегменту веб-середовища. Метою розробки є розробка автоматизованої системи інтелектуального моніторингу сегменту веб-середовища (соціальної мережі) на базі методів Data Mining. Об’єктом дослідження є процес моніторингу веб-середовища. Предметом дослідження є методи та засоби інтелектуального моніторингу сегментів веб-середовища. Методи дослідження базуються на методах захисту інформації, методах математичної статистики, методах розробки програмного забезпечення.
автоматизована система, моніторинг, соціальна мережа, архітектура, модель, Data Mining, інструментальний засіб, веб-середовище

Постановка проблеми. Комп'ютерні технології із застосуванням інтелектуальних обчислень переживають свій розквіт. Це пов'язано, головним чином, з потоком нових ідей, що виходять з галузі комп'ютерних наук, яка утворилась на перетині штучного інтелекту, статистики та теорії баз даних. Зараз відбувається стрімкий зріст числа програмних продуктів, що використовують нові технології, а також типів задач, де їх застосування надає значного економічного ефекту. Елементи моніторингу, автоматичної обробки і аналізу даних, що називають Data Mining стають невід'ємною частиною концепції електронних сховищ даних та організації інтелектуальних обчислень. Простий доступ користувача до сховища даних забезпечує тільки отримання відповідей на питання, що були задані, в той час як технологія Data Mining дозволяє побачити («знайти») приховані правила і закономірності у наборах даних, які користувач не може передбачити, і застосування яких може сприяти збільшенню прибутків підприємства.

Data Mining перекладається як «видобуток» чи «добування даних». Нерідко поруч з Data Mining зустрічаються слова «інтелектуальний моніторинг даних». Справа в тому, що людський розум сам по собі не пристосований для сприйняття великих масивів різнорідної інформації. Але і традиційна математична статистика, яка довгий час претендувала на роль основного інструмента аналізу даних, також нерідко відстає при вирішенні складних життєвих задач. Вона оперує усередненими характеристиками вибірки, що часто є фіктивними величинами (типу середньої температури пацієнтів в лікарні, середньої висоти будинку на вулиці тощо). Тому методи математичної статистики виявляються корисними, головним чином, для перевірки заздалегідь сформульованих гіпотез. Більшість підприємств накопичують під час своєї діяльності величезні обсяги даних, але єдине, що вони хочуть від

них одержати – це корисну інформацію. Яким чином можна довідатися з даних про те, що є найбільш потрібним для їхніх клієнтів, як найефективніше використати наявні ресурси або як мінімізувати втрати? Для вирішення цих проблем призначені новітні технології інтелектуального аналізу. Вони використовують складний статистичний аналіз і моделювання для знаходження моделей і відношень, прихованих у базі даних – таких моделей, що не можуть бути знайдені звичайними методами. Доти поки модель не відповідає існуючим реально відношенням, неможливо отримати успішні результати. Технології інтелектуального аналізу можуть не тільки підтвердити емпіричні спостереження, але і знайти нові, невідомі раніше моделі. За допомогою методів Data Mining можна знайти таку модель, що приведе до радикального поліпшення у фінансовому і ринковому становищі компанії. Хоча інструментарій інтелектуального аналізу і звільняє користувача від можливих складностей у застосуванні статистичних методів, він все-таки потребує від нього розуміння роботи цього інструментарію й алгоритмів, на яких він базується. Крім цього, технологія знаходження нового знання в базі даних не може дати відповіді на ті питання, що не були задані. Вона не заміняє аналітиків чи менеджерів, а дає їм сучасний, могутній інструмент для поліпшення роботи, яку вони виконують.

З огляду на це, тема роботи і поставлена задача розробки автоматизованої системи інтелектуального моніторингу веб-середовища є актуальною в наш час.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи інтелектуального моніторингу сегменту веб-середовища (соціальної мережі) на базі методів Data Mining.

Мета й завдання дослідження. Метою роботи є розробка автоматизованої системи інтелектуального моніторингу сегменту веб-середовища (соціальної мережі) на базі методів Data Mining.

Для досягнення поставленої мети роботи потрібно розв’язати такі задачі:

1. Проаналізувати сучасні методи та найбільш ефективні засоби (програмні продукти) моніторингу веб-середовища.

2. Розробити модель моніторингу Інтернет-середовища на базі ефективної технології Data Mining.

3. Розробити архітектуру автоматизованої системи інтелектуального моніторингу соціальної мережі.

Об’єктом дослідження є процес моніторингу веб-середовища.

Предметом дослідження є методи та засоби інтелектуального моніторингу сегментів веб-середовища.

Виклад основного матеріалу. Для виконання запиту користувача сукупністю мережних сервісів їх перш за все необхідно знайти серед чисельної кількості сервісів у мережі та далі забезпечити управління і координацію їх виконання. Управління взаємодією сервісів, або оркестровка, має забезпечуватись потоками інформації, що міститься в повідомленнях, якими обмінюються сервіси.

Загальну модель композиції сервісів, можна представити у трьох вимірах, кожен з яких має свою метрику. Вимір складності композитного сервісу визначає інформаційну місткість мов і моделей представлення сервісу. Наприклад, мова OWL-S в цьому вимірі має не високу міру, тому що засобами цієї мови сервіс описується тільки параметрами вхідної та вихідної інформації. Мова WSDL, що описує структурну інформацію сервісу засобами XML, більш інформативна, але також використовує тільки вхідну і вихідну інформацію. Другий вимір описує внутрішню структуру сервісів на рівні процесів та представляється такими моделями, як BPEL, CSP і p-Calculus, модель Міля, Римська модель, мережі Петрі. Ці моделі описують стани сервісу і відповідно послідовність активностей сервісу. Третій вимір – це здатність описувати «семантику». В цьому вимірі мова OWL–S описує властивості сервісу на рівні входів та виходів, а також конкретизує, як сервіс взаємодіє з абстрактною моделлю «реального світу». Представлення сервісів у такому «кластері» моделей робить

вищезазначені засоби дуже потужними. Розглянемо деякі з перелічених стандартів та моделей, спрямованих на вирішення задач композиції сервісів.

Особливості стандартів мережних сервісів

Для розуміння парадигми мережних сервісів у контексті мети композиції розглянемо систему стандартів. Основна причина їх створення, як наприклад, SOAP і WSDL, полягає в забезпеченні певного ступеня гнучкості при об'єднанні мережних сервісів для створення більш складних комбінацій з урахуванням динаміки середовища. Основна мета впровадження стандарту UDDI – створення засобів, які мають забезпечити автоматизований пошук і, тим самим, полегшити створення складових для композиції мережних сервісів. Стандарт BPEL забезпечує основу для ручної специфікації композиції мережних сервісів, використовуючи процедурну мову, яка забезпечує координування активностей мережних сервісів.

Більш потужні можливості мережних сервісів створюються шляхом залучення засобів DAML-S, OWL-S. Мета використання цих засобів полягає в забезпеченні зручних для читання машиною описів мережних сервісів, які дозволять автоматизувати пошук, ведення переговорів, ініціювання та виконання сервісів, здійснювати моніторинг сервісів у процесі їх активності. Мова OWL-S – мова онтологій, що використовується для опису мережних сервісів у термінах їх входів, виходів, передумов і умов отримання результатів, а також процесу виконання. Важливим в цьому стандарті є те, що OWL-S забезпечує формальний механізм для моделювання «реального світу» і опису того, як взаємодіють між собою окремі мережні сервіси. Стандартами також забезпечуються механізми для моделювання специфікації сервісів у нотації OWL-S. Модель існуючих стандартів мережних сервісів представляють шаровою структурою, яку показана на рис.1.

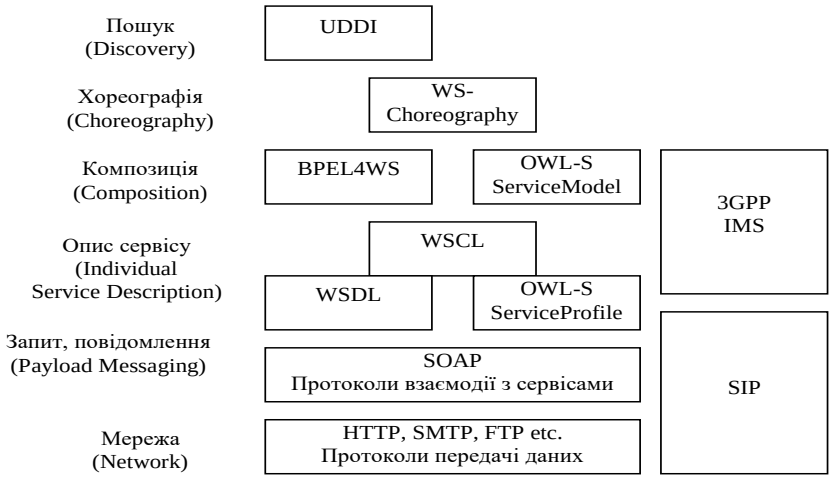


Рисунок 1 – Відкриті стандарти та засоби, що покладені в основу архітектури SOA

Мережні сервіси взаємодіють за допомогою передачі повідомлень у форматі XML з використанням типів. Стандарт SOAP використовується як протокол комунікації і підпису для мережних сервісів, які визначає стандарт WSDL. Функціональні описи мережних сервісів визначаються з використанням вищих горизонтальних стандартів, наприклад, таких як, BPEL, WSCL, BPML, OWL-S.

Модель сервісів, що викладена засобами WSDL, по суті не містить опису станів виконання сервісу. Стандарт WSDL 2.0 пропонує обмежену нотацію стану, яка дозволяє специфікувати визначені зразки повідомлень, які сервіс має задовольнити. Поки що внутрішній стан сервісу не визначається, але деяким режимам при виконанні сервісу потрібно контролювати цей стан (наприклад, щоб взаємодіяти коректно з іншими сервісами). Мова WSCL призначена для визначення вхідного та вихідного повідомлення сервісу, за

суттю є обмеженим кінцевим автоматом над азбукою типів повідомлень. Такий автомат у контексті сервісів називається розмовою.

Необхідно зазначити, що WSCL надзвичайно добре співпрацює з WSDL. Опис WSDL разом з переговорами сервісів WSCL використовують семантику сервісу, але тільки на період, коли зберігається стан внутрішнього виконання сервісу («короткою пам'яттю»).

Стандарти WSDL і WSCL тільки визначають мережні сервіси. Для композиції сервісів необхідна мова на відповідному рівні абстракції. Мова BPEL розроблена як для «ручного» програмування мережних сервісів, так і для їх специфікації. Ідентифікують дві топології сервісів: «peer-to-peer» – кожен з кожним, і «hub-and-spoke» – з медіатором (посередником). Медіатори – це сервіси-посередники, які забезпечують координацію активностей інших мережних сервісів. Первинна мета BPEL була такою, щоб забезпечити мову для конкретизації поведінки сервісу посередника, а не як засіб, що призначений для універсального програмування.

У противазі до BPEL, WS-хореографія намагається конкретизувати на глобальному рівні спосіб поведінки складових сервісів. WSCDL робить наголос на аспектах «хореографії»: ролі сервісів, інформації, що передається між сервісами, каналами, які забезпечують потоки інформації.

У вершині стандартів визначений стандарт UDDI, який забезпечує реєстрацію сервісів у різних застосуваннях. Сервіси, що зареєстровані, можуть бути знайденими, якщо їх реєстрація забезпечена цим стандартом.

Задачі та моделі композиції сервісів

Ідентифікують такі проблеми композиції сервісів

1. Координація мережних сервісів. Інфраструктура мережного сервісу задовольняє вимогам простої взаємодії мережних сервісів. Але для композитного сервісу та складних сервісних застосувань необхідно координувати послідовність операцій, що виконуються різними сервісами для того, щоб гарантувати коректне та надійне їх спільне виконання. Потрібні нові протоколи і абстрактні моделі, які забезпечать точну координацію сервісів. Необхідно забезпечити моделювання і спростити розробку композитних мережних сервісів у частині їх координації. У цьому напрямку спрямовані зусилля виробників на створення стандартів, наприклад, WS-координація фірми IBM або WS-CF фірми Sun.

2. Управління транзакціями взаємодії сервісів. Для реалізації схеми координації сервісів застосовують протоколи управління транзакціями (WS-транзакції), які забезпечують короткотривалі операції, які викликані атомарними процесами, такими, що забезпечують довготривалі операції, що викликані бізнес процесами. Проблема полягає у тому, що в разі виконання довготривалої операції не завжди можливо гарантувати такі властивості композитного сервісу як атомарність, цілісність і стійкість виконання операцій. У цьому сенсі необхідно розширити можливість протоколу транзакції. Наприклад, будувати WS-транзакції щодо схеми WS-координації для протоколів централізованої та однорангової транзакції.

Моделі активності сервісу описують приховані та явні транзакції між станами сервісу. Для моделювання транзакцій, використовуються властивості активації, які описують засоби запуску транзакцій, властивості операції які конкретизують результат аварійного завершення сервісу і властивості резервуваня ресурсів протягом даного часу.

У цьому напрямку розроблені абстрактні моделі активності сервісу та моделі завершення, вони містять операції компенсації дій у випадку аварійного завершення виконання. Наприклад, викликається функція, яка відміняє виконання сервісу або резервування ресурсу.

3. Контекст взаємодії сервісів. Термін контекст має багато визначень. Щодо мережних сервісів, контекст визначається як деяка додаткова інформація, яка використовується мережним сервісом або кількома сервісами, щоб забезпечити необхідну поведінку при виконанні сервісу. Контекст може містити інформацію, наприклад, ім'я користувача, адреса, розташування, пристрої, які використовуються, програмне забезпечення, засоби комунікації

тощо. Контекст може визначати середовище виконання сервіса та розширюватися новими типами інформації у будь-який час (динаміка середовища) без змін інфраструктури композитного сервісу. Стандарт WS конкретизує контекст у частині його сумісного використання сервісами та засоби управління контекстом.

4. Моделювання розмови. Модель розмови забезпечує динамічне зв'язування сервісів, створення схеми композиції сервісу, перевірку коректності композиції сервісу.

Для реалізації розмови мережних сервісів використовуються засоби WSCL (Web Services Conversation Language), WSCI специфікація (Web Service Choreography Interface), а також WS-координація і WS-транзакції. Розроблені абстракції моделюються взаємодії сервісів, наприклад, з використанням машин Миля. Взаємодія здійснюється через асинхронні повідомлення з підтримкою черг повідомлень.

5. Контроль за виконанням сервісів. Моніторинг. Засоби визначення стану композитного сервісу в процесі його виконання дають змогу втрутитися в процес виконання з метою забезпечення коректності та надійності виконання сервіса щодо зміни середовища. Відрізняють централізоване і розподілене виконання композиційних веб-сервісів. Централізоване виконання подібне парадигмі клієнт-сервер. У даному випадку сервер є центральний планувальник, який контролює процес виконання складових сервісів. Наприклад, засоби e-flow працюють за принципами централізованого планування.

Розподілена парадигма припускає, що зв’язані мережні сервіси розділяють контекст їх виконання. Кожний з хостів, на якому виконується сервіс, має власного координатора, який співпрацює з координаторами решти хостів, щоб гарантувати правильний порядок виконання складових сервісів. Використовується також гібридна форма, яка включає розподілену та централізовану парадигми управління. В цьому випадку сервіс може бути координатором, та контролювати не один, а набір композитних мережних сервісів.

6. Пошук мережних сервісів. Для пошуку мережних сервісів пропонуються моделі, засновані на обмеженнях основної моделі пошуку мережних послуг – UDDI. Стандарт UDDI містить тільки функціональні характеристики і в загальному випадку не повністю використовуються. Розширення існуючої моделі пошуку здійснюється шляхом додавання додаткових сутностей сервісу. В цьому випадку процес публікації, пошуку і зв'язування мережного сервісу такий самий, але збільшуються можливості пошуку. Коли користувач шукає сервіс, він може крім функціональних характеристик використати додаткову інформацію і отримати більш релевантний результат пошуку.

Модель специфікації сервісу містить тако ж якісні параметри сервісу, які використовуються для пошуку: маштабованість; ємність; потужність (час відповіді, затримка, пропускна здатність); надійність; гнучкість; виключення; точність; спосіб підтримки транзакцій; стандарти, що підтримуються; стабільність; вартість; повнота; безпека (аутентифікація, конфіденційність, можливість трасування, аудит, криптування даних, безвідкатність, тощо).

Якісні параменти сервісу орієнтовані на застосування, що побудовані на P2P архітектурах.

Соціальна мережа в середовищі Інтернет – це інтерактивний багатокористувацький веб-сайт, контент якого наповнюється самими учасниками мережі. Сайт являє собою автоматизоване соціальне середовище, що дозволяє спілкуватися групі користувачів, об'єднаних спільними інтересами. До них відносяться і тематичні форуми, особливо галузеві, які активно розвиваються останнім часом. В соціології – соціальна структура, що складається з групи вузлів, якими є соціальні об'єкти (спільнота, соціальна група, людина, особа, індивід).

Теорія соціальних мереж розглядає соціальні взаємовідносини в термінах вузлів та зв'язків. Вузли є відособленими акторами в мережах, а зв'язки відповідають стосункам між акторами. Може існувати багато типів зв'язків між вузлами. В найпростішій формі, соціальна мережа є відображенням всіх зв'язків, які мають відношення до дослідження, між вузлами. Мережі можуть використовуватись для встановлення соціального капіталу окремих акторів.

Ці концепції часто відображаються на діаграмі соціальної мережі, на якій вузлам відповідають точки, а зв'язкам – лінії.

Форма соціальної мережі допомагає визначити ступінь своєї корисності для її учасників. Менші, зв'язаніші мережі можуть бути менш корисними для своїх учасників, ніж мережі з багатьма слабкими зв'язками з особами ззовні від основної мережі. «Відкритіші» мережі, з багатьма слабкими зв'язками та соціальними взаєминами, вірогідніше будуть пропонувати нові ідеї та можливості для своїх учасників, аніж зачинені мережі з багатьма надлишковими зв'язками. Іншими словами, група знайомих друзів, які спілкуються лише один з одним вже володіють спільними знаннями та можливостями. Група осіб, із зв'язками з іншими соціальними спільнотами, вірогідно, отримуватимуть доступ до ширшого діапазону інформації. Для досягнення успіху, індивідам краще мати зв'язки з декількома мережами, аніж багато зв'язків в межах однієї мережі. Аналогічно, індивіди можуть впливати, або діяти в ролі брокера в середині своїх соціальних мереж з'єднуючи дві мережі, в яких відсутні безпосередні зв'язки (має назву заповнення соціальних дір).

Сила теорії соціальних мереж у її відмінності від традиційних соціологічних наук, згідно з якими вважається, що саме атрибути окремих акторів – дружність або недружність, рівень інтелекту, тощо – відіграють основну роль. У теорії соціальних мереж використовується інший погляд, коли атрибути окремих акторів менш важливі, аніж стосунки та зв'язки з іншими акторами в мережі. Цей підхід виявився корисним при поясненні багатьох реальних явищ, але залишає менше простору для індивідуальних дій, можливостей індивідів впливати на свій успіх, так як багато залежить від структури їхньої мережі.

Соціальні мережі, також, використовувались для дослідження того, як взаємодіють компанії, характеризуючи багато неформальних зв'язків, які поєднують між собою представників керівництв, а також асоціації та зв'язки між окремими робітниками в різних компаніях. Ці мережі дають можливості компаніям збирати інформацію, утримувати конкуренцію та, навіть, таємно змовлятись про встановлення цін або політик.

Першим веб-сайтом, який пропонував можливості роботи із соціальними мережами, був classmates.com, який з'явився в 1995 році. У слід за ним, в 1997 році з'явився sixdegrees.com. Починаючи з 2001 року почали з'являтись сайти, в яких використовувалась технологія під назвою «Коло друзів». Ця форма соціальних мереж, яка широко використовується у віртуальних спільнотах, набула широкої популярності в 2002 році та розквітнула з появою сайту Friendster. Наразі, існує більш ніж 200 сайтів з можливостями організації соціальних мереж. Популярність цих сайтів постійно зростала, і в 2005 році було більше переглядів сторінок сайту MySpace, а ніж сайту Google. Google також пропонує сайт з можливостями роботи із соціальними мережами orkut, який з'явився в 2004 році. Соціальні мережі почали розглядатись як складова Інтернет стратегії, приблизно в той самий час: в березні 2005, з'явився Yahoo! А в липні 2005 News Corportaion запустила MySpace. В цих спільнотах, спочатку, група перших користувачів надсилає запрошення членам власних соціальних мереж приєднатись до спільноти сайту. Нові члени повторюють цей процес, збільшуючи загальну кількість учасників та зв'язків в мережі. Сайти, також, пропонують такі можливості, як автоматичне оновлення адресних книг, перегляд особистої інформації один одного, утворення нових зв'язків за допомогою «служб знайомств» та інших форм соціальних зв'язків у мережі. Соціальні мережі також можуть організовуватись навколо ділових стосунків, як, наприклад, у випадку LinkedIn. Змішування мереж — це підхід до соціальних мереж, який комбінує особисті зустрічі та елементи комунікації в мережі. MySpace, наприклад, будується на основі незалежних музичних та святкових сцен, а Facebook віддзеркалює університетські спільноти. Нові соціальні мережі в Інтернеті все більше зосереджуються у певних галузях, наприклад, на мистецтві, спорті, автомобілях та навіть пластичній хірургії. Більшість із соціальних мереж в Інтернеті є публічними, дозволяючи будь-кому приєднатись. Деякі організації, такі як великі корпорації, також мають доступ до приватних служб соціальних мереж, наприклад Enterprise Relationship

Management. Вони встановлюють ці програми на власних серверах та надають можливість робітникам оприлюднювати свої мережі контактів та відносин із зовнішніми особами та компаніями.

Соціальні мережі вже давно захопили розуми звичайних користувачів Інтернету, і тепер прийшла черга бізнесу – вони фактично стали інструментом для бізнес-розвідки. Розмови про застосування даного інструменту в бізнесі велися досить давно, але впроваджувати подібні інновації не поспішали. Технології удосконалювалися, розмов ставало все більше, і це призвело до появи перших успішних прикладів. Одним з перших серйозних і цікавих прийомів стало впровадження соціальних мереж у бізнес-стратегію американської компанії Cisco Systems, Inc – лідера мережевих технологій для мережі Інтернет. Фахівці цієї компанії працюють в різних країнах світу, що неминуче викликає проблеми комунікації. Для передачі дуже важливої інформації співробітникам цієї компанії доводилося скликати дводенні конференції з необхідними фахівцями з різних країн, що, було дуже незручно і, найголовніше, вимагало значних грошових коштів. В результаті в рамках ініціативи Cisco 3.0 з'явилося рішення цієї проблеми – внутрішня корпоративна соціальна мережа, в якій містилася вся необхідна інформація і були закладені різні способи комунікації всередині компанії, що було особливо зручно співробітникам з різних країн. У цій соціальній мережі є внутрішні корпоративні блоги, навчальні матеріали, енциклопедії та інші елементи соціальних мереж. У тому ж 2007 році у cisco був відкритий «центр комунікаційної компетенції» (Communications Center of Excellence, CCoE) для допомоги співробітникам цієї компанії по використанню цієї соціальної мережі і всіх її переваг. Крім вирішення проблеми комунікації, соціальна мережа вирішує ще багато інших проблем, наприклад, з її допомогою співробітники активно спілкуються між собою, дізнаються про успіхи один одного, добре йде процес командоутворення і згуртування колективу. Ця компанія на своєму прикладі довела ефективність таких інструментів як соціальні мережі в різних бізнес-процесах. Це тільки один з перших кроків на шляху впровадження подібних інструментів у бізнес, як в цій конкретній компанії, так і в багатьох інших. Не можна забувати і про інше застосування соціальних мереж в бізнесі – це отримання інформації: про споживачів, про конкурентів, про працівників, про претендентів та про багато іншого.

Соціальними мережами називають також Інтернет-програми, які допомагають друзям, бізнес-партнерам або іншим особам спілкуватись та встановлювати зв'язки між собою використовуючи набір інструментів. Ці програми, відомі як «Онлайнові соціальні мережі», стають дедалі популярнішими. Багато людей не розуміють, що інформація, розміщена ними в соціальних мережах, може бути знайдена і використана ким завгодно, у тому числі не обов'язково з добрими намірами. Інформацію про учасників соціальних мереж можуть знайти їх роботодавці, батьки, діти, колишні або справжні дружини або чоловіки, збирачі боргів, злочинці, правоохоронні органи і так далі. Наприклад, відомий випадок, коли злочинниця шукала зовні схожих на себе жінок, вбивала їх і продавала їх квартири. Жінка розшукувала своїх двійників на сайті «Однокласники», «В контакті» та інших соціальних мережах. Майбутні жертви і не припускали, що їхня зовнішність стане для них страшним вироком. Збирачі боргів іноді використовують соціальні мережі, щоб знайти неплатників або отримати відомості про їхнє майно. Деякі роботодавці забороняють користуватися соціальними мережами – не тільки заради економії, а й щоб перешкодити витоку інформації.

Аналіз соціальних мереж перетворився на основний метод досліджень в сучасній соціології, антропології, географії, соціальній психології, інформатиці та дослідженні організацій, а також поширену тему для досліджень та дискусій. Дослідження в декількох академічних сферах показали, що соціальні мережі діють на багатьох рівнях, починаючи від родин, і закінчуючи цілими націями, та відіграють важливу роль в тому, як розв'язуються проблеми, працюють організації, та досягають успіху на шляху до власних цілей індивіди.

Підходи до аналізу та опису соціальної мережі

Соціальну онлайнову мережу можна розглядати як соціотехнічних об'єкт – в якому окремі учасники мережі – агенти з допомогою сукупності фізичної структури – комп'ютерів

учасників мережі – серверів каналів зв'язку і концентраторів реалізують свої потреби в спілкуванні, встановленні контактів, пошуку інформації, роботи, вирішують життєві завдання і замислюються над загальнолюдськими проблемами.

Якщо віртуальну соціальну мережу розглядати як фізичну систему – то для характеристики в ній процесів, що проходять, можливе застосовування відомих термодинамічних підходів і понять, такі як ентропія, енергія, робочі процеси.

Розглянуті нижче підходи можна віднести до системотехнічних, інтегральних, що дозволяє визначати соціальну мережу на основі ключових, основоположних понять і категорій теоретичної інформатики.

Серед можливих підходів до аналізу процесів соціальної мережі як соціотехничної системи можна вказати:

- Підхід теорії конфліктів і теорії ігор,
- Термодинамічний підхід,
- Гомеостатичні моделі.

Соціальна мережа як об'єкт моделювання

Класичний підхід до опису складної технічної системи передбачає ієрархію опису сукупністю вкладених моделей:

- Модель структури як сукупність елементів системи і зв'язків між ними.
- Функціонування або модель поведінки в часі.
- Модель ресурсів і цілій системі.

Якісні експертні оцінки і критерії

Соціальна мережа, як складний соціотехнічних об'єкт може оцінюватися як експертно, так і за допомогою деяких інтегральних, загальноприйнятих в техніці оцінок. Спостереження за процесами що відбуваються в соціальній мережі МойКруг дозволило сформулювати деякі підходи та оцінки. Скажімо, рівень «дорослості» обговорення в темах не викликає довіри.

Інший зовнішній критерій – рекомендована учасниками обговорення література та сайти. Наведу приклади. У під мереж «Інформаційні технології» - найбільш багатою і представницької – 6000 учасників, обговорюється 80 тем і 200 новин, «виставлено» 600 вакансій. Але навчальний відкритий ресурс Інтернет-Університету інформаційних технологій Шкред А.В. рекомендували своїм друзям – 100 чоловік. Ресурс «Віртуального комп'ютерного музею» Пройдакова Е.М. з півмільйоном відвідувачів – 3. В підрузі інтересів «Політика» заявлено 1500 учасників. Однак «Зіткнення цивілізацій» С. Хандінгтона – рекомендує прочитати тільки одна людина (і не будемо показувати пальцем). Такі логічні зв'язки в мережі можуть служити індикатором її якості.

Інтегральні термодинамічні показники

Соціотехнічну систему можливо охарактеризувати за допомогою поняття ентропія. Вперше термін був застосований Клаузіусом для позначення заходу деградації будь-якої системи. У процесах, що відбуваються без додаткового припливу енергії ззовні (ізоенергетичні процеси), зменшення внутрішньої енергії системи супроводжується пропорціональним збільшенням ентропії, і навпаки. Отже, ентропія є міра ймовірності фізичної системи, а її зростання – перехід від більшого порядку до меншого. Максимум ентропії досягається при рівноважному, найімовірніше стан системи. Закон зростання ентропії притаманний будь-якій ізольованій системі, наданій самій собі.

Для таких систем слід поміркувати більш докладно про закон зростання ентропії. У нашому випадку – випадку аналізу соціотехної системи має місце не просто ізольована система, а система з протидією і взаємообміном, тобто відкрита система.

Перший потік характеризує зростання ентропії як в будь-якій фізичній системі. Потужність цього потоку визначається градієнтом природного збільшення ентропії H_E. Елементи протиборства призводять до появи потоку ентропії, потужність якого визначається градієнтом штучного збільшення ентропії $H_и$. Величина цього градієнта може змінюватися в досить широких межах залежно від вирішуваних завдань (в залежності від цілей гри). Проте

ці межі не безмежні, а цілком кінцеві і визначаються інформацією (кількістю інформації) про протиборчих сторонах. Чим повніше інформація у гравця про своє противника, тим більшою мірою він може використовувати правило штучного збільшення ентропії.

А що ж перешкоджає зростанню ентропії? Перешкоджає зростання ентропії вільна енергія, отримана системою в процесі протиборства. Ця енергія (надлишок енергії) утворює потік «негативної ентропії», живість якого характеризується градієнтом H_O. Поява цього потоку рівносильна появі керуючого початку в у системі Р - Е, тобто рівносильна введенню в систему інформації. Чим більше цей керуючий початок, тим по більш жорстким законам діють протиборчі сторони, що призводить до зростання ймовірності досягнення мети гри.

Отже, ентропія системи Р - Е визначається сумою перерахованих вище потоків, тобто:

$$H_\Sigma = H_E + H_И + H_O$$

Якщо $H_E + H_И > H_O$, то взаємодія протиборчих супротивників швидко розпадається, що рівносильно нічийному результату. Якщо ж $H_E + H_И < H_O$, то система Р - Е може мати стаціонарний стан, тобто такий стан, коли відтік ентропії у зовнішнє середовище і приплив «негативної ентропіі» у вигляді вільної енергії (надлишків енергії) компенсує один одного. Саме в стаціонарному стані діють об'єктивні закони, за якими живе і розвивається система. Час життя системи в стаціонарному стані визначається величиною енергії (величиною надлишком енергії). Чим більше ця величина, тим більш тісно взаємодіють протиборчі сторони один з одним, тим більше ймовірно, що сторона, що має надлишкову енергію, вирішить протиборство на свою користь. У цих міркуваннях надлишкова енергія розуміється як негентропії, яка перешкоджає розпаду системи Р - Е, тобто утримує у взаємодії протиборчі сторони. Зауважимо, що необхідною умовою існування розв'язку гри є умова $H_O > 0$. Таким чином, якщо розглядати систему як термодинамічну, то тільки надлишки енергії (здатність здійснити роботу з утримання супротивників у взаємодії) є демпфером на шляху зростання ентропії. Саме ці надлишки енергії дозволяють в умовах лавиноподібного наростання ентропії вирішувати завдання гри із заданою вірогідністю.

Якщо все сказане має право на життя, то можна сформулювати один з принципів протиборства: яким би не був енергетичний запас динамічного об'єкта, який має ранг переслідувача, з часом він губиться, а це призводить до зростання ентропії системи Р - Е. Оскільки енергетичний запас завжди обмежений, то це в кінцевому рахунку не може перешкоджати зростанню ентропії в системі. Отже, чим більше час гри, тим менше шансів досягти успіху.

Розробка структурної схеми

Умовно підходи до композиції сервісів розділяються на два основних класи – статичний і динамічний. Статичний підхід до композиції є еквівалент ручної композиції, яка виконується на етапі проектування сервісу. Динамічні стратегії композиції мережних сервісів використовують час. Розрізняють п'ять категорій композиції: що орієнтується на модель і на бізнес-правила, декларативна, автоматична і семантичних веб-сервісів композиції;

Статична та динамічна композиція сервісів. Статична композиція використовується на етапі проектування, коли плануються архітектура і проект системи. Вибираються компоненти, які зв'язуються разом, \ далі вони компілюются і розгортаються для виконання. Такий підхід відмінно працює доти, доки компоненти сервісів не змінюются. Такі засоби як Biztalk фірми Microsoft і WebLogic фірми Bea – це приклади статичних засобів композиції.

Якщо бізнес-процеси зміюються, надають нові послуги або замінюють старі, можуть виникнути несумісні випадки. У такому разі, це веде до зміни архітектури програмного забезпечення й необхідності використовувати інші сервіси або навіть замінити систему. В ідеальному випадку процеси сервісу мають прозоро адаптуватись до середовища, яке змінюється, до вимог середовища та користувача з мінімальним ручним втручанням. Розвинутою платформою яка сфокусована на динамічну композицію сервісів є засоби Web Services Composition Platform фірми Sun, засоби e-flow фірми HP та інші.

Композиція сервісів, що заснована на моделях управління (Model driven service composition). Процесс розробки композитного сервісу можливо представити чотирма етапами: визначення сервісу, планування, конструювання, виконання. Початковою фазою визначення сервісу є абстрактна метамодель сервісу, яка моделює компоненти сервісу та відношення між ними. Цілями такого моделювання є вибір елементів композитного сервісу та правил їх композиції. Далі композиція сервісу зосереджується на формуванні моделі управління потоками робіт.

Композиція сервісів, яка заснована на бізнес-правилах. Вона визначається шляхом додавання бізнес-правил, що регламентують: перед- та після- умови; опис подій, що мали місце при виконанні процесів композиції сервісу; потоку процесів; визначення та блокування активностей; визначення повідомлень, що містять вхідну та вихідну інформацію; опис ролей у процесі композиції сервісів. Правила композиції сервісів можливо моделювати з використанням мови OCL (Object Constraint Language). Бізнес-правила можна класифікувати таким чином: структурні правила для формування процесів та структури; правила для планування пріоритету процесів у композиції; правила управління даними та повідомленнями; правила поведінки для управління процесами та забезпечення цілісності композитного процесу; правила використання ресурсів, вибору сервісів, провайдерів; правила для визначення виключень у поведінці сервісів; правила ролей для управління учасниками, залученими у сервісі; правила повідомлення для регулювання використовування інформації; правила для управління поведінкою композиції сервісу відповідно щодо очікуваних або непередбачених подій та інші.

Для опису абстракції високого рівня використовують мову UML (Unified Modelling Language), яка забезпечує опис бізнес-процесів, засоби підключення до інших стандартів, таких як BPEL4WS. Для формування бізнес-правил та опису потоку процесів використовується мова OCL, засобами якої описуються умови вибору сервісів та їх зв’язування, формування структури композитного сервісу і формування плану композиції сервісу.

Декларативна композиція сервісів. Більшість підходів засновані на тому, що спочатку мають бути створені бізнес-процеси. Декларативний підхід суттєво відрізняється від підходів, що засновані на бізнес-правилах та має дві фази: початкова фаза полягає в визначенні цілей композиції та конструювання планів для кожної цілі. Наступна фаза полягає у тому, що для кожного плану здійснюється пошук відповідних сервісів та будується схема потоку робіт. Перша фаза реалізується на основі PDDL (Planning Domain Definition Lenguage) та засобів XML Web services Request Language, які мають забезпечити машино читані семантичні об’єкти та специфікацію абстракції поведінки сервісу. Наступна фаза може бути реалізована на основі існуючих мовних засобів моделювання таких як BPEL.

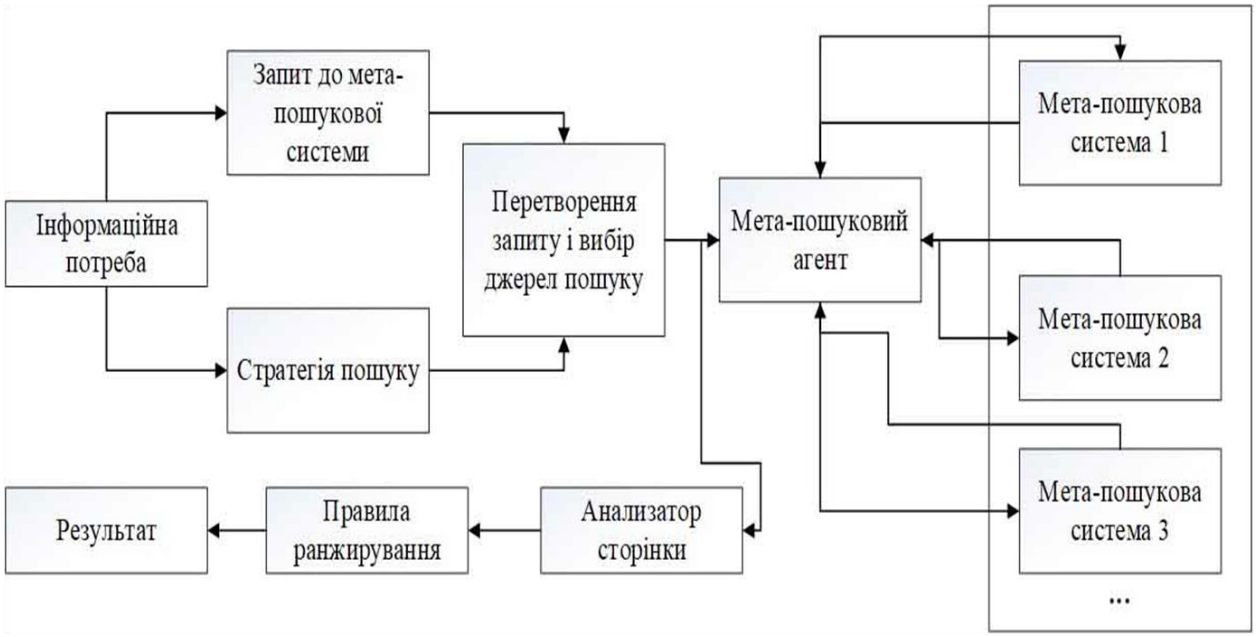


Рисунок 2 - Структурна схема системи

З точки зору архітектури декларативний підхід потребує перегляду концепції опису сервісів та реєстру сервісів. Наприклад, засоби WSDL не забезпечують опис необхідних атрибутів сервісу, а засоби UDDI не містять інформацію про те, що робить сервіс. Цільовий, або декларативний підхід забезпечується мовою опису композитного сервісу, яка відображає запити користувачів, визначає нові типи ресурсів, функції та їх відносини на основі унікальних імен URI. Для реалізації такого підходу необхідно розробити модель координації сервісів та універсальний протокол взаємодії.

Автоматична композиція сервісів. На відміну від ручної композиції сервісів, автоматична композиція потребує використання онтологій [11]. Відповідно щодо сервісів, онтологія визначається, як множина об'єктів, які розділяють ту ж саму предметну область, та правила, за якими сервіси можуть бути описані та доступні. Онтологічні мови, такі як RDF, DAML-S (DARPA Agent Markup Language for Web services), DAML+OIL, або OWL (Ontology Web Language) забезпечують формальні специфікації і можуть описувати значення для складних класів властивостей. Засоби DAML-S забезпечують механізм для онтологічної організації сервіса. В якості типів онтологій, необхідних для композиції сервісів є такі: метрик, одиниць виміру, одиниць коштів, властивостей, методів та інші.

Метою даної автоматизованої системи є підвищення оперативності та продуктивності процесу моніторингу сегменту веб-середовища (соціальної мережі) на базі методів Data Mining (дескриптивний, кореляційний та регресійний аналіз).

Для реалізації поставлених цілей система повинна відповідати наступним структурним вимогам:

–Система має проводити моніторинг (стеження, контроль, виявлення закономірностей) зовнішніх і внутрішніх інформаційних ресурсів у форматі PDF, що знаходяться у соціальних мережах та інших сегментах Інтернет.

–Система має відбирати джерела інформації за критеріями, що вказані авторизованими користувачами (наприклад, соціальні мережі УАнету; форуми, де основною мовою є українська тощо).

–Система має здійснювати спеціальну фільтрацію інформації, відкидаючи неінформативні, недоступні чи підозрілі джерела інформації (Фільтри створюються адміністратором, який формує «стоп-перелік» джерел інформації, доступ до яких потребує передплати, реєстрації, містить лише метадані щодо документів і т.д., а також програмними

застосуваннями, що не дозволяють видавати посилання на неіснуючі документи, або переправляють посилання до кешу системи, де цільові документи вже розміщені у результаті опрацювання попередніх запитів).

–Система має узагальнювати інформацію за рахунок використання правил асоціацій для знаходження закономірностей між зв'язаними подіями та даними у базах даних.

–Система має виконувати реферування інформації, тобто створювати короткі викладки матеріалів, анотації або дайджестів (отримання найважливіших відомостей з одного або з декількох документів та генерація на їх основі лаконічних та інформаційно-насичених звітів) методом квазіреферування чи іншим методом аналітико-синтетичної обробки інформаії.

–Система має виконувати категоризацію інформації, використовуючи ключові слова (якщо інформація представлена іншою мовою, то здійснюється переклад ключових слів іншими мовами, а потім відбувається класифікація документів за тематиками).

–Система має виконувати кластеризацію інформації на базі відповідних моделей. Моделі кластеризації використаються для класифікації об'єктів, за умови, що набір цільових класів невідомий; вони створюють так називані сегментовані моделі.

–Система має виконувати ранжирування інформації. Основним критерієм ранжирування інформації в сучасній метапошуковій системі має бути рейтинг пошукових систем. Якщо посилання на один і той же PDF-документ було отримано з різних пошукових систем, то вибирається те з них, яке містить найбільш повний опис.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів аналізу технології Data Mining. Розроблені під час виконання роботи алгоритми дозволяють успішно вирішувати завдання аналізу додатків рівня технології Data Mining. 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. При створені програмного забезпечення було використано об’єктно-орієнтований підхід, що відповідає сучасним тенденціям у галузі розробки комерційних програмних систем.

Список літератури

1. Андон П., Дерецький В. Проблеми побудови сервіс-орієнтованих прикладних інформаційних систем в semantic web середовищі на основі агентного підходу // Проблеми програмування. –2006. –№ 2–3. – Р. 493-503.
2. Архипенков С.Я. Аналитические системы на базе Oracle Express OLAP. - М.: Диалог - МИФИ, 2000. - 320 с.
3. Додонов А.Г., Ландэ Д.В. Методы и средства мониторинга, адаптивного агрегирования и обобщения информационнных потоков // Информационные технологии и безопасность. Проблемы научного и правового обеспечения кибербезопасности в современном мире. Материалы международной научной конференции ИТБ-2011. – К.: ИПРИ НАН Украины, 2011. – С. 6-9.
4. Додонов А.Г., Ландэ Д.В., Жигало В.В. Сетевые информационные потоки как содержательная составляющая информационно-аналитических систем // Реєстрація, зберігання і обробка даних, 2010. – 12. – № 1. – С. 39-48.
5. Додонов О.Г., Ланде Д.В., Путятін В.Г. Інформаційні потоки в глобальних комп'ютерних мережах. – К: Наукова думка, 2009, – 295 с.
6. Додонов О.Г., Путятін В.Г., Валетчик В.О. Інформаційно-аналітична підтримка прийняття управлінських рішень // Реєстрація, зберігання і обробка даних. – 2005. – 7.– № 2. – С. 77-93.
7. Дюк В.А. Data Mining – интеллектуальный анализ данных. http://www.olap.ru/basic/dm2.asp.
8. Дюк В.А. Data Mining – состояние проблемы, новые решения. http://www.inftech.webservis.ru/database/datamining/ar1.html.
9. Корнеев В.В. и др. Базы данных. Интеллектуальная обработка информации. - М.: Нолидж, 2000. - 352 с.
10. Ландэ Д.В., Снарский А.А., Жигало В.В. Метапоиск доступных научно-технических документов в Интернет // Труды 12й Всероссийской научной конференции «Электронные библиотеки: перспективные методы и технологии, электронные коллекции» – RCDL'2010, Казань, Россия, 2010. – С. 321-325.
11. Berardi D., Calvanese D., De Giacomo G., Hull R., and Mecella M. Automatic Composition of Transition-based Semantic Web Services with Messaging // Technical report, University of Rome, ”La Sapienza”, Roma.— Italy: 2005, April. – P. 613–624.

УДК 004

О. Майборода, магістр гр. КІ-19М-1,4
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ КОНТРОЛЮ РОБОТИ КОРИСТУВАЧА ПЕРСОНАЛЬНОГО КОМП`ЮТЕРА

У статті розроблено програмне забезпечення, яке призначено для системи контролю роботи користувача персонального комп`ютера. Метою розробки є дослідження та програмна реалізація системи контролю роботи користувача персонального комп`ютера. Об'єктом дослідження є процес контролю роботи користувача персонального комп`ютера. Предметом дослідження є методи контролю роботи користувача персонального комп`ютера. Методи дослідження базуються на методах захисту інформації, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи контролю роботи користувача персонального комп`ютера. 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, контроль роботи користувача

Постановка проблеми. На сучасному етапі розвитку інформаційних технологій практично жодне робоче місце не обходиться без персонального комп'ютера (ПК). При цьому проблеми адміністрування і нагляду керівництва за роботою підлеглих є дуже актуальними. Перевірити, чи користувач завантажений на 100%, чи ефективно використовується ПК, скільки часу використовується користувачем нераціонально (спілкування в Інтернеті, запуск ігор, відвідування сайтів у власних потребах, тощо) є на сьогодення нагальною проблемою керівників об'єктів будь-якої сфери діяльності та форми власності. Не секрет, що в умовах ринкової економіки підприємства прагнуть скоротити свої витрати і збільшити прибуток, підвищити трудову дисципліну на робочих місцях, що дозволить і краще збереження корпоративних даних, розташованих на ПК. Отже, написання програмного продукту, що ефективно реалізує вище описані задачі, є дійсно актуальним завданням. Контроль роботи персоналу за комп'ютером кадровим співробітником, який веде облік відпрацьованого часу, збирає і обробляє інформацію, є методом неточним, так як в цьому процесі присутній людський фактор. Адже співробітник може помилятися, чи не встигати обробляти великі обсяги інформації, спізнюватися зі звітами. Крім того, відстежити всі дії співробітників за комп'ютерами просто неможливо.

Спостереження за допомогою спеціальної програми, встановленої прямо на робочі комп'ютери, є досить зручним і надійним вирішенням вище окресленої проблеми. Таке програмне забезпечення буде не тільки вести контроль за витратою часу, але і фіксувати порушення, перелік документів з якими саме працюють співробітники, формувати звіти результатів контролю за будь-який термін часу.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи контролю роботи користувача персонального комп`ютера.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи контролю роботи користувача персонального комп`ютера.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем контролю роботи користувача персонального комп`ютера.

– Дослідження системи контролю роботи користувача персонального комп`ютера.

– Програмна реалізація системи контролю роботи користувача персонального комп`ютера.

Об'єктом дослідження є процес контролю роботи користувача персонального комп`ютера.

Предметом дослідження є методи контролю роботи користувача персонального комп`ютера.

Методи дослідження базуються на методах захисту інформації, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Архітектуру системи, що підлягає розробці в процесі виконання МР, доцільно організувати на основі сучасних комп'ютерних технологій, коли апаратні засоби та ПЗ існують в формі неподільного апаратно-програмного комплексу, кожний компонент якого повинен виконувати свою окрему, притаманну тільки йому, функцію.

Тому весь цикл розробки МР, використавши методику декомпозиції, розподілимо на послідовність трьох фаз проектування:

1) аналіз задачі вибору/розробки апаратних засобів;
2) розробка прикладного ПЗ;
3) комплектування апаратних засобів та ПЗ в прототип системи та його налаштування.

Разом з тим, перш ніж приступити до розробки механізма архітектури та конфігурації майбутньої системи, визначимо технічні вимоги, обмеження, які вона повинна виконувати та задовольняти в процесі експлуатації.

Визначимо режими роботи системи, що підлягає розробці:

– функція збирання і обробки результатів моніторингу ведеться безперервно і по бажанню відповідальної особи, результати моніторингу виводяться на екран ПК;

– функція передачі і одержання даних відбувається синхронно процесу моніторингу.

Ці функції підлягають розробці в процесі реалізації МР.

Однією з основних задач, що має бути розробленою в процесі виконання МР, є розширення стандартної архітектури «Клієнт-Сервер» шляхом введення до її складу багатопоточного сервера додатків. Сьогоднішні додатки «Клієнт-Сервер» так мало схожі на своїх попередників, що їм надано нове ім'я – багаторівневі додатки, або n-рівнева архітектура.

В таких системах обробка інформації розподіляється між клієнтом та сервером, а бізнес-логіка сконцентрована на окремому рівні системи. Саме цей рівень і буде предметом нашої розробки, оскільки дозволить реалізувати поставлені ТЗ задачі щодо прийняття з мережі та передачі на сервер результатів моніторингу роботи користувачів ПК.

Окрім цього, для роботи системи необхідна база даних (БД), до якої будемо надавати пріоритетний доступ клієнтів, адже в процесі роботи системи по виконанню поставлених задач виникає постійна необхідність в збереженні та обробці службової інформації.

В нашій розробці доцільно використати реляційну БД, в якій об'єкти та зв'язок між ними представляються у вигляді плоских прямокутних таблиць з рядків та стовпчиків.

Для зберігання даних використовуємо БД-SQLite 3 версії, це система керування базами з відкритим кодом, а для звернення клієнтів до БД Quick SQL-запити.

Особливістю SQLite є те, що вона не використовує парадигму клієнт-сервер, тобто рушій SQLite не є окремим процесом, з яким взаємодіє додаток, а надає бібліотеку – QtSql, з якою програма компілюється і рушій стає складовою частиною програми. Таким же чином, в якості протоколу обміну, використовуються виклики функцій (API) бібліотеки SQLite. Це дозволить зменшити накладні витрати, час відгуку і спрощує програму.

В попередніх розділах пояснювальної записки ми вже частково розглянули задачу організації роботи ПК в мережі, яка фактично зводиться до рішення задачі моніторингу додатків ОС Windows, та дійшли висновку, що моніторинг є украй важливою задачею в різноманітних ситуаціях: починаючи від виявлення несанкціонованої роботи користувачів в мережі і закінчуючи простим стеженням за системою для подальшого вивільнення системних ресурсів.

Система що підлягає розробці, повинна забезпечити повною мірою отримання системи адміністратором/відповідальною особою, усього обсягу необхідної інформації по використанню ПК користувачами, які працюють в глобальній мережі.

До цієї інформації віднесемо наступне:

1) час початку роботи користувача на ПК;
2) час завершення роботи користувача на ПК.

Таким чином, в процесі розробки ПЗ системи необхідно забезпечити реалізацію наступних основних функціональних можливостей:

1) спеціально розроблений модуль повинен забезпечити моніторинг додатків;
2) виведення системному адміністратору/відповідальній особі подробиць про той або інший процес на основі одержаної в процесі моніторингу детальної інформації про нього (вміст процесу).

Для того, щоб забезпечити виконання визначених функцій системою, необхідно в першу чергу вирішити основну задачу по організації моніторингу відкритих додатків на ПК користувачів в мережі. Це дозволить в повному обсязі виявити активність користувачів при їх роботі на ПК. Визначимо більш детально функції кожного з цих механізмів.

Механізм моніторингу додатків дозволить виявити та контролювати час запуску і закриття додатку та час переключення між додатками, тобто – всі аспекти, які характеризують роботу користувача ПК.

Означені механізми моніторингу при побудові системи планується реалізувати окремим модулем власної розробки.

SQLite зберігає всю базу даних (включаючи визначення, таблиці, індекси і дані) в єдиному стандартному файлі на тому комп'ютері, на якому виконується додаток. Простота реалізації досягається за рахунок того, що перед початком виконання транзакції весь файл, що зберігає базу даних, блокується; ACID-функції досягаються, зокрема, за рахунок створення файлу-журналу.

Кілька процесів або потоків можуть одночасно без жодних проблем читати дані з однієї бази. Запис в базу можна здійснити тільки в тому випадку, коли жодних інших запитів у цей час не обслуговується; інакше спроба запису закінчується невдачею, і в програму повертається код помилки. Іншим варіантом розвитку подій є автоматичне повторення спроб запису протягом заданого інтервалу часу.

У комплекті постачання надається також функціональна клієнтська частина у вигляді виконуваного файлу sqlite3, за допомогою якого демонструється реалізація функцій основної бібліотеки. Клієнтська частина працює з командного рядка, і дозволяє звертатися до файлу БД на основі типових функцій ОС. А завдяки архітектурі рушія можливо використовувати SQlite як на вбудовуваних системах, так і на виділених машинах з гігабайтними масивами даних.

Створення та обслуговування БД буде здійснюватися через текстову консоль SQL-командами або через спеціальні інструменти, у тому числі-через графічний інтерфейс користувача.

Таблиці БД клієнтів та правил зображені на рисунку 1.

Предметною областю БД є клієнти та перелік дозволених до запуску програм.

Користуватись БД може тільки адміністратор. Основні види запитів:

1) занесення й одержання інформації про клієнтів;
2) занесення й одержання інформації про дозволені до запуску програми;

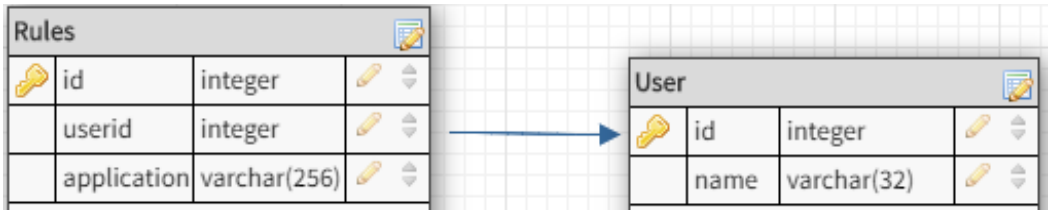


Рисунок 1 – Скриншот таблиць бази даних MP

До складу структури системи необхідно також ввести інтерфейс користувача, який є сукупністю засобів і правил, що забезпечують взаємодію пристроїв, програм і людини.

У сучасних комп'ютерних технологіях найбільше поширеним є три типи інтерфейсів: командний, WIMP, SILK. Розглянемо та проведемо аналіз цих типів:

1. Командний інтерфейс, при якому взаємодія людини з комп'ютером здійснюється шляхом подачі комп'ютера команд, які він виконує і видає результат користувачеві. Командний інтерфейс реалізується у вигляді технології командного рядка.
2. WIMP (window, image, menu, pointer) – інтерфейс. Характерною рисою цього інтерфейсу є те, що діалог користувача з комп'ютером ведеться не за допомогою командного рядка, а за допомогою вікон, графічних образів меню, курсору і інших елементів. Хоча в цьому інтерфейсі подаються команди машині, але це робиться через графічні образи.
3. SILK (speech, image, language, knowledge) – інтерфейс. Цей інтерфейс найбільш наближений до звичайної людської форми спілкування. У рамках цього інтерфейсу йде звичайна розмова людини і комп'ютера. При цьому комп'ютер сам визначає для себе команди, аналізуючи людську мову і знаходячи в ній ключові фрази. Результати виконання команд він також перетворює в зрозумілу людині форму: голосове повідомлення, виведення повідомлення на екран ПК, виведення повідомлення на принтер, тощо.

Для забезпечення діалогу між програмою та користувачем, для програмного додатку, вирішено використати найпоширеніший тип інтерфейсу користувача – WIMP, характеристики якого повністю задовольняють вимоги до системи.

Для того, щоб полегшити побудову структури інтерфейсу функціональні можливості було розподілено на наступні інструменти:

1) кнопки управління записом;
2) елементи відображення запущених додатків;
3) елементи для відображення, раніше записаних файлів;
4) список підключених ПК;
5) елемент введення команд.

Інтерфейс програми моніторингу дій користувача ПК планується реалізувати по Т-подібній структурі, програмний додаток складається з одного головного вікна, в якому містяться всі необхідні елементи керування.

Його планується розробити за допомогою Windows Forms з використанням наступних компонентів:

1) Button – кнопка;
2) Label – текстова інформація;
3) TextBox – поле введення текстової інформації;
4) OpenFileDialog – діалог відкриття файлів;
5) RichTextBox – область виведення вмісту файлів;
6) DataGridView – таблиця;
7) ToolStripButton – кнопка панелі інструментів;
8) ContexMenuStrip – контектсне меню;
9) NotifyIcon – піктограма трею.

Діалогові вікна будуть відображаютись тоді, коли програмі для подальшої роботи потрібна відповідь. На відміну від звичайних вікон, більшість діалогових вікон не можна розгорнути або згорнути, так само як і змінити їх розмір. Проте їх можна переміщувати. Для

налаштування процесу моніторингу, буде розроблено діалогове вікно, на якому розміститься всі необхідні налаштування для забезпечення роботи системи по виконанню функцій ТЗ і збереження її результатів в файл.

Для того, щоб воно не заважало під час самого запису, його можна викликати будь-коли за допомогою головного меню або спеціальної кнопки на панелі інструментів. Завдяки відповідній піктограмі на кнопці, вона є зрозумілою для користувача і через те, що не вимагає письмового пояснення, займає мало місця.

Таким чином, визначивши та виконавши опис функціонування системи, означивши основні складові її архітектури переходимо до побудови архітектури системи та розробки її структурної схеми.

Розробка структурної схеми

Перед початком проектування МР необхідно визначити основні структурні складові частини системи та зв'язок між ними, означити які моделі ввійдуть до складу системи, означити які з них запозичені, а які підлягають розробці в процесі МР.

Структурна схема ПЗ системи контролю дій користувача ПК, зображена на рисунку 2, складається з двох частин:

– Частина 1: клієнт.

– Частина 2: сервер.

Згідно з ТЗ та постановки задачі, система повинна забезпечувати виконання наступних функцій:

1) встановлення з'єднання через сокет 7007 по протоколу TCP\IP з сервером;
2) прийом файлу з переліком дозволених на запуск програм від серверу;
3) запис списку дозволених до запуску програм в розділ регістру RestrictRun;
4) створення списку запущених процесів користувача;
5) визначення часу роботи з програмою та запис даних до журналу роботи користувача;
6) перехоплення трафіку за допомогою RAW-сокета;
7) фільтрація власних IP-адрес;
8) перетворення IP-адреси в назву сайту та запис його до журналу роботи користувача;
9) передача за вимогою серверу та по завершенню роботи клієнта, журналу роботи користувача;
10) створення БД для списку клієнтів та правил запуску програм;
11) встановлення та перевірка зв'язку сервером з усіма клієнтами;
12) збереження журналів роботи до лог-файлів.

Система буде мати архітектуру яка складається з 2-х змістовних частин:

Частина 1: «Клієнт», до складу якої ввійдуть наступні модулі:

1) server socket – забезпечить встановлення каналу зв'язку з сервером;
2) список дозволених програм – містить назви програм, дозволених до запуску;
3) register file – створення розділу RestrictRun в реєстрі Windows і запис вмісту списку дозволених програм;
4) таймер – забезпечить період спрацьовування 1 секунда;
5) визначення часу роботи з програмою;
6) журнал роботи – веде записи про час роботи з програмами;
7) IP-протокол;
8) raw-сокет – надає повний доступ до IP-пакетів;
9) аналізатор трафіку – виконує перехоплення IP-пакетів;
10) фільтр пакетів з власним IP – для визначення відвіданих IP-адрес;
11) перетворення IP в ім'я – запит на визначений IP з поверненням назви сайту;

Частина 1: «Клієнт», до складу якого ввійдуть наступні модулі:

1) база даних SQLite – використовується для зберігання списку клієнтів та програм, дозволених до запуску.

2) GUI включає в себе форми в які виводиться інформація, отримана від клієнта.

3) Client socket – для встановлення зв'язку з списком клієнтів.

Окрім цього, до складу структурної схеми треба ввести допоміжну частину, тобто набір протоколів для організації взаємодії клієнтської та серверної частини системи. Для утворення передачі даних через мережу WAN використаємо наступні протоколи: TCP/IP, сокетну технологію. Це дозволить передавати дані з великою швидкістю та уникнути їх втрати.

Для сховища даних використаємо СУБД SQLite. Це забезпечить надійне зберігання інформації та простий спосіб запису і читання даних за допомогою мови запитів Quick SQL.

Для забезпечення:

– коректної роботи усіх модулів та системи в цілому;

– в повнму обсязі функціонування розробленого ПЗ, необхідна наступна конфігурація ПК:

– процесор з частотою 1 ггц (або швидше);

– оперативна пам'ять 2 гб;

– операційна система Windows 10 (64-бітової версії);

– жорсткий диск обсягом 100 гб.

До всіх визначених рішень основних робочих функцій, додаємо наступне:

1) ПЗ системи повинне мати модульну структуру побудови, що дозволить легко адаптувати його під будь-яку конфігурацію ПЗ на ПК та без суттєвих доробок перейти на новий тип ПК;

2) без суттєвих доробок та перебудови структури розширити її функції шляхом введення нових модулів;

3) графічний інтерфейс повинен відповідати вимогам ергономіки, бути зручним та україномовним;

Фактично залишилось визначити, які модулі будуть запозичені, а які підлягають розробці в процесі виконання МР:

1) запозичено: register file, IP-протокол, СУБД SQLite;

2) всі інші модулі, які зображені на структурній схемі на рисунку 2, підлягають розробці.

Таким чином, нами визначені складові ПЗ, компоненти системи, тому можемо приступити до розробки структурної схеми (рисунок 2).

Клієнтська програма не має інтерфейсу і завантажена в операційній системі в режимі Service.

Після отримання від серверу списку дозволених до запуску програм, вони записуються в файл налаштувань та реєстр Windows до розділу RestrictRun.

Основну роботу клієнтського ПЗ виконує таймер, який після спрацьовування з інтервалом в 1 секунду, створює список запущених процесів – визначає час запуску або завершення певного процесу та записує це до журналу.

Інший таймер з періодом в 10 хвилин порівнює файли реєстру з файлом налаштувань та перезаписує список дозволених до запуску програм в разі їх зміни в файлі реєстру.

Також в ПЗ присутній моніторинг відвіданих інтернет-ресурсів, який реалізований через сніфер. Для того, щоб отримати прямий доступ до IP-пакету, створюється RAW-сокет. Після цього за допомогою сніфера йде цикл захоплення

IP-пакетів. Всі захоплені IP-пакети фільтруються і залишаються тільки ті, які містять IP-адресу клієнта, це означає, що саме цей сайт відвідував клієнт. Наступною дією йде перетворення IP-адрес у всім зрозумілу назву сайту, яка записується до журналу клієнта.

По завершенню роботи клієнт передає запит прийому журналу на сервер.

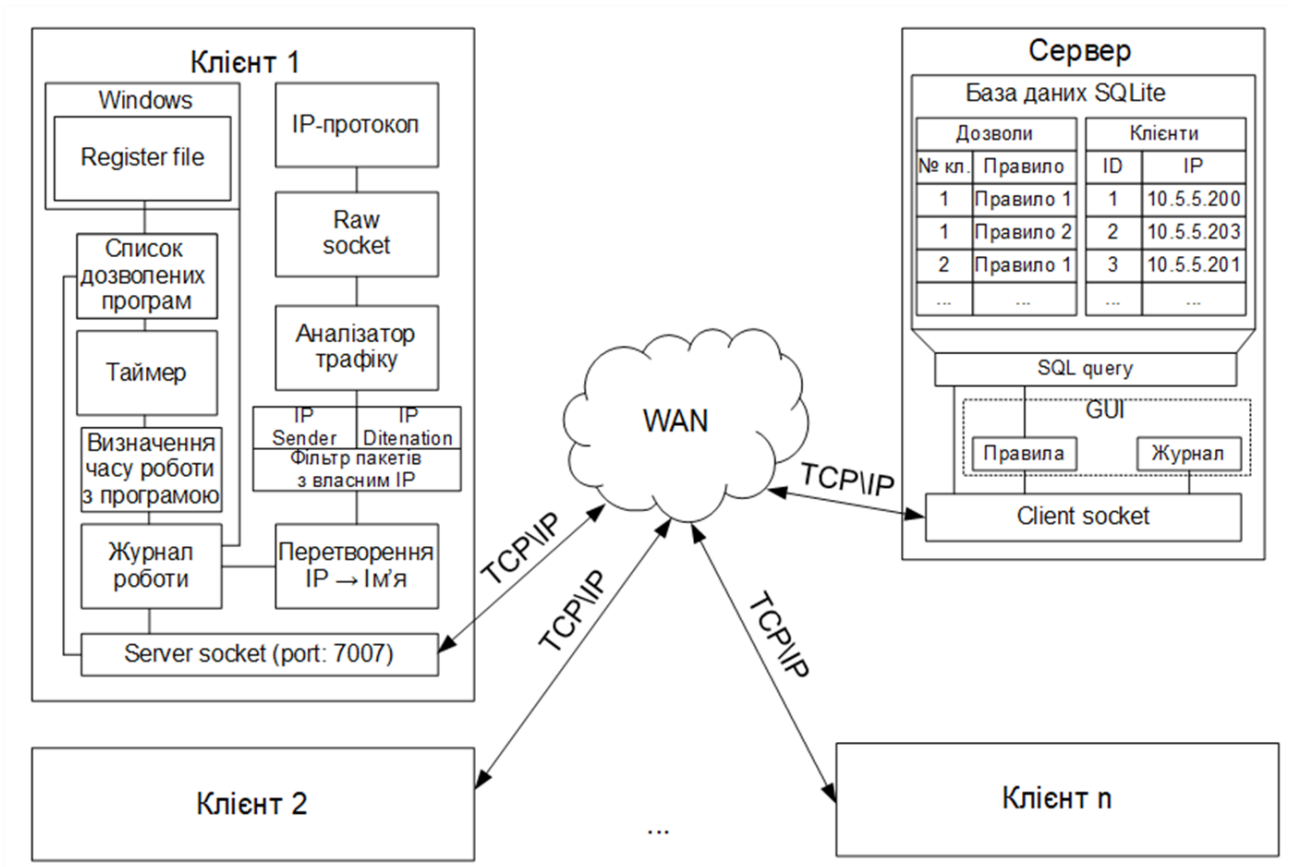


Рисунок 2 – Структурна схема системи контролю дій користувача ПК.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів контролю роботи користувача персонального комп`ютера. В межах України в недостатній мірі представлені вітчизняні розробки в цій області. У роботі наведені теоретичне узагальнення й рішення наукового завдання дослідження методів контролю роботи користувача персонального комп`ютера. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем контролю роботи користувача персонального комп`ютера; Досліджена система контролю роботи користувача персонального комп`ютера; На основі отриманих результатів досліджень створена програмна реалізація системи контролю роботи користувача персонального комп`ютера. Розроблені під час виконання роботи алгоритми дозволяють успішно вирішувати завдання контролю роботи користувача персонального комп`ютера. 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. 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 IT-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 (ІТ & І): 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

Л. Марченко, магістр гр. КІ-19М-1,4
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ РОЗГАЛУЖЕНОЇ СИСТЕМИ ВІДЕОСПОСТЕРЕЖЕННЯ НА ОСНОВІ БЕЗДРОТОВИХ КАМЕР І КАНАЛІВ LTE

У статті розроблено програмне забезпечення, яке призначено для розгалуженої системи відеоспостереження на основі бездротових камер і каналів LTE. Метою розробки є дослідження та програмна реалізація розгалуженої системи відеоспостереження на основі бездротових камер і каналів LTE. Об'єктом дослідження є процес відеоспостереження на основі бездротових камер і каналів LTE. Предметом дослідження є методи відеоспостереження на основі бездротових камер і каналів LTE. Методи дослідження базуються на методах обробки відеоданих, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація розгалуженої системи відеоспостереження на основі бездротових камер і каналів LTE.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, відеоспостереження, LTE

Постановка проблеми. Сучасні мережні відеокамери мають убудовані функції відеоаналітики, а програмне забезпечення, здатне вирішувати різноманітні завдання відеоспостереження, містить у собі системи моніторингу й керування записом, а також відеоклієнти з підтримкою різних пристроїв. Сама система відео спостереження – один з найбільше швидкозростаючих сегментів світової галузі ІТ. Системи відеоспостереження впроваджуються на транспорті, у комунальному господарстві, готельній галузі,

промисловості, держустановах, спортивних і розважальних центрах, у комерційних організаціях. Вони використовуються для рішення завдань бізнесу й забезпечення безпеки. По оцінках аналітиків IHS, в 2019 році обсяг світового ринку відеоспостереження становив 13,5 млрд доларів, причому мережне відеоспостереження переважало над аналоговим – зараз біля половини продажів доводиться на мережне відео. Як очікується, до 2021 року частка останнього перевищить три чверті ринку, а його сукупний обсяг збільшиться до більш ніж 24 млрд доларів. Середньорічні темпи росту можуть досягти 22% по мережному відеоспостереженню й 12% по ринку відеоспостереження в цілому. По даним Intel, світовий ринок IP-відеоспостереження росте в середньому на 24% у рік, ще швидше зростає обсяг генеруємих цими системами даних.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні розгалуженої системи відеоспостереження на основі бездротових камер і каналів LTE.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація розгалуженої системи відеоспостереження на основі бездротових камер і каналів LTE.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

1. Огляд існуючих систем відеоспостереження на основі бездротових камер і каналів LTE.
2. Дослідження розгалуженої системи відеоспостереження на основі бездротових камер і каналів LTE.
3. Програмна реалізація розгалуженої системи відеоспостереження на основі бездротових камер і каналів LTE.

Об'єктом дослідження є процес відеоспостереження на основі бездротових камер і каналів LTE.

Предметом дослідження є методи відеоспостереження на основі бездротових камер і каналів LTE.

Методи дослідження базуються на методах обробки відеоданих, методах математичної статистики,методах розробки програмного забезпечення.

Виклад основного матеріалу. Розглянемо наступну класифікація продуктів. Всю продукцію систем відеоспостереження умовно можна розділити на 3 типи.

Тип 1 – IP відео спостереження. 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.

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 свій 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.

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.

На сьогоднішній день люди намагаються захистити себе, своє рідне й близьких, а також своє майно від грабіжників і злочинців. Відеоспостереження встановлюють практично скрізь: в офісах, з метою контролю за неретельними працівниками, у магазинах, з метою запобігання великого відсотка крадіжок, і навіть у власному будинку, намагаючись постійно стежити за дітьми, їхнім навчанням і поводженням. Але погодитеся, що це одна з найефективніших можливостей захистити й убезпечити себе й свій будинок. І так, огляд систем відеоспостереження.

Вивчивши критерії, опираючись на які покупці здобували системи відеоспостереження, можна виділити наступне: по-перше, такі системи повинні бути доступними за ціною, а по-друге, вони повинні бути наділені якими-небудь унікальними характеристиками, і повністю відповідати конкретним вимогам або завданням, які поставив покупець.

Тип 2 – Системи не потребуючі 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.

Тип 3 – 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.

Топ самих популярних систем відеоспостереження:

– Перше місце займають багатоканальні камери, які є доступними за ціною.

– Бездротові системи, які необхідні для здійснення спостереження або охорони за своїм житлом.

– Комплекти, у які входять від двох і більше камер. Найчастіше, такі системи застосовуються для охорони в маленьких магазинах, офісах, або часток будинках.

– Комплекти відеоспостереження, що складаються з 4 камер. Як показує практика, таку систему відеоспостереження використовують у тому випадку, якщо необхідно охорону будинку й, наприклад, паркування.

– Зовнішні камери. Вони призначені для установці камер на вулиці. Такі камери захищені від «руйнівників», тобто мають міцний корпус.

Розробка структурної схеми

Розглянемо розроблену структурну схему яка зображена на рисунку 3.1. Широке поширення IP-Камер з функціями відеоаналітики й зберігання інформації може стати каталізатором росту даного сегмента й консолідації ринку великими гравцями.

Серед технологічних аспектів розвитку систем відеоспостереження можна виділити підвищення продуктивності мікропроцесорів для відеокамер, збільшення ємності кеш-пам'яті й швидкості її роботи. Потужності сучасних процесорів досить для інтелектуальної обробки зображення й виконання аналітичних додатків безпосередньо в камері.

Відкритість для інтеграції – ще один важливий тренд, що відкриває можливості побудови комплексних систем різного масштабу. Все більшою популярністю користуються мобільні рішення й керування системами відеоспостереження зі смартфонів і планшетів. Наприклад, мобільний додаток Axis Camera Companion (ACC), оптимізоване для малих систем відеоспостереження (до 16 камер), надає доступ до системи відеоспостереження з мобільного телефону, дозволяє зберігати конфігурації в хмарі й оптимізує навантаження на мережу за рахунок застосування технології Axis Mobile Streaming.

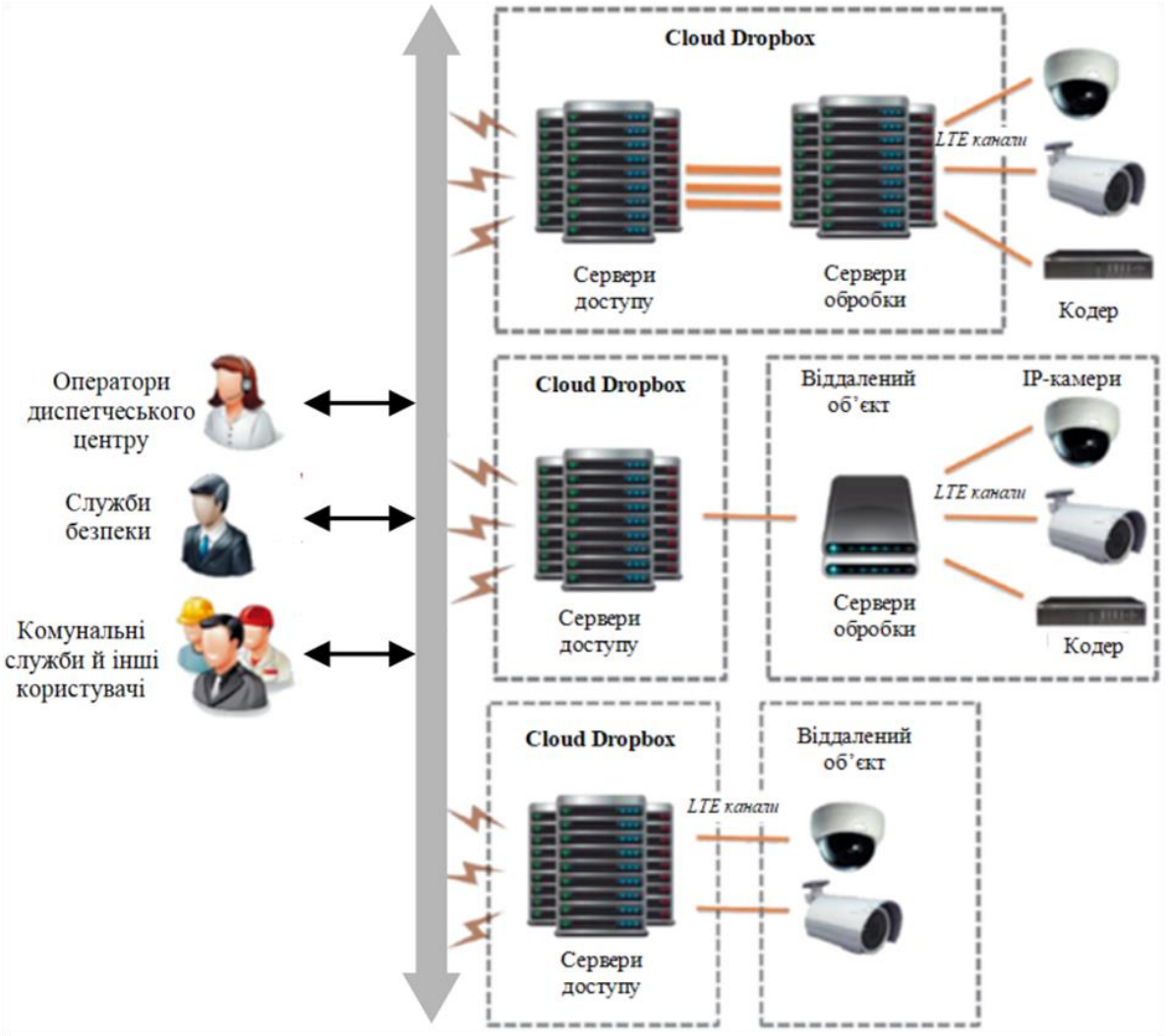


Рисунок 1 – Структурна схема системи

Хмарне відеоспостереження (VSaaS) – зберігання відеоархіву в хмарі – дає такі переваги, як резервування, масштабованість і перенос капітальних витрат на поточні операційні витрати. Простота установки, налаштування й експлуатації як апаратної, так і програмної складових систем відеоспостереження – ще одна очевидна тенденція, обумовлене ростом популярності мережних рішень і необхідністю зниження витрат.

Ключовою тенденцією залишається підвищення якості зображення. Сучасні мережні камери навіть в умовах недостатньої освітленості забезпечують відмінну деталізацію й передачу кольору. Серед технологічних новинок Axis – функція широкого динамічного діапазону (WDR) нового покоління. WDR-Forensic Capture дозволяє вести відеоспостереження в дуже складних умовах висвітлення, одержувати чітке зображення об'єктів, що перебувають у тіні, або в тих випадках, коли світло, приміром, падає позаду. WDR оптимізує відеозйомку, гранично підвищуючи деталізацію в затінених і в яскраво освітлених областях.

Дозвіл Ultra HD. Одна з найбільш помітних тенденцій – зростаючий попит на відео високого розрішення. Технології, які вже знайшли застосування на ринку побутових пристроїв, проникають у сегмент професійного відеоспостереження. Характерний приклад – продукти з розрішенням 4К. Однак виникає чимало питань: як використовувати цю відеоінформацію, як неї передавати й зберігати. Фахівці Axis визнають, що висока вартість СЗД і моніторів 4К поки обмежує попит на такі пристрої. До того ж у камер 4К більше низька світлочутливість, чим в HD-Камер, і вони придатні для використання лише при гарній освітленості. Axis планує продовжувати роботу над підвищенням якості зображення й зменшенням шумів.

Стандарт 4К (Ultra HD, або UHD) перевершує дозвіл Full HD приблизно вдвічі по горизонталі й вертикалі. Оскільки 8К – це приблизно 8 тис. пікселів по горизонталі, а стандарт 8К має дозвіл 7680x4320 (33,1 Мпікс), зображення містить у чотири рази більше пікселів, чим Full HD. Таке відео пред'являє набагато більше високі вимоги до інфраструктури передачі даних і їхньому зберіганню.

Поширення камер UHD буде стимулювати впровадження нових протоколів передачі відео. У свій час поява формату H.264 сприяло переходу на Full HD. UHD знову висуває на перший план завдання стиску зображення. В 2016 році був затверджений формат High Efficiency Video Codec (HEVC), або H.265, – наступне покоління H.264. Він приблизно на третину ефективніше кодека попереднього покоління, дозволяє стискати відео з розрішенням до 8192x4320 і підтримує роботу із прогресивним розгорненням. Деякі виробники вже випустили продукти, що функціонують у новому форматі, і перехід на нього – справа часу.

UHD вимагає спеціальних оптичних вузлів, вартість яких часом не уступає вартості самої камери. Для передачі відеопотоку UHD від камери до реєстратора потрібна мережа з високою пропускною здатністю, та й реєстратор повинен справлятися з такими відеоданими. Обробка й зберігання відео UHD зажадає значних додаткових витрат. Однак рух ринку в цьому напрямку очевидно. Альтернативний варіант – склейка зображень від декількох камер з більше низьким розрішенням, наприклад, для одержання панорами.

«Розумні» камери. Завдяки високому розрішення IP-Камер, збільшенню потужності процесорів і ємності убудованої пам'яті розроблювачам вдається наділяти камери усе більше розвиненими аналітичними функціями й поліпшувати якість зображення. Однак якщо для базових функцій відеоаналітики досить уже наявних процесорних потужностей, те більше складна обробка повинна виконуватися на сервері. Така аналітика навряд чи буде в доступному для огляду майбутньому реалізована «на борті» камер.

Тим часом технології відеоаналітики стрімко розвиваються, відкриваючи можливості для рішення різноманітних завдань. Убудована відеоаналітика дозволяє значно знизити вартість мережної інфраструктури й систем зберігання, а виходить, скоротити бюджет проекту відеоспостереження, адже передавати відео можна лише при виявленні значимих подій, а не транслювати весь відеопотік.

На відміну від сервера, на який надходить безліч відеопотоків, процесору камери досить обробляти всього один потік, причому мова йде про незжатий відео будь-якого розрішення – до 4/8K. Тим самим не тільки підвищується якість виконання аналітичних завдань, але й виключається етап декодування відео на сервері для застосування засобів аналітики. Зараз убудована відеоаналітика застосовується лише в декількох відсотках інсталяцій, але згодом ця частка може вирости до 20-30%, і навіть до 50%. Серверна відеоаналітика залишається важливою технологією для реалізації алгоритмів, які поки не можна реалізувати в програмному забезпеченні камери.

Від продуктів до рішень. Вендори усе активніше переходять від продуктів до рішень і реалізують аналітичні функції, адаптовані до потреб замовника. Багато компаній, у тому числі Axis, Samsung і Panasonic, роблять свої платформи відкритими, що дозволяє стороннім розроблювачам доповнювати їхньої камери новими інтелектуальними функціями, а замовникам – установлювати додатка для рішення конкретних завдань.

Є впевненість, що в остаточному підсумку всі розроблювачі відкриють свої платформи й камери стануть оснащуватися найширшим спектром аналітичних функцій, що, у свою чергу, дасть можливість вирішувати найрізноманітніші завдання. На жаль, дотепер інтерфейси для інтеграції модулів відеоаналітики не стандартизовані. У рамках ONVIF це завдання ще не вирішене.

У той же час зростаюча конкуренція на ринку, скорочення бюджетів і строків впровадження стимулюють створення готових, «коробкових» рішень, не потребуючі проектування системи відеоспостереження.

Для зниження вартості проектів відеоспостереження спрощуються процедури інсталяції й впроваджуються функції вилученого обслуговування, для передачі відео використовуються існуючі мережі, а IP-Камери застосовуються для рішення відразу декількох завдань, наприклад підрахунку числа відвідувачів і охорони об'єкта.

Системи відеоспостереження стають усе більше доступними. Системи середнього класу поступово витісняються недорогими рішеннями. Перші затребувані у великих роздрібних мережах, у банківській галузі, у сфері виробництва, будівництва й логістики. Великі проекти реалізуються на транспорті, на стадіонах, підприємствах ПЕК, в оборонній галузі, у системах рівня «Безпечне місто». На українському ринку відеоспостереження чимало кваліфікованих постачальників, висока конкуренція, однак у сегменті систем старшого класу конкуренція помірна, хоча й тут є гідні рішення.

Розвиваються нові підходи до проектування користувальницького інтерфейсу. Це обумовлено тим, що доступ до систем відеоспостереження тепер мають не тільки служби охорони, але також керівники підприємств і адміністративних працівників. Сьогодні потрібні більше прості, крос-платформні універсальні рішення. Нерідко інтерфейс реалізується на основі Web-Браузера без прив'язки до конкретної платформи.

Спрощення програмного забезпечення й поставки готових рішень – найбільш яскраві тенденції ринку відеоспостереження, як світового, так і українського.

Віртуалізація. Віртуалізація в системах відеоспостереження відкриває можливість для більше ефективного використання ресурсів і наявної інфраструктури при рішенні різних завдань. Віртуалізація – абстрагування програмного забезпечення від апаратних платформ – сприяє реалізації масштабних проектів і допомагає оснащувати системи новітніми функціями, такими, наприклад, як миттєвий пошук в архіві. Ця тенденція підкріплюється попитом на послуги відеоаналітики.

Основна відмінність віртуалізованої архітектури від традиційної полягає в тому, що камери не прив'язані до фізичного сервера, а навантаження балансується автоматично. Спрощується адміністрування: замість індивідуального налаштування кожного фізичного сервера централізовано настроюється логічна група серверів («кластер» віртуальних машин), а підключаються камери до логічного (віртуальному) серверу. Ліцензується таке рішення по числу камер. Основна перевага даного підходу – ефективне використання встаткування й розподіл навантаження.

Віртуалізована архітектура дозволяє знизити витрати приблизно на 30% (за рахунок більше повного завантаження встаткування, простого налаштування, підтримки й резервування) і забезпечує впровадження відеоаналітики операторського рівня. А Web-інтерфейс допомагає розширити коло користувачів системи відеоспостереження.

Крім того, завдяки віртуалізації спрощується створення кластерів серверів – об'єднання декількох однорідних елементів (у цьому випадку віртуальних машин) – і з'являється можливість реалізувати програмно-апаратні комплекси відеоспостереження з недорогим резервуванням на рівні ВМ. Одночасно заставляється основа для розвитку хмарних сервісів.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів розгалуженої системи відеоспостереження на основі бездротових камер і каналів LTE. В межах України в недостатній мірі представлені вітчизняні розробки в цій області. У роботі наведені теоретичне узагальнення й рішення наукового завдання дослідження методів відеоспостереження на основі бездротових камер і каналів LTE. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем відеоспостереження на основі бездротових камер і каналів LTE; Досліджена система відеоспостереження на основі бездротових камер і каналів LTE; На основі отриманих результатів досліджень створена програмна реалізація розгалуженої системи відеоспостереження на основі бездротових камер і каналів LTE. Розроблені під час виконання роботи алгоритми дозволяють успішно вирішувати завдання відеоспостереження на основі бездротових камер і каналів LTE. 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. 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. Марченко Л.В. Дослідження та програмна реалізація розгалуженої системи відеоспостереження на основі

бездротових камер і каналів LTE // Збірник праць молодих науковців ЦНТУ. – Вип. 11. – Кропивницький: ЦНТУ, 2021.

УДК 004

О. Маслюков, бакалавр гр. КН-19-1,9
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ РЕАЛІЗАЦІЇ МІЖМЕРЕЖНОГО ЕКРАНУ З ВИКОРИСТАННЯМ ПІДХОДУ INTERNAL SEGMENTATION FIREWALL

У статті розроблено програмне забезпечення, яке призначено для системи реалізації міжмережного екрану з використанням підходу Internal Segmentation Firewall. 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, Internal Segmentation Firewall

Постановка проблеми. Якщо всі елементи безпеки починають «спілкуватися» у рамках єдиної фабрики, рішення виявляється набагато більше ефективним. Торік представлена концепція відкритої фабрики безпеки – Security Fabric, націленої на реалізацію безперервного захисту (від кінцевих пристроїв, у тому числі IoT, до центрів обробки даних і хмар), ефективність якої підвищується завдяки взаємодії різних засобів ІБ. Кордони й бар'єри стираються: сьогодні вже неможливо виділити який-небудь конкретний периметр, якому потрібно захищати, тому мова йде, скоріше, про безперервну сегментацію й безперервний захист. Концепція фабрики безпеки орієнтована на створення адаптивної всеосяжної комплексної системи. Вона дозволяє блокувати всі можливі вектори атак, у всякому разі найбільш популярні з них. Для цього пристрої безпеки – міжмережевий екран (ММЕ), система захисту пошти, система емуляції кодів, агенти на клієнтській робочій станції – повинні постійно взаємодіяти, обмінюючись інформацією про погрози. Наприклад, перевірка поштовою системою вкладень на предмет спаму сприймається як щось саме собою що розуміє. Однак така перевірка не дозволяє виявити таргетовану атаку, коли у вкладенні присутнє схований шкідливий код. При взаємодії ж із системою емуляції кодів таке вкладення можна відфільтрувати, запустивши його в пісочниці. Або інший приклад. Міжмережевий екран налаштовується таким чином, щоб підозрілі файли направлялися в пісочницю для аналізу, за результатами якого буде прийматися рішення, пропускати або не пропускати їх далі.

У підсумку створюється універсальна платформа, що дозволяє працювати із самими різними кубиками корпоративної системи безпеки, і за рахунок цього досягається синергетичний ефект.

Таким чином, виходячи з вищеперерахованого, розробка програмного забезпечення системи реалізації міжмережевого екрану з використанням підходу Internal Segmentation Firewall, є актуальною задачею, яка потребує вирішення у даній бакалаврській дипломній роботі.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи реалізації міжмережного екрану з використанням підходу Internal Segmentation Firewall.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація міжмережного екрану з використанням підходу Internal Segmentation Firewall.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих міжмережних екранів.

– Дослідження міжмережного екрану з використанням підходу Internal Segmentation Firewall.

– Програмна реалізація міжмережного екрану з використанням підходу Internal Segmentation Firewall.

Об'єктом дослідження є процес Розробки міжмережного екрану з використанням підходу Internal Segmentation Firewall.

Предметом дослідження є методи Розробки міжмережного екрану з використанням підходу Internal Segmentation Firewall.

Методи дослідження базуються на методах захисту інформації, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Пристрої захисту такі як Cisco ASA і Cisco PIX Firewall – одні з багатьох фаєрволів на сьогоднішньому ринку. Різні виробники втілюють різні технології у своїх пристроях. У даному розділі ми розглянемо ці технології. Це стаття, що стосується щаблі професійної сертифікації Cisco в області захисту мереж – Securing Networks with PIX and ASA (SNPA)

Насамперед, визнаніжося з термінологією. Фаєрволи аналізують потік даних (трафік) у мережі. Можна виділити кілька видів трафіку:

– Packets – пакети.

– Connections – з'єднання або сесії.

– State – стан сеансу зв'язку.

Для того, щоб розібратися в різних технологіях фаєрволів, необхідно гарне розуміння еталонної мережевої моделі OSI. Семирівнева модель OSI є стандартом для мережевих комунікацій і основою, на якій побудована будь-яка технологія фільтрації.

Фаєрвол аналізує IP пакет і порівнює його із заданим набором правил, аксес листом (ACL – Access Control List). ACLs задаються адміністратором вручну. Аналізуються тільки наступні елементи:

– Адреса джерела.

– Порт джерела.

– Адреса призначення.

– Порт призначення.

– Протокол.

– Деякі фаєрволи також можуть аналізувати інформацію із заголовка пакета, перевіряючи, чи є пакет частиною нового або встановленого з'єднання.

Якщо пакет, не задовольняє правилам заданим в ACL , по яких він може бути пропущений у захищену мережу, пакет відкидається. Перевага статичної пакетної фільтрації в її швидкодії.

У статичної пакетної фільтрації є наступні недоліки:

– Довільний пакет буде пропущений у мережу, якщо він задовольняє правилам ACL (наприклад, спуфінг).

– Пакети, які повинні бути відфільтровані, можуть потрапити в мережу, якщо вони фрагментовані.

– У процесі завдання правил ACL можуть формуватися дуже більші списки, якими складно управляти.

– Ряд сервісів не може контролюватися пакетною фільтрацією. Це, наприклад, застосунки мультимедіа, де з'єднання динамічно встановлюються на довільних портах, номера яких будуть відомі тільки після установки з'єднання

Статична пакетна фільтрація часто використовується на маршрутизаторах. Пристрою захисту Cisco також можуть використовувати таку фільтрацію.

Проксі-фаєрвол (proxy-firewall)

Проксі-фаєрвол, називаний також проксі-сервером – це звичайно прикладна програма, установлювана на сервер, що має доступ у захищену й зовнішню мережу.

Всі з'єднання хостов захищеної мережі з хостами зовнішньої мережі здійснюються від імені проксі-фаєрвола, як якби проксі-фаєрвол сам установлював ці з'єднання. Хости захищеної мережі ніколи самі не встановлюють з'єднань із зовнішнім світом. Для установки зв'язку, хости внутрішньої мережі посилають запити проксі-фаєрволу, запити рівняються з базою правил. Якщо запит відповідає правилу в базі й дозволений, проксі-фаєрвол надсилає запит зовнішньому хосту й потім форвардить відповідь внутрішньому хосту.

Проксі-фаєрволи працюють на верхніх рівнях моделі OSI. З'єднання встановлюються між мережевим і транспортним рівнем, однак проксі-фаєрвол аналізує запит аж до сьомого рівня на предмет відповідності набору правил, якщо все ок, він установлює з'єднання.

У цій технології зберігається стан кожної відкритої сесії. Щораз, коли встановлюється дозволене зовнішнє або внутрішнє TCP або UDP з'єднання, інформація про це з'єднання запам'ятовується в таблиці стану сесій. У таблицю заноситься адреса джерела й призначення, номера портів, порядкові номери TCP сесії (sequence numbers), також додаткові прапори.

Навіщо це необхідно? Для аналізу пакетів, що повертаються, у кожній конкретній сесії на предмет їхньої легітимності (ті ж порти, правильні порядкові номери сесії, прапори й т.д.). Тобто тепер всі вхідні й вихідні пакети рівняються з інформацією в таблиці стану.

Тобто в загальному зміст роботи динамічної фільтрації полягає в наступному – якщо з'єднання, запитуване хостом, дозволене Cisco фаєрволом, то він запам'ятовує це й поміщає інформацію про з'єднання в таблицю станів (state table) і при поверненні трафіку, тобто при відповіді іншого хоста на запит, пакети дозволяються, якщо вони відповідають тому, що очікує пристрій захисту, тобто відповідають інформації, що зберігається в state table.

Цей метод ефективний по трьох причинах:

– Він працює й з пакетами й із з'єднаннями.
– Продуктивність вище, ніж у проксі-фаєрволів.
– Зберігається інформація кожного з'єднання, що дозволяє визначити чи є пакет частиною цього з'єднання.

Динамічна пакетна фільтрація (stateful packet filtering)

Дана технологія забезпечує кращу комбінацію безпеки й продуктивності. Використовується не тільки ACL, але також аналізується стан сесії, записуване в базу, що називають таблицею стану (state table). Цю технологію Cisco переважно використовує у своїх пристроях захисту.

Після того як з'єднання встановлене, всі дані сесії рівняються з таблицею стану. Якщо дані сесії не відповідають інформації в таблиці стану для цієї сесії, з'єднання скидається.

У цій технології зберігається стан кожної відкритої сесії. Щораз, коли встановлюється дозволене зовнішнє або внутрішнє TCP або UDP з'єднання, інформація про це з'єднання запам'ятовується в таблиці стану сесій. У таблицю заноситься адреса джерела й призначення, номера портів, порядкові номери TCP сесії (sequence numbers), також додаткові прапори.

Навіщо це необхідно? Для аналізу пакетів, що повертаються, у кожній конкретній сесії на предмет їхньої легітимності (ті ж порти, правильні порядкові номери сесії, прапори й т.д.). Тобто тепер всі вхідні й вихідні пакети рівняються з інформацією в таблиці стану.

Тобто в загальному зміст роботи динамічної фільтрації полягає в наступному – якщо з'єднання, запитуване хостом, дозволене Cisco фаєрволом, те він запам'ятовує це й поміщає

інформацію про з'єднання в таблицю станів (state table) і при поверненні трафіку, тобто при відповіді іншого хоста на запит, пакети дозволяються, якщо вони відповідають тому, що очікує пристрій захисту, тобто відповідають інформації, що зберігається в state table.

Цей метод ефективний по трьох причинах:

– Він працює й з пакетами й із з'єднаннями.
– Продуктивність вище, ніж у проксі-фаєрволів.
– Зберігається інформація кожного з'єднання, що дозволяє визначити чи є пакет частиною цього з'єднання.

Рівні безпеки в PIX і ASA

Рівень безпеки – це значення від 0 до 100, призначуване адміністратором на інтерфейсі Cisco ASA або фаєрвола. Рівень безпеки визначає чи довіряємо ми даному інтерфейсу (ті він більше захищений) або не довіряємо (менш захищений) щодо іншого інтерфейсу.

Певний інтерфейс уважається більше захищеним (і довіру до нього більше) у порівнянні з іншим інтерфейсом, якщо його рівень безпеки вище. Відповідно, інтерфейс уважається незахищеним (з меншим ступенем довіри) у порівнянні з іншим інтерфейсом, якщо його рівень безпеки нижче. От така от проста істина.

Зміст даної концепції полягає в тому, що інтерфейс із більше високим рівнем безпеки (захищений інтерфейс) може обмінюватися даними з інтерфейсом, чий рівень безпеки нижче (незахищений), а от плин трафіку з незахищеного інтерфейсу на захищений неможливі без завдання аксесс листів (ACL) і інших параметрів.

Рівень безпеки 100: Найвищий рівень безпеки пристрою захисту. За замовчуванням призначений внутрішньому (inside) інтерфейсу пристрою. Тому що 100 визначає саму захищену мережу, ваша корпоративна мережа повинна бути за цим інтерфейсом. Ніхто не зможе одержати доступ до цієї мережі без створених вами дозволів, при цьому пристрою вашої мережі зможуть мати доступ на інші (зовнішні) інтерфейси.

Рівень безпеки 0: Це найменший рівень безпеки. За замовчуванням призначений зовнішньому (outside) інтерфейсу пристрою. Тому що 0 є найнижчим значенням, за ним повинна перебуває сама незахищена мережа (наприклад, інет), щоб ніхто із цієї мережі не одержав доступу до інших інтерфейсів без явного вашого дозволу.

Рівні безпеки 1-99: Ці рівні безпеки ви можете призначати на інші інтерфейси (інтерфейси периметра), якщо вони задіяні на пристрої захисту cisco. Значення будуть залежати від типу доступу, що ви бажаєте надати.

Приклади з'єднань

Розглянемо три простих приклади з'єднань:

1. З'єднання із захищеного (більше високий рівень безпеки) на незахищений (менший рівень безпеки) інтерфейс:

Трафік, наприклад, що виходить із внутрішнього (inside) інтерфейсу з рівнем безпеки 100 на зовнішній (outside) інтерфейс із рівнем безпеки 0, підкоряється правилу: Дозволити весь IP трафік, якщо він явно не обмежений аксесс списками (ACLs), ідентифікацією (authentication) або авторизацією (authorization).

2. З'єднання з незахищеного інтерфейсу на захищений: Трафік, наприклад, що виходить із зовнішнього (outside) інтерфейсу з рівнем безпеки 0 на внутрішній (inside) інтерфейс із рівнем безпеки 100, підкоряється правилу: Відкидати всі пакети, якщо вони явно не дозволені аксесс списками. Далі трафік обмежити ідентифікацією (authentication) або авторизацією (authorization), якщо такі мають місце бути.

3. З'єднання із інтерфейсів з однаковим рівнем безпеки: Плин трафіку між даними інтерфейсами за замовчуванням заборонено.

Відкриття й закриття портів на PIX Firewall

Кожний інтерфейс на PIX повинен мати рівень безпеки від 0 (найменш безпечний) до 100 (найбільш безпечний). Наприклад, ви повинні призначити для самої захищеної мережі, такий як внутрішня мережа, де розташовані ваші хости, рівень 100. А для

зовнішньої мережі, наприклад, Інтернет, може бути призначений рівень 0. Іншим мережам, таким як DMZ, рівень безпеки призначається в проміжку між 0 і 100. Ви можете призначити один рівень безпеки відразу для декількох інтерфейсів.

За замовчуванням на інтерфейсі outside всі порти заблоковані (рівень безпеки 0), а на інтерфейсі inside (рівень 100) всі порти відкриті. У такий спосіб весь вихідний трафік може проходити через PIX без якої-небудь спеціальної конфігурації пристрою, але вхідний трафік повинен бути явно дозволений за допомогою листів доступу й конфігурацією статичної трансляції адрес (static nat).

Як правило, всі порти заблоковані при проходженні трафіку з найменш безпечної зони в найбільш безпечну, і всі порти відкриті при проходженні трафіку з найбільш безпечної зони в менш безпечну. Це здійснюється за допомогою механізму інспектування станів мережевих з'єднань.

П'ять різних серверів розташовані в зоні DMZ. Необхідно обмежити до них доступ із внутрішньої мережі, і в той же час дозволити доступ із зовнішньої мережі.

Блокування портів

Пристрій безпеки дозволяє проходження будь-якого вихідного трафіку, доти, поки він не буде блокований явним списком доступу (ACL). Список доступу складається з одного або більше елементів (ACE). Залежно від типу списка ви можете вказати адреси відправника й одержувача, протокол, TCP/UDP порти, тип повідомлення ICMP (для протоколу ICMP) і навіть EtherType (для фреймов)

Для протоколів без установлення з'єднання (наприклад, ICMP), пристрій безпеки встановлює односпрямовані сесії, тому вам потрібний список доступу, що дозволяє проходження ICMP в обох напрямках, або ви повинні включити інспектування протоколу ICMP, що виключено за замовчуванням. У цьому випадку інспекційний движок буде трактувати ICMP сесії як двонаправлені з'єднання.

Виконаємо наступні кроки для того, щоб блокувати порти для трафіку який йде з інтерфейсу inside в DMZ.

1. Створюємо список доступу, щоб заблокувати певний порт

access-list <name> extended deny <protocol> < source-network/source IP> < source-netmask>

< destination-network/destination IP>

< destinamtion-netmask> eq <port number> access-list <name> extended permit ip any any

2. Прив'язуємо створений ACL до потрібного інтерфейсу

access-group <access list name> in interface <interface name>

Приклади:

Блокуємо HTTP трафік: Для того, щоб заблокувати внутрішню мережу 10.1.1.0 від доступу до Web сервера 172.16.1.1, розташованому в DMZ мережі, створюємо ACL виду:

ciscoasa(config) #access-list 100 extended deny tcp 10.1.1.0 255.255.255.0 host 172.16.1.1 eq 80

ciscoasa(config) #access-list 100 extended permit ip any any

ciscoasa(config) #access-group 100 in interface inside

Блокуємо FTP трафік: Для того, щоб заблокувати внутрішню мережу 10.1.1.0 від доступу до FTP сервера 172.16.1.2, розташованому в DMZ мережі, створюємо ACL

ciscoasa(config) #access-list 100 extended deny tcp 10.1.1.0 255.255.255.0 host 172.16.1.2 eq 21

ciscoasa(config) #access-list 100 extended permit ip any any

ciscoasa(config) #access-group 100 in interface inside

Відкриваємо порти

Пристрій безпеки забороняє проходження будь-якого вхідного трафіку, доти, поки він не буде дозволений явним списком доступу (ACL).

Якщо ви ходите, що зовнішні хости могли одержати доступ до внутрішніх хостам, ви повинні застосувати вхідний ACL на зовнішній інтерфейс. В ACL вам потрібно вказати трансльовану адресу внутрішнього хоста тому, що тільки ці адреси можуть використовуватися на зовнішній мережі. Як приклад, розв'язний проходження трафіку з інтерфейсу outside на інтерфейс inside або з DMZ в inside.

1. Створюємо фіксовану трансляцію реальної адреси в мапувану адресу. Мапована адреса – це така адреса, що хости перебувають в Internet можуть використовувати для доступу до сервера розташованому в DMZ, без необхідності знання його реальної адреси (адреси інтерфейсу):

static (real_ifc,mapped_ifc) mapped_ip {real_ip [netmask mask] | access-list access_list_name | interface}

2. Створюємо ACL щоб дозволити трафік на указаний порт:

access-list <name> extended permit <protocol> < source-network/source IP> < source-netmask>

< destination-network/destination IP> < destinamtion-netmask> eq <port number>

3. Прив'язуємо ACL на потрібний інтерфейс:

access-group <access-list name> in interface <interface name>

Приклади:

Відкриваємо трафік для SMTP. Відкриваємо порт tcp 25 для того, щоб хости в Інтернет могли відправляти порту на сервер розташований в DMZ. Команда **static** мапує зовнішня адреса 192.168.5.3 у реальний DMZ адреса 172.16.1.3:

ciscoasa(config)#static (DMZ,Outside) 192.168.5.3 172.16.1.3 netmask 255.255.255.255

ciscoasa(config) #access-list 100 extended permit tcp any host 192.168.5.3 eq 25

ciscoasa(config) #access-group 100 in interface outside

Відкриваємо трафік для HTTPS. Відкриваємо порт tcp 443, щоб користувачі зовнішньої мережі могли одержати доступ до web сервера:

ciscoasa(config)#static (DMZ,Outside) 192.168.5.5 172.16.1.5 netmask 255.255.255.255

ciscoasa(config) #access-list 100 extended permit tcp any host 192.168.5.5 eq 443

ciscoasa(config) #access-group 100 in interface outside

Дозволяємо DNS трафік. Аналогічним образом відкриваємо порт udp 53:

ciscoasa(config)#static (DMZ,Outside) 192.168.5.4 172.16.1.4 netmask 255.255.255.255

ciscoasa(config) #access-list 100 extended permit udp any host 192.168.5.4 eq 53

ciscoasa(config) #access-group 100 in interface outside

Принципи роботи PIX/ASA firewall

Часто firewall представляється якимось чорним ящиком який просто фільтрує минаючі пакети. Дана замітка допоможе зрозуміти, що саме відбувається при фільтрації й у якій послідовності.Що відбувається з пакетом який попадає усередину PIX/ASA firewall, по яких параметрах приймається рішення пропускати пакет чи далі ні?

Насамперед, помічу, що мінімальними вимогами до пакета є:

– настроєна трансляція адрес між інтерфейсами. Звичайно, ця вимога можна відключити за допомогою команди no nat-control, однак поводження за замовчуванням саме таке;

– політика доступу (access-list) розв'язний доступ.

Спробуємо розібратися, що відбувається на кожному кроці.

1. Initial checking

Базові перевірки на цілісність пакета, припустимі опції та інше. Саме на цьому етапі проводиться перевірка Reverse Path Forwarding про яку я вже розповідав.

Відзначу, що RPF буде повноцінно працювати тільки у випадку спуфінгу адрес між інтерфейсами. У класичному випадку outside – ASA – inside спуфінг на outside інтерфейсі визначити він не зможе.

2. Xlate lookup (outbound)

Саме зараз перевіряється одна з мінімальних умов – трансляція адрес між інтерфейсами. Зовсім неважливо буде це статична трансляція one to one або динамічна із застосуванням overload.

Спочатку firewall спробує знайти вже існуючу трансляцію (можна подивитися по show xlate), у випадку невдачі намагається створити, якщо звичайно політика це передбачає. Цей крок відбувається на різних етапах у випадку вхідні/вихідного з'єднання. Перевірка здійснюється на другому кроці у випадку вихідного з'єднання. Цьому є логічне пояснення – адреса джерела буде переписаний і саме він повинен фігурувати в подальших перевірках (acl).

Повторюся. Це поводження можна виключити використовуючи no nat-control. Однак, до версії прошивання 7.1 цього зробити було не можна.

Також саме тут firewall перевіряє такі параметри як:

- ліміти на кількість активних з'єднань;
- ліміти на кількість напів-відкритих з'єднань (embryonic);
- таймаути на з'єднання.

3. Connection lookup

Оскільки firewall у нас "розумний" і знає, що таке stateful фільтрація, йому необхідно колись перевіряти стан з'єднання. Чому б не на цьому етапі? :)

Літератури по stateful фільтрації досить, описувати ще раз не буду.

4. ACL lookup

Саме на цьому етапі відбувається щось знайоме. Як видно з назви перевіряється політика доступу – пошук відповідного access-list

За замовчуванням ніяких ACL не застосовано. Трафік дозволений з більше безпечного інтерфейсу на менш безпечний. Рівень безпеки визначається значенням security level.

5. Xlate lookup (inbound)

Відбувається та ж перевірка, що й на кроці 2. Але тільки для вхідного трафіку.

6. Uauth lookup

У випадку якщо firewall використовується як cut-through authentication proxy на цьому кроці перевіряються логін/пароль користувача для його автентифікації.

Якщо це не перше з'єднання ініціюємо користувачем перевіряється таймер автентифікації.

7. Inspection

На останньому кроці здійснюється інспекція протоколу. Конкретні дії виконувані в цьому випадку дуже сильно залежать від інспектуємого протоколу.

Різниця між брандмауерами прикладного й сеансового рівня

У сьогоднішніх взаємозалежних середовищах, концентрованих на додатках, що випливає покоління брандмауерів (брандмауери прикладного рівня) потрібно для того, щоб знизити потенційні можливості атак.

Екскурс із історії, за давніх часів люди спочатку використовували дерева й колоди, щоб захищати свою домашню худобу на території села, багато потенційних небезпек, такі як леви або представники інших племен, небагато стримувалися цим захистом, але вона не могла повністю перешкоджати ім. У міру розвитку технології кочівники стали фермерами, були винайдені забори з каменю, такі кам'яні забори були не тільки краще дерев'яних, але їх було сутужніше обійти або минути. Згодом цілі села стали розташовуватися в рамках фортець, високі огорожі цих фортець могли забезпечити безпека домашній худобі й населенню.

Те ж саме можна сказати щодо брандмауерів; на початку були доступні тільки маршрутизатори зі списками доступу, тому що це було все, що було потрібно на той момент. Керування мережею за допомогою списків контролю доступу й деяких основних фільтрів було цілком достатньо для захисту від неавторизованих користувачів. Справа була саме так, оскільки маршрутизатори лежали в основі кожної мережі, і ці пристрої

використовувалися для маршрутизації трафіку з і на такі WAN з'єднання, як філії й інтернет.

Справа в тому, що не багато чого змінилося касаємо маршрутизаторів, лише невеликі модифікації в способі фільтрації трафіку, а організації, що робили ці пристрої, концентрувалися на підвищенні безпеки до того рівня, на якому ці пристрої здатні забезпечити цю безпеку. Що я хочу сказати? Забір, вибудуваний з колод, завжди буде забором з дерева, не таким надійним, як з каменю.

Брандмауери сеансового рівня також відомі, як брандмауери канального (Circuit) рівня або канальні шлюзи. Брандмауери сеансового рівня мають наступні характеристики; вони працюють на TCP рівні моделі OSI. Звичайно такі брандмауери використовують NAT (Network Address Translation – трансляція мережевих адрес) для захисту внутрішньої мережі, і ці шлюзи мають малий зв'язок (або не мають її взагалі) із прикладним рівнем, і тому не можуть фільтрувати більше складні підключення. Такі брандмауери здатні захищати трафік тільки на базі основних правил, таких як порт джерела й пункту призначення.

У міру розвитку технології виникла потреба в керуванні вихідними мережами. Користувачі мали можливість виходити в інтернет і користувалися слабістю бревенчатого забору, оскільки вони могли обходити його, причиняючись вівцею, насправді, будучи вовком в овечій шкірі.

Це означало, що користувачі з легкістю могли минути безпеку пристроїв п'ятого рівня використовуючи telneting підключення до порту, що був відкритий у вихідному напрямку, але не був портом telnet (з порту 23 підключалися через telnet до порту 80). Маршрутизатор зі списком доступу дозволяв користувачам підключатися до порту, хоча це не був порт telnet, а був порт для іншої служби. Це означало, що маршрутизатор не оглядав пакет (вівцю), коли він виходив за огорожу. Маршрутизатор лише здійснював просту перевірку, думаючи так, якщо це виглядає як вівця й залишає загін, щоб погуляти в поле, те її можна пропустити. Тому вовки могли преспокійно розгулювати серед овець. Така технологія застосовувалася в обох напрямках і в 90-их була основою всіх брандмауерів. Наприкінці 90-их широко розповсюджені проксі сервери з'явилися на сцені. Вони містили в собі базову технологію міжмережевого захисту. Ці 'проксі брандмауери' могли перехоплювати трафік між джерелом місцем призначення, суб'єктом і об'єктом, а оскільки 'проксі брандмауер' розташований посередині, він має можливість оглядати пакети відповідно до визначеного зводу правил, які мають більший компонент строгості.

Брандмауери сеансового рівня працюють на п'ятому рівні моделі OSI. Раніше такого захисту було досить для мереж 90-их років, але в міру того, як атакуючі користувачі розвилися до прикладного рівня, а також у міру росту інтернету й розвитку коду, що втримується там, брандмауери сеансового рівня більше не є адекватними мірами захисту. У результаті без брандмауерів з механізмом захисту прикладного рівня з'являється можливість неправильної роботи й уразливості операційної системи, підданої впливу інтернету, оскільки все, що може запропонувати брандмауера сеансового рівня, це таблицю маршрутизації й списки контролю доступу як базовий рівень захисту.

Невеликі поліпшення в брандмауерах сеансового рівня дозволяють їм оглядати трафік на більше глибокому рівні на наявність загальних протоколів, але ці міри легко минути, використовуючи такі інструменти, як metasploit і backtrack. У сьогоднішнім інтерактивному середовищі єдиною можливістю є установка брандмауера прикладного рівня, що робить щось більше, ніж оглядає ACL і порт джерела й пункту призначення. Більше глибокий огляд пакетів, повноцінне керування підключеннями й фільтрація на прикладному рівні є життєво важливим компонентом при взаємодії із сучасними додатками. Із цих причин, організації, які серйозно ставляться до безпеки, навіть не будуть розглядати альтернативу використання брандмауерів сеансового рівня (маршрутизаторів зі списками доступу) замість брандмауерів прикладного рівня.

Третє покоління брандмауерів відомо як брандмауери прикладного рівня або проксі брандмауери, ці брандмауери здатні передавати й приймати трафік в обох напрямках, тим самим захищаючи суб'єкт і об'єкт від необхідності вступати в безпосередній контакт один з одним. Модулі доступу (proxy) є посередниками в з'єднаннях і, таким чином, здатні фільтрувати й управляти доступом і вмістом с/к об'єкту/суб'єктові. Цього можна домогтися різними способами за допомогою інтеграції у вже існуючі директорії, наприклад LDAP для доступу користувачів або груп користувачів.

Брандмауер прикладного рівня також здатний емулювати сервер, що він підключає до інтернету, тому користувач-відвідувач одержує набагато більше захищене підключення. Справа в тому, що коли користувач відвідує публічний сервер, він насправді відвідує публічний порт брандмауера сьомого рівня, а запит перевіряється й потім аналізується базою правил для подальшої обробки. Коли цей запит проходить базу правил і відповідає певному правилу, він передається на сервер, але різниця полягає в тому, що це з'єднання може виділятися з поліпшеного кешу, поліпшуючи тим самим продуктивність і безпека підключення.

Якщо говорити простою мовою, модель OSI являє собою рівневу модель мережевої архітектури. Ця модель управляє тим, як дві взаємозалежні системи взаємодіють.

Верхній рівень (прикладний) – це звичайно рівень, на якому працюють 'брандмауери на базі proxy'. Брандмауери прикладного рівня являють собою брандмауери третього покоління, які можуть сканувати всі нижчерозташовані рівні. Якщо порівнювати із брандмауерами сеансового або канального рівня, то брандмауери прикладного рівня включають функції брандмауерів сеансового рівня, а також багато поліпшені можливостей, такі як оборотний proxy для безпечної публікації веб сайтів.

Модель OSI, рівень 5 – це сеансовий рівень, а рівень 7 – це прикладний рівень. Рівень, розташований над прикладним рівнем уважається восьмим рівнем, на ньому звичайно розташовуються користувачі й політики.

Сьогоднішні атаки вже настільки розвинені, що більшість брандмауерів сеансового рівня не можуть зупинити навіть основні атаки застосунків. У силу цих причин старі брандмауери п'ятого рівня необхідно доповнювати або заміняти більше надійними 'брандмауерами прикладного рівня'. PCI DSS дозволяє використовувати цей тип брандмауерів для захисту інформації кредитних карт.

Незалежно від того, як сильно ми залежимо від наших старих звичок і старих технологій, більше нові вдосконалені методи мережевого захисту вже є. Інтернет намагається влізти в порти 80 і 443, а перед професіоналами забезпечення безпеки мереж коштує непросте завдання керування користувачами, які вчаться тому, як шифрувати свій трафік, щоб уникнути керування. Рішенням є впровадження брандмауерів прикладного рівня, які здатні проводити огляд навіть зашифрованих потоків. На зовнішньому, більше структурованому прикладному рівні, атаки створюються на щоденній основі, і єдиним способом упоратися з такими погрозами є використання більше зроблених брандмауерів прикладного рівня.

Брандмауери для застосунків Web

Захист застосунків Web на підприємствах і пов'язаних з ними баз даних здобуває все більше значення для запобігання атак з Internet. Якщо колись задовільний захист від погроз із Internet міг запропонувати правильно зконфігурований міжмережевий екран, то згодом широке поширення одержали «чирви», що працювали на рівні застосунків, що зажадало використання ефективних систем запобігання вторгнень (Intrusion Prevention System, IPS). Нині з'явилися нові погрози, які здатні обійти IPS завдяки стратегіям нападів, націленим на додатки Web. Для того щоб гідно протистояти небезпеці, у багатьох великих обчислювальних центрах застосовуються брандмауери для застосунків Web.

Міжмережеві екрани – перша лінія оборони

Уже більше 15 років міжмережеві екрани ставляться до стандартного оснащення мережевої інфраструктури і являють собою першу лінію оборони. Якщо, приміром,

додаток Web виконується на якому-небудь сервері, розташованому в демілітаризованій зоні або центрі даних, то екран стежить за тим, щоб вступники через межі внутрішньої локальної мережі запити направлялися тільки на порти HTTP Port 80 і HTTPS Port 443. Без міжмережевого екрана ресурсами сервера Web легко могли б зловживати хакери – за допомогою сканерів портів або протоколів віддаленого доступу, наприклад Telnet.

Однак у більшості випадків міжмережеві екрани не пропонують ніяких функцій для дослідження пакетів прикладного рівня (рівня 7, або рівня корисних даних) у потоках даних. Зловмисники навчилися використовувати це слабке місце у свою користь, впроваджуючи здійснювані на рівні застосунків атаки в не зухвалих підозр запити до Web. «Хробаки» на базі Web ставляться до перших прикладів даного виду небезпек. Code Red, Nimda і Slapper – от найбільш відомі з них, які нанесли значна втрата користувачам по усьому світі.

Системи IPS – друга лінія оборони

Системи запобігання вторгнень зупиняють «хробаків» і відбивають інші атаки, які завдають удару в слабкі місця комерційного й безкоштовного програмного забезпечення, як, наприклад, сервери Web (IIS, Apache і т.д.) і сервери баз даних (Oracle, MS SQL і т.п.). Система IPS перевіряє вміст пакетів на рівні застосунків і порівнює його зі списком відомих шаблонів даних (сигнатур).

Все-таки й системи IPS мають лише обмежене коло можливостей: через залежність від сигнатур вони безпомічні проти нападів через «проломи» у додатках Web відомих виробників (SAP, Oracle, Peoplesoft і т.д.) і в самостійно написаних додатках Web (у застосунках .asp або .php). Розповсюдженим прикладом подібної погрози є так звана «ін'єкція SQL», коли зловмисник знаходить у модулі уведення застосунки (Input Validation – перевірка правильності уведення) «пролом» у системі безпеки, що дозволила б йому заміняти правильні дані, що вводилися, на спеціальні команди, адресовані базі даних. Ці команди передаються серверу бази даних і тут уже виконуються з повноваженнями програми.

Небезпека «ін'єкцій SQL»

За допомогою «ін'єкції SQL» хакер може викрасти номера кредитних карт, імена користувачів і паролі або навіть одержати необмежений доступ до всієї бази даних.

Подібно атакам з використанням «хробаків», атаки на додатки Web з погляду протоколів виглядають як законні потоки даних HTTP, тому міжмережеві екрани не здатні їх розпізнати. Однак на відміну від «хробаків» вони не використовують яке-небудь відоме слабке місце й тому не можуть бути перервані за допомогою сигнатури. Деякі виробники IPS наголошують на тому, що їхні системи здатні відбивати частина атак на додатки Web, перевіряючи сигнатури, які містять часто використовувані під час атак на Web послідовності символів, наприклад union, select або script.

Однак ці слова нерідко зустрічаються й на зовсім звичайних сайтах Web, які надалі будуть помилково класифіковані як небезпечні. Таким чином, у більшості випадків функція сигнатур відключається. Але навіть якщо вона залишається активної, її легко обійти за допомогою відомих технологій.

Брандмауер для застосунків Web (Web Application Firewall, WAF) покликаний протистояти зростаючому числу зловмисників, що активно вишукує слабкі місця в додатках Web. Такий брандмауер будує порівняльну модель (часто називану «позитивною моделлю безпеки»), що описує, як додаток Web працює при нормальних умовах. Потім він порівнює реальні потоки даних з моделлю, що дозволяє йому ідентифікувати незвичайне поводження.

Ефективна модель застосунку WAF включає у свій состав динамічні URL (.asp, .php і т.д.), параметри, методи HTTP, маркери (cookies), ідентифікатори сеансу, схеми XML/SOAP і багато чого іншого. У деяких продуктах WAF першого покоління моделі доводилося створювати вручну – украй складне й трудомістке завдання, причому у випадку зміни застосунків Web її нерідко доводилося вирішувати щодня. Цей процес був

автоматизований у системах WAF другого покоління: у ході його проводиться моніторинг трафіку даного застосунки в реальному часі й за допомогою статистичних алгоритмів, що навчаються, автоматично будується повноцінна модель поводження в нормальних умовах.

Тепер, якщо зловмисник загрожує передачі дані додатки, негайно включається WAF. Скажемо, хакер на сайті електронної торгівлі Web заміняє який-небудь чисельний параметр кошика покупця на рядок SQL UPDATE, приміром, для зміни ціни, тоді WAF розпізнає незвичайну дію, що суперечить типовому поводженню застосунку.

Хоча UPDATE і є частиною припустимого рядка SQL, WAF навчився ідентифікувати неправомочне використання параметра, завдяки чому частота помилкових спрацьовувань радикально зменшилася. Таким чином, при використанні сучасних систем WAF налаштовування вручну вже не потрібна.

Спрощення й масштабування обчислювальних центрів

Реалізація систем WAF пред'являє до застосунків, мережевим рішенням і рішенням підвищеної готовності певні вимоги. З погляду застосунку архітектура WAF першого покоління ґрунтується на технології зворотного посередника (reverse proxy) для перевірки на рівні застосунків. Однак при реалізації наявність посередника привносить безліч ризиків:

– зниження продуктивності – починаючи з перших міжмережевих екранів архітектури з посередником ставали причиною зниження пропускної здатності мережі й підвищення часу реакції (затримки);

– зміни в обчислювальному центрі – архітектури з посередником змінюють трафік даних у мережі, тому в обчислювальному центрі необхідно зробити узгодження IP-адресації, IP-маршрутизації, URL застосунків, убудованих викликів застосунків і т.д.;

– єдина точка відмови/підвищена готовність – рішення зі зворотним посередником приводять до появи точки загальносистемної відмови (Single Point of Failure), їх варто розробляти з особливою старанністю для забезпечення максимально можливої готовності.

У нових системах WAF застосовуються технології обробки даних на рівні ядра, що дозволяє позбутися від недоліків рішень із посередником. Вони дозволяють збільшити пропускну здатність до декількох гігабіт у секунду, знизити затримку до мікросекунд і обійтися без внесення змін в інфраструктуру обчислювального центра. Крім того, що працюють на рівні ядра продукти допускають кілька сценаріїв застосування для забезпечення підвищеної готовності.

Установлювані в розрив на мережевому маршруті (inline), вони підтримують прозору передачу навантаження при збої (failover). У випадку помилки сеанси не перериваються. Крім того, ці продукти можна використовувати й в автономному режимі (offline) у якості мережевого монітора, тоді атаки відбиваються шляхом скидання TCP.

Захист для будь-якого інтерфейсу

З погляду мережі системи WAF повинні прозоро інтегруватися в наявної архітектури другого рівня, щоб підтримувати складну топологію віртуальних локальних мереж і такі процеси, як агрегація каналів. Продукти першого покоління не відповідали цій вимозі, що іноді приводило до серйозних проблем в обчислювальних центрах.

Останнє покоління платформ забезпечення безпеки має параметри продуктивності, що дозволяють домогтися прозорості застосунків у нових системах WAF. Це дає можливість брандмауерові для застосунків Web захищати трафік даних, що надходить через будь-який інтерфейс. Крім того, нові платформи забезпечення безпеки в стані представити віртуальні локальні мережі стосовно застосунків у якості або власного, або стандартизованого інтерфейсу Ethernet.

І нарешті, ще один аспект, що не варто недооцінювати: модульна архітектура нових платформ забезпечення безпеки пропонує повну надмірність на рівні портів, апаратного забезпечення й застосунків. Таким чином, ці платформи відповідають вимозі підвищеної готовності систем WAF другого покоління. Саме модульність пропонує ще одна важлива

перевага: продуктивність системи лінійно масштабується завдяки додаванню нових модулів або інтерфейсних карт.

Захист за допомогою триступінчастого підходу

Забезпечення безпеки застосунків Web породжує цілих коло складних завдань. Це висловлення звучить досить банально, оскільки вірно для занадто великого числа питань забезпечення безпеки, однак у цьому випадку вимагає дуже серйозного осмислення: особи, відповідальні за безпеку, повинні розуміти, що спектр потенційних погроз надзвичайно широкий – від простих атак на мережу за допомогою «хробаків» до атак на додатки Web. Максимально можливий захист застосунків Web вимагає триступінчастого підходу, що базується на технологіях міжмережевих екранів, систем запобігання вторгнень і брандмауерів для захисту застосунків Web.

Міжмережевий екран або мережевий екран – комплекс апаратних або програмних засобів, що здійснює контроль і фільтрацію минаючих через нього мережевих пакетів на різних рівнях моделі OSI відповідно до заданих правил.

Основним завданням мережевого екрана є захист комп'ютерних мереж або окремих вузлів від несанкціонованого доступу. Також мережеві екрани часто називають фільтрами, тому що їхнє основне завдання – не пропускати (фільтрувати) пакети, що не підходять під критерії, певні в конфігурації.

Деякі мережеві екрани також дозволяють здійснювати трансляцію адрес – динамічну заміну внутримережевих (сірих) адрес або портів на зовнішні, використовувані за межами ЛОМ.

Головна тенденція цього ринку – постійна зміна проблем, з якими зіштовхуються люди через виникнення всі нових і нових комп'ютерних погроз. А оскільки міняються погрози, то міняються й вимоги до засобів захисту. Із цим і зв'язана поява мережевих екранів наступного покоління.

Відповідно до політики Gartner, у число лідерів «магічного квадранта» у сегменті Enterprise Network Firewall входять як великі, так і середні компанії, а об'єднуюніж фактором служить те, що всі вони розробляють рішення, здатні задовольнити потреби IT-середовища в масштабі підприємства. Серед цих потреб можна відзначити розмаїтість застосовуваних моделей пристроїв, підтримку віртуалізації й віртуальних локальних мереж, а також можливості керування й формування звітів для великих і комплексних середовищ – багаторівневе адміністрування, мінімізація кількості правил і політик і т.п. Важливим елементом є підтримка нового покоління міжмережевих екранів (NGFW), тому що компанії поступово відходять від застосування виділених IPS-пристроїв по периметрі IT-інфраструктури й у віддалених кінцевих точках. Розроблювачі рішень, що ввійшли в «магічний квадрант», є лідерами ринку. Вони пропонують нові функції для захисту від погроз, реалізуючи в них весь свій експертний потенціал. Пропоновані ними системи забезпечення мережевої безпеки мають високий авторитет серед споживачів завдяки відсутності уразливостей. Відмітні характеристики таких рішень – це надвисока пропускна здатність і продуктивність, а також можливість апаратного прискорення.

UTM-пристрою – це багатофункціональні програмно-апаратні комплекси, у яких сполучені функції різних пристроїв – міжмережевого екрана, системи виявлення й запобігання вторгнень у мережу, антивірусного шлюзу. UTM-пристрої використовуються для швидкої й ефективної побудови системи безпеки мережевих ресурсів.

Міжмережевий екран нового покоління був визначений аналітиками Gartner як технологія мережевої безпеки для великих підприємств, що включає повний набір засобів для перевірки й запобігання проникнень, перевірки на рівні застосунків і точного керування на основі політик.

Якщо організація вивчає можливість використання міжмережевого екрана нового покоління, то саме головне – визначити, чи забезпечить такий екран можливість безпечного впровадження застосунків у благо організації. На першому етапі вам буде потрібно одержати відповіді на наступні питання:

– Чи дозволить міжмережевий екран нового покоління підвищити прозорість і розуміння трафіку застосунків у мережі?

– Чи можна зробити політикові керування трафіком більше гнучкої, додавши додаткові варіанти дій, крім дозволу й заборони?

– Чи буде ваша мережа захищена від погроз і кібератак, як відомих, так і невідомих?

– Чи зможете ви систематично ідентифікувати невідомий трафік і управляти їм?

– Чи можете ви впроваджувати необхідні політики безпеки без шкоди продуктивності?

– Чи будуть скорочені працезатрати вашої команди по керуванню міжмережевим екраном?

– Чи дозволить це впросити керування ризиками й зробити даний процес більше ефективним?

– Чи дозволять впроваджувані політики підвищити рентабельність роботи підприємства?

У випадку позитивної відповіді на вищенаведені питання можна зробити наступний крок і обґрунтувати перехід зі старих міжмережевих екранів на міжмережеві екрани нового покоління. Після вибору постачальника або вузького кола постачальників, виконаного за допомогою заявки, піде етап оцінки фізичних функцій міжмережевого екрана, виконуваної із застосуванням трафіку різних типів і комбінацій, а також об'єктів і політик, які точно передають особливості бізнес-процесів організації.

Основним завданням мережевого екрана є захист комп'ютерних мереж або окремих вузлів від несанкціонованого доступу. Також мережеві екрани часто називають фільтрами, тому що їхнє основне завдання – не пропускати (фільтрувати) пакети, що не підходять під критерії, певні в конфігурації.

Захист корпоративних мереж базується на міжмережевих екранах, які тепер повинні не тільки фільтрувати потоки інформації з портів, але й контролювати дані, передані по найбільш популярним з них. По оцінках експертів SophosLabs компанії Sophos, до 80% нападів відбуваються з використанням веб-браузера по протоколах HTTP або HTTPS, однак простим фільтруванням цих протоколів проблему не вирішити. Таким чином, до нового покоління міжмережевих екранів, сполучених із системами виявлення вторгнень, з'являються нові вимоги.

Міжмережеві екрани нового покоління рекомендується впроваджувати для рішення наступних завдань:

– контролю окремих веб-застосунків;

– виявлення вторгнень по найбільш популярних протоколах, таким як HTTP, SMTP і POP3;

– створення VPN-З'єднань для віддаленого підключення мобільних користувачів;

– оптимізації мережевої взаємодії.

Слід зазначити, що наявність систем виявлення вторгнень потрібно також при обробці персональних даних, захисту банківських і платіжних систем, а також і інших складних інформаційних інфраструктур. Сполучення ж їх з міжмережевими екранами дуже зручно й вигідно для користувачів.

Інші назви

Брандма́уер (ньому. Brandmauer) – запозичений з німецької мови термін, що є аналогом англійського firewall у його оригінальному значенні (стіна, що розділяє суміжні будинки, охороняючи від поширення пожежі). Цікаво, що в області комп'ютерних технологій у німецькій мові вживається слово «firewall».

Фаєрво́лл, фаєрво́л, файерво́л, фаєрво́л – утворено транслітерацією англійського терміна firewall, еквівалентного терміну міжмережевий екран, у цей час не є офіційним запозиченим словом у російській мові.

Функції мережевих екранів

Сучасна корпоративна мережа – не замкнутий інформаційний простір. Найчастіше це розподілена мережа, пов'язана із зовнішнім ЦОДом, що використовує хмари й периферію, що складається з безлічі сегментів. Сучасний корпоративний міжмережевий екран повинен мати відповідні функції для її захисту.

Різновиду мережевих екранів

Мережеві екрани підрозділяються на різні типи залежно від наступних характеристик:

– чи забезпечує екран з'єднання між одним вузлом і мережею або між двома або більше різними мережами;

– чи відбувається контроль потоку даних на мережевому рівні або більше високих рівнях моделі OSI;

– чи відслідковуються стани активних чи з'єднань ні.

Залежно від охвату контрольованих потоків даних мережеві екрани діляться на:

– традиційний мережевий (або міжмережевий) екран – програма (або невід'ємна частина операційної системи) на шлюзі (сервері передавальному трафік між мережами) або апаратне рішення, що контролюють вхідні й виходячі потоки даних між підключеними мережами.

– персональний мережевий екран – програма, установлена на користувальницькому комп'ютері й призначена для захисту від несанкціонованого доступу тільки цього комп'ютера.

Вирождений випадок – використання традиційного мережевого екрана сервером, для обмеження доступу до власних ресурсів.

Залежно від рівня, на якому відбувається контроль доступу, існує поділ на мережеві екрани, що працюють на:

– мережевому рівні, коли фільтрація відбувається на основі адрес відправника й одержувача пакетів, номерів портів транспортного рівня моделі OSI і статичних правил, заданих адміністратором;

– сеансовому рівні (також відомі як stateful) – сеанси, що відслідковують, між додатками, не проникні пакети специфікації, що порушує, TCP/IP, часто використовуваних у зловмисних операціях – скануванні ресурсів, зломах через неправильні реалізації TCP/IP, обривши/із з'єднань, ін'єкція даних.

– рівні застосунків, фільтрація на підставі аналізу дані додатки, переданих усередині пакета. Такі типи екранів дозволяють блокувати передачу небажаної й потенційно небезпечної інформації, на підставі політик і налаштовувань.

Деякі рішення, які відносяться до мережевих екранів рівня застосунки, являють собою проксі-сервери з деякими можливостями мережевого екрана, реалізуючи прозорі проксі-сервери, зі спеціалізацією по протоколах. Можливості проксі-сервера й багатопротокольна спеціалізація роблять фільтрацію значно більше гнучкої, ніж на класичних мережевих екранах, але такі додатки мають всі недоліки проксі-серверів (наприклад, анонімізація трафіку).

Залежно від відстеження активних з'єднань мережеві екрани бувають:

– stateless (проста фільтрація), які не відслідковують поточні з'єднання (наприклад, TCP), а фільтрують потік даних винятково на основі статичних правил;

– stateful, stateful packet inspection (SPI) (фільтрація з урахуванням контексту), з відстеженням поточних з'єднань і пропуском тільки таких пакетів, які задовольняють логіці й алгоритмам роботи відповідних протоколів і застосунків. Такі типи мережевих екранів дозволяють ефективніше боротися з різними видами DoS-атак і уразливостями деяких мережевих протоколів. Крім того, вони забезпечують функціонування таких протоколів, як H.323, SIP, FTP і т.п., які використовують складні схеми передачі даних між адресатами, що погано піддаються опису статичними правилами, і, найчастіше, несумісних зі

стандартними, stateless мережевими екранами.

Ознака якнайшвидшої кончини фаєрволів – зростаюча популярність хмарних технологій.

Еволюція IT-інфраструктури й поява ще більш хитромудрих погроз послужили поштовхом для занепокоєння, що не припиняється, про те, що фаєрволи застарівають і не справляються зі своїми завданнями. Уперше такі думки пролунали наприкінці 90-х, коли в корпоративних середовищах стали всі частіше використовуватися ноутбуки й віддалений доступ, а серед користувачів почалися розмови про зростаючу уразливість мереж. Прогнози повторилися через кілька років, коли стала рости популярність SSL VPN і наступив бум використання смартфонів і персональних пристроїв для доступу до мережі. Остання ознака якнайшвидшої кончини фаєрволів – зростаюча популярність хмарних технологій[2].

Функціональність фаєрволів у наші дні значно розширилася, і тепер це не просто засобу моніторингу певних портів, IP-адрес або пакетної активності між адресами й прийняття рішень із дозволу й відмові. Спочатку в ці системи входили функції інспекції пакетів з урахуванням стану протоколу, моніторингу потоків даних, зіставлення із шаблоном і аналізу. Тепер фаєрволи детально перевіряють певну активність застосунків і користувачів. Фаєрволи, здатні ідентифікувати використовувані додатки, часто називають фаєрволами нового покоління, однак ця назва не зовсім правильне, тому що ця функціональність використовується вже більше десяти років.

У кожному разі, сама злободенна проблема для фаєрволів сьогодні – вивчення минаючі через них інтернет-трафіку й виявлення використовуваних корпоративних і веб-застосунків, а також їхніх користувачів. Точно визначати тип трафіку й тих, хто його запитує, – життєво важлива необхідність для організацій, оскільки це дозволяє їм оптимізувати використання субзастосунків (таких як Facebook,YouTube, Google Apps і інші додатки Web 2.0) і управляти ними. Маючи такі знання, IT-Відділи одержують можливість адаптувати використання застосунків у мережі відповідно до потреб кожного користувача й потребами організації.

Сучасні фаєрволи не тільки розвиваються відносно перевірки й керування трафіком, але й надають додаткові можливості забезпечення безпеки, які організації можуть активувати для обслуговування своїх потреб. Серед цих функцій -URL-фільтрація, антивірус, захист від спама й ботів, запобігання витоків даних, контроль доступу з мобільних пристроїв, а також багато інші, що роблять фаєрвол мультисервісним шлюзом безпеки. За допомогою модульного підходу, керованого програмним способом, можна додавати й розгортати ці функції, підсилюючи захист мережі й вирішуючи нові проблеми в міру їхнього виникнення.

Отже, сьогодні фаєрволи не тільки захищають периметр мережі, як вони завжди це робили, але й дозволяють додавати такі можливості забезпечення безпеки, про які не можна було й мріяти 20 років тому. Незважаючи на регулярні пророкування неминучої втрати популярності, зараз фаєрволи перебувають у самому розквіті свого розвитку.

Internal Segmentation Firewall (ISFW)

Internal Segmentation Firewall – адаптивна система мережевої безпеки, орієнтована на відстеження й керування погрозами корпоративним мережам з боку IoT.

Адаптивна система мережевої безпеки містить функції відстеження, інтеграції, керування й масштабування інфраструктури, вони забезпечують ефективний захист від погроз, ріст кількості яких пов'язаний з поширенням пристроїв IoT.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів реалізації міжмережевого екрану з використанням підходу Internal Segmentation Firewall. В межах України в недостатній мірі представлені вітчизняні розробки в цій області. Дане 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.

Список літератури

1. Розробка методів підвищення оперативності передачі та захисту інформації у телекомунікаційних системах: звіт про НДР (проміжний) / Наук. кер. О.А. Смірнов. – К.:КНТУ, 2013 № ДР 0113U003086
2. 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.
3. 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.
4. 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.
5. 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.
6. Смирнов А.А. Метод обнаружения вредоносного программного обеспечения на основе корреляционного анализа сетевого трафика / Д.А. Даниленко // Матеріали XII всеукраїнської наукової інтернет-конференції «Наукові дослідження: зв'язок теорії і практики». м. Тернопіль. 29-30 квітня 2012 р. – Тернопіль: ТНЕУ. – 2012. – С. 9-10.
7. Смирнов А.А. Метод детектирования вредоносного трафика в телекоммуникационных сетях на основе использования bds-тестирования / Д.А. Даниленко // Збірник тез V міжнародної науково-практичної конференції «Комп'ютерні системи та мережні технології» (CSNT-2012). м. Київ. 13-15 червня 2012 р. – Київ: НАУ. – 2012. – С. 121.
8. Смирнов А.А. Обнаружение и предотвращение вторжений в компьютерных сетях на основе статистического анализа сетевого трафика / А.А. Смирнов, Д.А. Даниленко // Збірник тез доповідей науково-практичної конференції «Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку». м. Харків. 12-13 березня 2014 р. – Харків. АВВ МВС. – 2014. – С. 13-14.
9. Смірнов О.А. дисперсійний аналіз мережного трафіку для забезпечення інформаційної безпеки телекомунікаційних систем та мереж / О.А. Смірнов, Д.О. Даниленко // Збірник тез V Всеукраїнської науково-практичної конференції "Інформатика та системні науки". м. Полтава. 13-15 березня 2014 р. – Полтава: ПУЕТ. – 2014. – С. 289-291.
10. Смирнов А.А. Метод дисперсионного анализа сетевого трафика для обнаружения и предотвращения вторжений в телекоммуникационных системах и сетях/ А.А. Смирнов, Д.А. Даниленко // Збірник тез VI міжнародної науково-практичної конференції "Проблеми і перспективи розвитку ІТ-індустрії". м. Харків. 17-18 квітня 2014 р. – Харків: ХНЕУ. – 2014. – С. 258.
11. Смірнов О.А. метод забезпечення інформаційної безпеки телекомунікаційних систем з використанням дисперсійного аналізу мережного трафіку / О.А. Смірнов, Д.О. Даниленко // Збірник тез міжнародної науково-практичної конференції «Інформаційна та економічна безпека» (INFECO-2014)». м. Харків. 15-16 травня 2014 р. – Харків: ХІБС УБС НБУ. – 2014. – С. 135-139.

УДК 004

М. Мулярчук, магістр гр. КІ-19М-1,4
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ КІБЕРБЕЗПЕКИ ПОБУДОВАНОЇ НА ВИКОРИСТАННІ CYBER THREAT HUNTING ТА DATA SCIENCE

У статті розроблено програмне забезпечення, яке призначено для системи кібербезпеки побудованої на використанні Cyber Threat Hunting та Data Science. Метою розробки є дослідження та програмна реалізація системи кібербезпеки побудованої на використанні Cyber Threat Hunting та Data Science. Об'єктом дослідження є процес кібербезпеки побудованої на використанні Cyber Threat Hunting та Data Science. Предметом дослідження є методи кібербезпеки побудованої на використанні Cyber Threat Hunting та Data Science. Методи дослідження базуються на методах захисту інформації, методах математичної статистики, методах розробки програмного забезпечення. 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, Cyber Threat Hunting, Data Science

Постановка проблеми. Штучний інтелект і пов'язані з ним терміни машинне навчання й нейромережі сьогодні активно використовують для просування нового покоління інформаційних систем. Терміни «самонавчаємий», «інтелектуальний» стали маркетинговими «мемами», як колись слово smart («розумний»), згадайте – смартфон, розумні годинники, розумний будинок і т.д., тому ними користуються зайво часто. «Інтелектуальний», як і «розумний», – завжди дорожче, ніж звичайний, тому важливо відрізняти, де це слово означає технології, що створюють принципово нову якість, а де тільки обгортка й маркетинг. Особливо це важливо в інформаційній безпеці, де часто помилка – це прямий збиток.

Специфіка інформаційної безпеки, на відміну від інших інформаційних технологій, у тому, що навчання на старих даних не ефективно. Якщо справа стосується розпізнавання осіб, планування товарних запасів або машинного перекладу текстів – то навчання на старих паттернах – основа успіху таких алгоритмів машинного навчання. Чим більше правильно розпізнаних осіб, правильно перекладений текст, правильно спланованих запасів – тим краще алгоритми будуть працювати в майбутньому – об'єкт вивчення не буде сильно мінятися й можна усе більше заглиблюватися в деталі – адже не можна очікувати, що в людей з'явиться третє око або в мові радикально зміниться морфологія або синтаксис.

Cyber Threat Hunting (тут і далі – також хантинг) – це процес проактивного й ітеративного пошуку й виявлення просунутих погроз, які неможливо виявити традиційними засобами захисту. Даний процес розпадається на ряд загальновизнаних технік хантингу.

Data Science – наука про дані, відповідальна за обробку й добування корисної інформації з масивів структурованих або неструктурованих даних. Термін Data Science окреслює досить об'ємну предметну область, що вимагає конкретизації в кожному окремому випадку. Так, якщо говорити про симбіоз Cyber Threat Hunting і Data Science, визначення останньої як науки про дані, трохи міняється. Термін «Data Science» у контексті Cyber Threat Hunting розкривається як набір технік і прийомів, за допомогою яких здійснюється хантинг і які несуть у собі специфічні принципи роботи з даними.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи кібербезпеки побудованої на використанні Cyber Threat Hunting та Data Science.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи кібербезпеки побудованої на використанні Cyber Threat Hunting та Data Science.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем кібербезпеки побудованої на використанні Cyber Threat Hunting та Data Science.

– Дослідження системи кібербезпеки побудованої на використанні Cyber Threat Hunting та Data Science.

– Програмна реалізація системи кібербезпеки побудованої на використанні Cyber Threat Hunting та Data Science.

Об'єктом дослідження є процес кібербезпеки побудованої на використанні Cyber Threat Hunting та Data Science.

Предметом дослідження є методи кібербезпеки побудованої на використанні Cyber Threat Hunting та Data Science.

Методи дослідження базуються на методах захисту інформації, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Штучний інтелект і машинне навчання істотно прискорюють реагування на погрози, визнають аналітики Nemertes Research. За їхніми словами, сьогодні це вже серйозний ринок, сформований під впливом реальної потреби.

В Nemertes провели глобальне дослідження, присвячене безпеки, і його результати свідчать: у середньому на виявлення атаки й реагування на неї в організаціях іде 39 днів, однак у деяких компаніях зуміли скоротити цей час до лічених годин. Швидкість реагування прямо залежить від рівня автоматизації, що забезпечується засобами AI і машинного навчання.

Середній час виявлення атаки – година. У найефективніших компаніях, що застосовують машинне навчання, на виявлення йде менш 10 хвилин, а у відстаючих – дні або тижні. Що стосується середнього часу аналізу погроз, воно становить третя година. У кращих компаніях на такий аналіз ідуть хвилини, у гірших – дні або тижні. Поведінковий аналіз погроз уже застосовується в 21% компаній, що брали участь в опитуванні, і ще в 12% повідомляють, що впровадять відповідні засоби до кінця поточного року.

На передовий перебувають компанії сфери фінансових послуг. Оскільки їхні дані мають підвищену цінність, вони звичайно по кібербезпеки йдуть на крок попереду всіх і вкладають значні кошти в нові далеко не дешеві технології.

За масштабами застосуваннях AI і машинного навчання в цілому показники ще вище. Відповідно до дослідження Vanson Bourne, сьогодні в 80% організацій застосовують для тих або інших цілей штучний інтелект, і це вже окупається. Найбільше дивідендів він приносить в області досліджень і розробки нових продуктів – 50% респондентів повідомили, що нововведення забезпечує позитивні результати. Друге й третє місця – у ланцюжка поставок (46%) і основної діяльності (42%). Ненабагато відстають безпека й керування ризиками: 40% респондентів повідомили про позитивний досвід застосування AI у цих областях.

Перераховані показники продовжать рости: як виявило недавнє дослідження Spiceworks, в 30% організацій, що мають більше 1 тис. співробітників, застосовують штучний інтелект в IT-службах, в 25% збираються почати це робити в наступному році.

У маркетинговому агентстві Garrigan Lyman Group впроваджують штучний інтелект і машинне навчання для рішення цілого ряду завдань кібербезпеки, у тому числі для виявлення незвичайної активності мережі й користувачів, а також для розпізнавання нових кампаній фішингу. Без нових технологій було б неможливо нормально працювати, оскільки

зловмисники вже давно прибігають до автоматизації своєї діяльності, зізнаються в Garrigan Lyman.

Штучний інтелект і машинне навчання забезпечують цієї компанії перевага. Сама вона невелика, усього 125 співробітників, але завдяки хмарним сервісам має можливість швидко впроваджувати самі нові технології. В Garrigan Lyman вдається вводити в експлуатацію корисні нововведення всього за пару тижнів. Зокрема, тут користуються засобами безпеки зі штучним інтелектом компаній Alert Logic і Barracuda Networks, і, як зізнаються в Garrigan Lyman, системи «розумніють буквально на очах».

Штучний інтелект допомагає системам адаптуватися до вимог компанії без об'ємного попереднього навчання. Наприклад, як відзначають в Barracuda, модель AI може самостійно зрозуміти, що, коли генеральний директор компанії певного типу користується некорпоративною адресою електронної пошти, це аномалія. У деяких організаціях, якщо керівник спілкується через особисту пошту на мобільному пристрої, це норма, а от якщо головний бухгалтер відправляє повідомлення з персональної адреси, це вже аномалія.

Ще одна перевага хмарної доставки: розроблювачам простіше вдосконалювати свої продукти виходячи із клієнтських відгуків.

Кібербезпека – це як сусідська пильність: якщо я помітив щось підозріле в нашім кварталі, то попереджу інших. Фішингові повідомлення або мережні атаки можуть бути виявлені раніше в інших годинних поясах, завдяки чому в компаній з'являється час підготуватися. Природно, повинне бути довіра до постачальника сервісу. В Garrigan Lyman при виборі постачальників проводили докладний аналіз – наприклад, засвідчували в тому, що кандидат дотримується певних норм проведення аудита, і в тому, що доступ до клієнтських даних можуть одержати тільки уповноважені особи.

Недовіра до нововведень утрудняє перехід від традиційних процесів до автоматизації на основі штучного інтелекту – адже крім знання особливостей роботи вашого постачальника не перешкодять відомості про те, як саме AI приймає рішення. Принципи роботи експертних систем повинні бути зрозумілими, щоб їм можна було довіряти. Розуміючи, як діє система, клієнт дає свої відкликання й побажання, це допомагає вдосконалювати моделі машинного навчання.

У компанії LexisNexis Legal and Professional 12 тис. її співробітників недавно почали для захисту електронної пошти користуватися системою GreatHorn. Тепер, якщо, приміром, починають надходити повідомлення з домену, за написанням схожого на добре відомий, система автоматично відзначить його в якості «самозванця» і повідомить, чому це зроблено: «Оцінку поставлена, оскільки домен схожий на той, з яким ви звичайно обмінюєтеся повідомленнями, однак його технічна інформація виглядає підозріло».

У міру росту рівня довіри до системи й точності її рішень в LexisNexis хочуть перейти від простого маркування підозрілих повідомлень до автоматичного переміщення таких повідомлень у карантин. На сьогодні результати досить вражаючі: маркіруються саме шкідливі повідомлення. А коли буде налагоджено карантинування, користувачі взагалі перестануть їх бачити. Після цього інструмент планується впровадити й в інших підрозділах компанії, а також вивчити інші можливості використання AI для забезпечення безпеки.

Як штучний інтелект дозволяє випередити зловмисників

AI удосконалюється в міру росту обсягу одержуваних даних. При нагромадженні досить більших зрізів дані системи здатні виявляти дуже ранні ознаки появи нових погроз. Приклад – SQL-ін'єкції. У компанії Alert Logic щокварталу збирають дані приблизно по 500 тис. інцидентів, що відбуваються в 4 тис. її клієнтів. Біля половини таких інцидентів пов'язані з атаками на основі SQL-ін'єкцій. У жодній компанії світу немає можливості розглядати кожний такий інцидент окремо, щоб з'ясувати, чи вдалася спроба ін'єкції, упевнені в Alert Logic.

Завдяки машинному навчанню системи компанії не тільки швидше обробляють дані, але й корелюють події, що відбувалися в різні періоди часу в різних регіонах. Деякі атаки можуть повторюватися через кілька тижнів або місяців, при цьому виходити з інших

сегментів Інтернету. Якби не машинне навчання, такі інциденти в Alert Logic упускали б, упевнені в компанії.

Великі обсяги інформації про погрози також збирають в GreatHorn, компанії, що є оператором хмарного сервісу безпеки електронної пошти для Microsoft Office 365, Google G Suite і Slack.

Сервіси GreatHorn здатні виявляти нові кампанії фішингових розсилань і переносити повідомлення в карантин або доповнювати їхніми попередженнями за кілька днів до того, як дослідники прийдуть до виводу про появу нової погрози.

Перспективи використання штучного інтелекту у світі безпеки

Виявлення підозрілої активності користувачів і мережного трафіку – саме очевидне застосування машинного навчання. Нинішні системи усе більш успішно справляються з виявленням незвичайних подій у більших потоках даних, рішенням стандартних завдань аналізу й розсиланням повідомлень.

Наступний крок – використання AI для боротьби з більше складними проблемами. Наприклад, рівень кіберризику для компанії в кожний конкретний момент залежить від безлічі факторів, у тому числі від наявності систем без латок, незахищених портів, надходження повідомлень спрямованого фішингу, рівня надійності паролів, обсягу незашифрованих конфіденційних даних, а також від того, чи є організація об'єктом атаки з боку спецслужб іншої держави.

Доступність точної картини ризиків дозволила б більш раціонально використовувати ресурси й розробити більше детальний набір показників ефективності забезпечення безпеки. Сьогодні відповідні дані або не збираються, або не перетворяться в осмислені відомості.

Фахівці реалізували 24 види алгоритмів, які вишиковують «теплову карту» ризиків, що враховує всі особливості клієнтського середовища й що дозволяє з'ясувати, чому та або інша «гаряча» область позначена в якості такої. При цьому сервіс видає ради по виправленню ситуації – якщо піти їм, «гаряча» червона область стане спершу жовтої, потім зеленої. Системі також можна задавати питання начебто «Що саме мені варто почати в першу чергу?», «Який мій ризик фішингу?» або «Який мій ризик виявитися жертвою WannaCry?».

Надалі штучний інтелект буде допомагати компаніям визначатися, у які нові технології безпеки варто вкладатися. У більшості компаній сьогодні не знають, скільки і як витрачати на кібербезпеку. Штучний інтелект потрібний, щоб виявити показники, на основі яких IT-директор зможе звернутися до керівника компанії або в раду директорів і пояснити, скільки і які ресурси потрібно для того або іншого проекту, підкріпивши вимоги конкретними даними». Є великий простір для розвитку. Сьогодні AI використовується в безпеці дуже обмежено. Можна говорити про відставання від інших галузей, і навіть разюче, що самокеровані автомобілі з'являються раніше, ніж мережі, що захищають самі себе. Нинішні платформи AI ще по суті не «розуміють» навколишній світ. Ці технології добре справляються із класифікацією даних, які схожі на зрізи і які використовувалися для навчання. Але штучний інтелект не є по-справжньому розумним – він не може зрозуміти ідею, що лежить в основі тієї або іншої атаки. Тому людина як і раніше є ключовим елементом будь-якого рішення в області кіберзахисту.

В інших областях, де зараз застосовується AI, наприклад у розпізнаванні образів, мови й прогнозуванні погоди, ситуація інша. Ураган не може змінити закони фізики й змусити воду випаровуватися якось по-іншому, щоб ускладнити вам завдання його виявлення. А у світі кібербезпеки все відбувається саме так».

І все-таки прогрес у боротьбі з кіберзагрозами є. Існує такий напрямок досліджень, як генеративні змагательні мережі, – коли одночасно працюють дві моделі машинного навчання із протилежними цілями. Наприклад, одна намагається щось виявити, а інша – сховати те ж саме від виявлення. Цим принципом можна користуватися при створенні команд умовного супротивника, щоб з'ясовувати, якими можуть бути нові погрози.

Розробка структурної схеми

Штучний інтелект, нейромережі, машинне навчання – у контексті інформаційної безпеки ці терміни сьогодні звучать всі частіше. У середовищі IT нерідкими стали розмови про наростаючу конкуренцію між людьми й машинами.

Деякі експерти впевнені, що застосування технологій машинного навчання й штучного інтелекту в сфері інформаційної безпеки – це питання відточування практики використання нових інструментів і підбора потрібних ваг і порогів, при яких дана функціональність активується в продуктах для забезпечення інформаційної безпеки. Важливо не зібрати якнайбільше даних – їх і так навколо дуже багато, а зрозуміти, як їх правильно структурувати і обробляти, щоб автоматизовані інструменти захисту працювали ефективно. І цей процес можна прискорити, якщо використовувати підходи, раніше відточені в інших областях.

Приміром, в IBM сьогодні створений цілий ряд ІБ-продуктів, які використовують потужності суперкомп'ютера Watson. Споконвічно цей проект запускався для сфери охорони здоров'я, але сьогодні це вже не настільки важливо – Watson уміє структурувати дані, і системі вже не так важлива конкретна галузь її застосування. Чи існують реальні застосування цього підходу? Так. Наприклад, розроблена IBM система може брати інформацію з інциденту (якийсь його артефакт), відправляти її в хмару, одержуючи у відповідь інформацію про те, де й коли він зустрічався раніше, а також набір рекомендацій з подальшого аналізу (скажемо, як інцидент може повторитися). Це дозволяє виявляти трояни й ботнети, які можуть у майбутньому брати участь в атаці, аналогічній вже здійсненій.

Технології розширюють можливості фахівців із захисту

Основний плюс нових технологій у сфері інформаційної безпеки полягає в тому, що вони значно розширюють можливості працюючих у галузі фахівців.

Приміром, по статистиці Microsoft, 96% злобливого софту проявляє активність один раз, а випадків, коли зловред атакує понад тисячу разів, усього 0,01%. Виділити з мільярдів сигналів і величезних масивів різноформатних даних інформацію, що реально важлива для відбиття атаки, украй складно. Людина витратить на такий аналіз занадто багато часу. І навпроти, убудована в Windows Defender система машинного навчання може проводити поведінковий аналіз мільярдів сигналів щодня. Це дозволяє значно скоротити час реагування на інциденти.

Так при атаці на звичайного користувача Windows (наприклад, з метою установки майнера в браузер), система розпізнає й блокує її за мілісекунди, а атаку на компанію enterprise-рівня система виявляє за кілька секунд. У підсумку на кожний екземпляр злобливого софту, проаналізований експертом компанії, існуюча система на базі Machine Learning і Artificial Intelligence забезпечує захист ще від 4500 зловредів.

Як вирішується проблема актуальності даних про уразливостях

Допомагають машинне навчання й штучний інтелект і в справі рішення проблеми підтримки актуальності інформації про кіберзагрозах. Сьогодні для визначення критичності уразливостей використовують різні схеми підрахунків (наприклад, CVSS) і калькулятори. Всі вони не враховують людський фактор, що може впливати. Те, які дані будуть уведені в калькулятор підрахунку CVSS score, залежить від людини, що, як показує практика, може бути підданий впливу ззовні.

Наприклад, якщо якусь уразливість активно обговорюють у медіа, те така погроза може йому здаватися більше серйозної, або навпаки – недолік информованості приведе до недооцінки. Крім того, навряд чи людина буде проводити повторний аналіз через час. У результаті виникають ситуації, як це було у випадку уразливості HeartBleed, чия базова оцінка CVSS споконвічно становила всього лише 5 з 10. При цьому практично миттєво сталі з'являтися експлойти для її використання – а виходить, із самого почала ризик був куди вище.

Якщо довірити підрахунок балів CVSS навченої моделі, то таких проблем можна уникнути й одержати постійно обновляється залежно від нових даних оцінку критичності в цей момент.

Ефективність можлива не тільки в хмарі

Не меншу ефективність технології машинного навчання можуть продемонструвати й стосовно до завдань захисту критичної інфраструктури, що стали суперактуальними в останні роки.

Однак у даному контексті, на відміну від хмарної моделі, використовуються локальні рішення, які не передають дані в зовнішній мир. Типовий промисловий об'єкт генерує до 10 тисяч сигналів у день (дані із сенсорів і т.п). Це великий, досить зашумленний потік даних.

Однак той факт, що всі дані корельовані й базуються на законах фізики, можна використовувати для створення автоматизованих засобів захисту, упевнені експерти.

Адже якщо атака на один елемент індустріальної системи впливає на сигнали, генеруємі іншими, то системи машинного навчання тут можуть «вивчити» взаємозв'язку між сигналами й генерувати пророкування про те, як зміна в одному з них вплине на інший.

Проте практичні спроби застосувати технології Machine Learning і Artificial Intelligence для рішення деяких завдань по захисту інформації буксують.

Наприклад, створення рішення по виявленню аномалій у трафіку й поводженні користувачів програмних продуктів на базі технологій ML і AI виявилося сполучене з різними проблемами.

І одна з основних – величезний обсяг даних, які необхідно проаналізувати в мережі досить великої компанії. Для того щоб робота мала сенс, аналізувати необхідно терабайти даних, які вкрай зашумлені.

Реалізувати по-справжньому ефективний підхід до фільтрації експертам поки не вдалося, і з такими проблемами, на його думку, зштовхнеться будь-який розроблювач «розумних» ІБ-рішень на базі нових технологій, тому що готових моделей для рішення цього завдання на сьогоднішній момент не існує.

Всі частіше в сфері інформаційних технологій ми чуємо про значимість науки про дані й про успішність застосування технологій машинного навчання. Динаміка останніх подій у світі інформаційної безпеки свідчить про серйозну трансформацію методів і технологій здійснення атак з боку зловмисників. Багато компаній зіштовхуються з атаками, при яких традиційні засоби захисту інформації виявляються не просто малоефективними, але й марними.

У зв'язку із цим, виникає питання – як захиститися компаніям в умовах, коли погрози неможливо формалізувати й описати сигнатурою?

Що таке Cyber Threat Hunting & Data Science?

Cyber Threat Hunting (тут і далі – також хантинг) – це процес проактивного й ітеративного пошуку й виявлення просунутих погроз, які неможливо виявити традиційними засобами захисту. Даний процес розпадається на ряд загальновизнаних технік хантингу.

Data Science – наука про дані, відповідальна за обробку й добування корисної інформації з масивів структурованих або неструктурованих даних. Термін Data Science окреслює досить об'ємну предметну область, що вимагає конкретизації в кожному окремому випадку. Так, якщо говорити про симбіоз Cyber Threat Hunting і Data Science, визначення останньої як науки про дані, трохи міняється. Термін «Data Science» у контексті Cyber Threat Hunting розкривається як набір технік і прийомів, за допомогою яких здійснюється хантинг і які несуть у собі специфічні принципи роботи з даними.

Всі представлені техніки Cyber Threat Hunting так чи інакше ставляться до предметного поля Data Science.

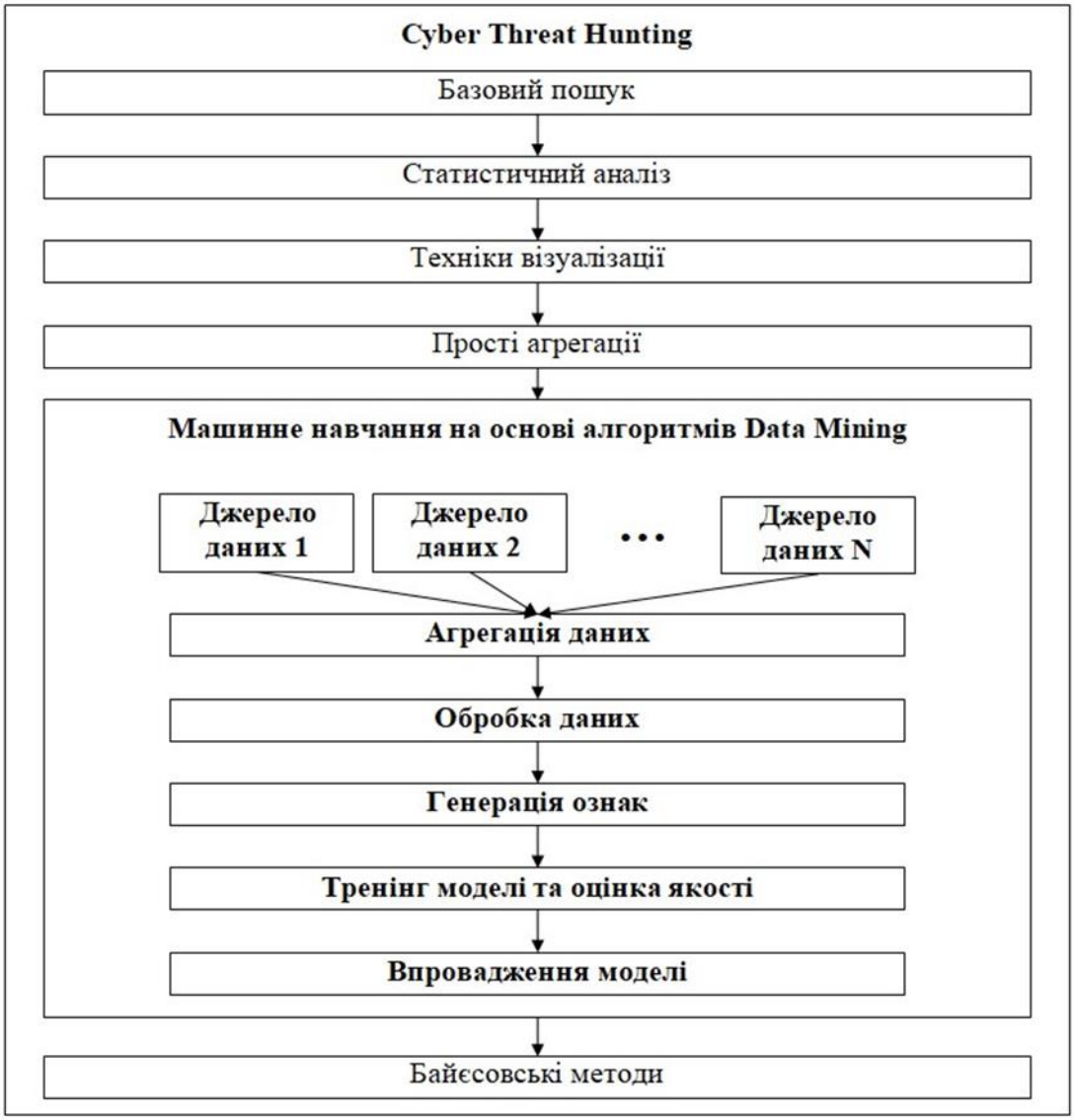


Рисунок 1 – Структурна схема системи

Далі розглянемо кожну з технік.

Техніки Cyber Threat Hunting

Базовий пошук

Базовий пошук – це найбільше часто використовувана техніка в Cyber Threat Hunting. Цей метод має на увазі використання спеціалізованих запитів, які повертають деякі результати пошуку. Через складність формалізації завдання по пошуку невідомої погрози не завжди можливо однозначно вказати, що шукає аналітик, коли починає пошук. Із цієї причини область пошуку не повинна бути ні занадто широкою, що охоплює безліч факторів і видає достаток результатів, ні занадто вузькою, тому що з'являється висока ймовірність упустити потенційні погрози, які не були включені в пошук.

Статистичний аналіз

Статистичний аналіз – це техніка, заснована на математичній моделі статистичних відхилень. Така модель застосовна для побудови типовий користувальницької / мережної активності з наступним виявленням аномальних подій. Основні етапи застосування даної техніки зазначені на прикладі завдання по виявленню DDoS-атак:

– створення поведінкових профілів, засноване на середньозваженому трафіку в розрізах min/hour/week/month;

– накладення в реальному часі отриманого поведінкового профілю на вступник трафік для здійснення щоденного моніторингу;

– у випадку відхилення від поведінкового профілю події ідентифікуються як аномальні із присвоєнням відповідного рівня ризику.

Техніки візуалізації

Техніки візуалізації являють собою інструменти по візуалізації даних. Після збору досить великого масиву даних виникає завдання їхнього аналізу. Одним зі способів рішення зазначеного завдання є візуалізація даних шляхом використання продуктів класу BI або аналогічних за функціоналом інструментів. Значно простіше побачити градацію подій за рівнем ризику, наприклад, на каскадній діаграмі, або помітити викиди й аномалії на крапковому графіку.

Прості агрегації

Прості агрегації – це техніка оптимізації аналізу. У процесі аналізу досить часто «сирі» вибірки даних мають невиправдано більші обсяги. Це негативно позначається на апаратних ресурсах, якості аналізу й результативності застосування аналітичних моделей. У зв'язку із цим дані обов'язково повинні бути агреговані по ключових полях з метою оптимізації пошуку й процесу аналізу в цілому.

Машинне навчання

Етапи створення математичної моделі на основі алгоритмів Data Mining

Алгоритми машинного навчання (Data Mining), у якості ще однієї техніки Cyber Threat Hunting, успішно застосовні при фільтрації спаму, виявленні шкідливого трафіку й детектувані шахрайських дій. Успішно впроваджені в процес хантингу алгоритми здатні істотно підвищити ефективність захисту інформації. Зазначені алгоритми можна впроваджувати в засоби захисту інформації, які вимагають серйозної ресурсної й організаційної підготовки, як в IT, так і в ІБ-секторі.

Дані алгоритми підрозділяються на два типи: «навчання із вчителем» і «навчання без вчителя».

Навчання із вчителем

Найпоширенішими завданнями для цього типу алгоритмів машинного навчання є завдання по класифікації й регресії. Рішення завдання класифікації дозволяє розподілити вхідні параметри по заздалегідь відомих групах, а рішення завдання регресії дозволяє пророчити конкретне значення для кожної із вхідних величин. Алгоритми рішення обох завдань можуть ефективно використовуватися в області інформаційної безпеки – стає можливим визначення критичності активу, що залежить від мережного розташування активу, знайдених уразливостей у програмному забезпеченні й інцидентах, що відбулися, на цьому активі. Також можливе пророкування користувальницької шкідливої діяльності усередині організації залежно від останніх дій користувача в інфраструктурі протягом часового зрізу (не менш місяця).

Навчання без вчителя

Типовим завданням для цього типу алгоритмів машинного навчання є кластеризація, тобто розподіл вхідних величин по групах, найменування й кількість яких заздалегідь невідомо. Через труднощі формалізації зазначеного завдання, її рішення є набагато більше складним розділом машинного навчання. В області інформаційної безпеки алгоритми типу «навчання без вчителя» орієнтовані на завдання пошуку схованих закономірностей у діях користувачів і виявлення шкідливого програмного забезпечення.

Байєсовскі методи

Байєсовскі методи – це «просунутий» тип алгоритмів машинного навчання, що дозволяє ефективно вирішувати такі завдання машинного навчання, як класифікація, зменшення розмірності й тематичне моделювання. При даному підході ймовірність можна інтерпретувати як міру незнання, а не як випадковість. Таким чином, використання байєсовских методів дозволяє задати чіткий математичний опис навчання й чисельні

метрики, що дозволяють оцінити якість і вірогідність деякого числа гіпотез, у той час як класичні підходи, як правило, дозволяють оцінити одну єдину гіпотезу.

Більшість виробників ринку інформаційної безпеки вже випускають готові рішення, що успішно використовують методи машинного навчання. У побудові процесу Cyber Threat Hunting можна використовувати як готові рішення, так і власні розробки.

Описані техніки, що ставляться до науки про дані, будучи інтегрованими в процеси Cyber Threat Hunting, дозволяють вирішити безліч актуальних завдань інформаційної безпеки, особливо тих, які на сьогоднішній день вирішуються традиційними засобами захисту неефективно або не вирішуються зовсім.

З кожним роком компанії роблять вибір на користь рішень із акцентом на проактивні технології захисту, а рішення, засновані на сигнатурних методах, стають усе менш ефективними й поступово йдуть на другий план. Для багатьох компаній вектор розвитку змістився убік впровадження технологій, що підтримують симбіоз Cyber Threat Hunting і Data Science.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів системи кібербезпеки побудованої на використанні Cyber Threat Hunting та Data Science. В межах України в недостатній мірі представлені вітчизняні розробки в цій області. У роботі наведені теоретичне узагальнення й рішення наукового завдання дослідження методів кібербезпеки побудованої на використанні Cyber Threat Hunting та Data Science. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем кібербезпеки побудованої на використанні Cyber Threat Hunting та Data Science; Досліджена система кібербезпеки побудованої на використанні Cyber Threat Hunting та Data Science; На основі отриманих результатів досліджень створена програмна реалізація системи кібербезпеки побудованої на використанні Cyber Threat Hunting та Data Science. Розроблені під час виконання роботи алгоритми дозволяють успішно вирішувати завдання кібербезпеки побудованої на використанні Cyber Threat Hunting та Data Science. 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. Смірнов О.А. Дисперсійний аналіз мережного трафіку для забезпечення інформаційної безпеки телекомунікаційних систем / О.О. Кузнецов, О.А. Смірнов, Д.О. Даниленко // Інформаційна та економічна безпека: сучасний стан та тенденції розвитку : монографія за заг. ред. – Х.: ХІБС УБС НБУ – 2014 – С. 82-100.
2. Смірнов О.А. Дослідження методів виявлення вторгнень в телекомунікаційні системи та мережі / Д.О. Даниленко, О.А. Смірнов, Є.В. Мелешко // Системи озброєння і військова техніка. – Випуск 1(29) – Х.: ХУПС – 2012. – С. 92-100.
3. Смирнов А.А. Метод обнаружения вредоносного программного обеспечения. Часть 1. Корреляционный анализ сетевого трафика // А.А.Смирнов, Д.А. Даниленко, Е.В.Мелешко // Науково-технічний журнал «Інформаційно-керуючі системи на залізничному транспорті» – Випуск 4(95). – Х.: УкрДАЗТ – 2012. – С. 8-14.
4. Смирнов А.А. Методы обнаружения вредоносного программного обеспечения в телекоммуникационных системах и сетях / Д.А. Даниленко // Збірник наукових праць "Системи обробки інформації". – Випуск 3(101) том 2. – Х.: ХУПС – 2012. – С. 152-155.
5. Смирнов А.А. Системы обнаружения и предотвращения вторжений для защиты телекоммуникационных сетей от вредоносного программного обеспечения / Д.А. Даниленко, А.А. Смирнов, А.В. Коваленко // Системи управління, навігації та зв'язку. – Випуск 1 (21) том 2. – Київ: ДП «ЦНДІНУ». – 2012. – С. 183-186
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» (ІІРТК-2012). м. Київ. 15-16 травня 2012 р. – Київ: НАУ. – 2012. – С. 314-315.

УДК 004

Є. Нестеряк, магістр гр. КН-19М-1,4
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ ВІДЕОНАГЛЯДУ ГАЗОВОГО РОДОВИЩА НА ОСНОВІ ОБЛАДНАННЯ AXIS

У статті розроблено програмне забезпечення, яке призначено для системи відеонагляду газового родовища на основі обладнання Axis. Метою розробки є дослідження та програмна реалізація системи відеонагляду газового родовища на основі обладнання Axis. Об'єктом дослідження є процес відеонагляду газового родовища на основі обладнання Axis. Предметом дослідження є методи відеонагляду газового родовища на основі обладнання Axis. Методи дослідження базуються на методах захисту інформації, методах обробки зображень, методах телетрафіку, методах математичної статистики, методах розробки програмного забезпечення. 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, відеонагляд, Axis

Постановка проблеми. За міжнародними показниками, Україна не бідна в енергетичному відношенні держава: при території, що дорівнює 0,4% світової, сировинні запаси надр України складають 5% світових.

З моменту першої появи систем відеоспостереження й контролю доступу компанії по видобутку газу починали впроваджувати їх і використовувати для контролювання внутрішньої території, периметра, пропускних пунктів і критично важливих об'єктів. Якийсь час назад діюча аналогова система відеоспостереження перестала відповідати корпоративним стандартам, виникла необхідність її модернізації.

Через критичну важливість проекту процедура вибору виробника системи відеоспостереження тривала більше року, після чого був проведений пілотний проект по установці близько 20 мережевих камер Axis на одному з об'єктів. Результати випробувань перевищили всі очікування, і в компанії вирішили продовжити модернізацію охоронної системи винятково на основі продукції Axis.

У цей час на заводах і на зовнішній території встановлено вже більше 400 камер Axis, проект поетапно розвивається. Основний використовуваний модельний ряд устаткування – мережеві камери Axis серій AXIS Q60, AXIS Q16, AXIS Q17, AXIS P33 і AXIS P56, але й триває розширяться модельний ряд використання. Удосконалена

технологія відеоспостереження дозволяє службі безпеки підприємства більш ефективно захищати інфраструктуру важливих об'єктів, утягуючи при цьому менше людських ресурсів і в такий спосіб заощаджуючи значні засоби на експлуатаційних витратах.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи відеонагляду газового родовища на основі обладнання Axis.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи відеонагляду газового родовища на основі обладнання Axis.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем відеонагляду газового родовища на основі обладнання Axis.

– Дослідження системи відеонагляду газового родовища на основі обладнання Axis.

– Програмна реалізація системи відеонагляду газового родовища на основі обладнання Axis.

Об'єктом дослідження є процес відеонагляду газового родовища на основі обладнання Axis.

Предметом дослідження є методи відеонагляду газового родовища на основі обладнання Axis.

Методи дослідження базуються на методах захисту інформації, методах обробки зображень, методах телетрафіку, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. На газовому підприємстві, де праця найчастіше пов'язана з ризиком для їхнього життя й здоров'я, постійний автоматизований контроль за дотриманням техніки безпеки й порядку критично важливий. Після декількох успішних проектів по заміні застарілого обладнання для відеоспостереження на камери Axis на об'єктах у компанії вирішили використовувати в майбутньому продукцію тільки компанії Axis Communications. Можна сказати, що мережеві камери Axis стали в замовника стандартом якості.

Для розуміння масштабу поточного проекту необхідно уточнити, що площа території, що займає газове родовище, становить 2500 кв. км. На десятках об'єктів – на родовищах, в адміністративних будинках, на складах, заводах, на транспорті – трудяться близько 3,5 тис чоловік. Основним функціональним завданням комплексної системи мережевого відеоспостереження є перегляд території й об'єктів, контроль за дотриманням співробітниками режиму й техніки безпеки, виконання поставлених завдань персоналом і підрядними організаціям, мінімізація крадіжок і проведення розслідувань. Відповідно, на підприємствах необхідна установка різних мережевих камер. Для огляду території необхідні пристрої із широким кутом і великою дальністю огляду, спроектовані для роботи в різних кліматичних умовах. Особлива увага повинне приділятися периметру, для захисту якого окремі моделі камер Axis мають спеціальні аналітичні можливості, у тому числі функцією контролю за перетинанням границі.

На контрольно-пропускних пунктах і усередині будинків установлюються більше компактні камери, з метою розпізнавання осіб – це допомагає в забезпеченні порядку й розслідуванні інцидентів. Тут також застосуємо «коридорний» формат запису, що забезпечує економію місця на пристроях зберігання даних.

У компанії не бояться експериментувати: недавно була закуплена для тестування тепловізійна мережева камера AXIS серії Q19, виконується проектування по використанню недавно анонсованих Радарів AXIS D 2050-VE, розглядаються варіанти використання встаткування контролю доступу виробництва Axis.

Компанія використовує програмне забезпечення, що має можливість повної інтеграції системи відеоспостереження із системою контролю доступу й інших спеціальних

функцій, а також аналітики. Знаходять своє застосування в проекті також інтелектуальні функції камер і аналітичні здатності відкритої платформи Axis, куди можна встановити відповідне ПЗ й почати одержувати дані будь-якого характеру.

Представники служби безпеки компанії свідчать про те, що завдяки якісній передачі зображення, можливості зручного зберігання й оперативного перегляду записів, а також аналітичним функціям, сучасна система відеоспостереження на основі мережевих камер дійсно більш ефективно, ніж колись аналогова, допомагає усувати причини будь-яких позаштатних ситуацій, стимулювати персонал до дотримання техніки безпеки, захищати критичні активи компанії.

В 2016 році компанії-партнери спільного підприємства остаточно затвердилися у фінансуванні Проекту майбутнього розширення (Future Growth Project – FGP) – Проекту керування гирловим тиском, що є наступним етапом розширення виробничих потужностей родовища. Сьогодні в рамках FGP на території підприємства будується новий нафтопереробний завод, на якому планується використовувати камери Axis як на зовнішніх об'єктах, так на самих заводських установках – у вибухозахищеному виконанні ATEX. Так само було ухвалене рішення використовувати продукцію Axis у проекті будівництва нового заводу й на тимчасових об'єктах у період будівництва.

Відомо, що компанія вже закупила першу партію вибухозахищених камер Axis серій XF і XP для установки на діючих заводах

Пріоритетна продукція

Мережеві тепловізори Axis в умовах темряви працюють значно краще оптичних камер, а також відмінно підходить для виявлення людей і об'єктів при цілодобовому відеоспостереженні, в умовах від повної темряви до залитої сонцем автостоянки.

Тепловізійні камери Axis

У мережевій купольній камері AXIS Q 6155-E PTZ Dome Network Camera застосовується сучасна лазерна технологія, тому вона ідеально підходить для відеоспостереження там, де потрібна миттєве фокусування на об'єктах, що рухаються, і швидко мінливій обстановці.

PTZ-камери Axis

Мережевий радар-детектор Axis прекрасно підходить для моніторингу невеликих площ на відкритому повітрі. Цей пристрій служить доповненням до системи охоронного відеоспостереження поряд з мережевими камерами Axis, рупорними гучномовцями Axis і іншими мережевими пристроями.

Мережевий радар-детектор AXIS D 2050-VE Network Radar Detector

Фіксовані мережеві камери серії AXIS Q16, призначені для установки в приміщеннях і на відкритому повітрі, забезпечують найвища якість зображення в складних умовах відеоспостереження, наприклад при низькому або постійно, що змінюється рівні, освітленості.

Розробка структурної схеми

Працюючи з Axis, ми допомагаємо вам повною мірою використовувати потенціал мережевого відеоспостереження для рішення наступних завдань:

- захист персоналу, майна й активів;
- оптимізація процесів;
- підвищення ефективності бізнесу.

Рушійна сила для розвитку мережевого відеоспостереження складається з таких компонентів як ресурси, висококваліфіковані кадри й досвід, які є в нашому розпорядженні і які допомагають вам використовувати відеоспостереження для досягнення ваших цілей.

Компанія Axis пропонує широкий діапазон рішень для найрізноманітніших галузей і сфер застосування. Незалежно від того, скільки вам потрібно камер – кілька штук або кілька тисяч штук – наші рішення нескладно встановити й легко адаптувати до мінливих потреб. Коротше кажучи, ми пропонуємо економічні системи, які будуть залишатися актуальними не один рік.

Стійкі результати

Крім того, також пропонуємо спеціальні рішення для особливих ситуацій. Чи не час розширити й модернізувати вашу існуючу аналогову CCTV-Систему? Ви займаєтеся установкою своєї першої системи охоронного IP-відеоспостереження? Ми можемо запропонувати масштабоване рішення на основі відкритих стандартів, що забезпечить вам одержання стійких результатів. При цьому в нас є рішення для роботи в приміщеннях і на вулиці, для провідної й бездротової мережі, а також спеціально для найсуворіших умов і віддалених об'єктів.

Тільки відкриті стандарти

В основі рішень Axis лежить відкритий інтерфейс прикладного програмування, розроблений у компанії Axis (VAPIX®), тому рішення характеризуються простотою інтеграції й масштабованістю за рахунок використання відкритих технологічних стандартів, стандартних мереж і IT-устаткування. Помітимо, що Axis відіграє провідну роль у рамках ONVIF, глобальної ініціативи по стандартизації для мережевих відеопродуктів.

Разом зі своїми партнерами компанія Axis створює рішення для відеоспостереження, придатні для будь-яких типів підприємств і розмірів установки, і ці рішення допоможуть вам реалізувати своє бачення – як у цей час, так і в майбутньому.

Рисунок 1 – Структурна схема системи

Система мережевого відеоспостереження дозволяє переглядати й записувати відео з будь-якої крапки мережі, незалежно від того, локальна це мережа або глобальна, така як Інтернет.

Системи мережевого відеоспостереження, також часто називані системами відеоспостереження на базі IP або охоронним IP-відеоспостереженням, використовують провідну або бездротову IP-мережу як середовище передачі відео, аудіо й інших даних. При використанні технології Power over Ethernet (PoE) мережею також можна здійснювати живлення пристроїв мережевого відеоспостереження.

Система мережевого відеоспостереження дозволяє переглядати й записувати відео з будь-якої крапки мережі, незалежно від того, локальна це мережа або глобальна, така як Інтернет.

Базовими компонентами системи мережевого відеоспостереження є мережева камера, відеокодер (застосовується для підключення аналогових камер), мережа, сервер і система зберігання, а також ПЗ для керування відео. Мережеві камери й відеокодери створені на основі комп'ютерів, тому вони мають можливості, недоступними аналоговим камерам. Мережева камера, відеокодер і ПЗ для керування відео- це основа для рішення по охоронному IP-відеоспостереженню.

Мережа, системи зберігання й сервери – стандартне IT-устаткування. Здатність використовувати звичайне серійне встаткування – одне з головних переваг мережевого відео. Інші компоненти системи мережевого відеоспостереження містять у собі різні аксесуари: кожухи для камер, інжектори живлення за технологією PoE, активні розгалужувачі. Детальні описи кожного з компонентів можна знайти в інших розділах.

Переваги

Цифрова система мережевого відеоспостереження має переваги й функціональністю, недоступними аналоговим системам спостереження. До таких переваг ставляться: можливість віддаленого доступу, висока якість зображення, керування подіями й інтелектуальними відеотехнологіями, простота в інтеграції й розширюваність, гнучкість і економічну ефективність.

Простота в інтеграції й орієнтованість на майбутній розвиток

Засновані на відкритих стандартах пристрої мережевого відеоспостереження легко інтегруються з комп'ютерними й заснованими на технології Ethernet інформаційними системами, з аудіосистемами й системами безпеки й інших цифрових пристроїв поряд з ПЗ для керування відео. Наприклад, відео з мережевої камери може бути інтегроване в касовий термінал або в систему керування будинком.

Висока якість зображення

У рішеннях для охоронного відеоспостереження якість зображення відіграє головну роль для можливості чітко зафіксувати що відбувається і ідентифікувати учасників.

Використання прогресивного розгорнення й мегапіксельної технології в мережевих камерах дозволяє досягти кращої якості й більшого дозволу зображення, чим в аналогових камерах.

Також, у системі мережевого відеоспостереження домогтися високої якості зображення простіше чим в аналогових системах охоронного спостереження. У цей час в аналогових системах, що використовують цифрові відеореєстратори, відбувається кілька аналого-цифрових перетворень: спочатку аналогові сигнали перетворяться в камері в цифрові, потім назад в аналогові для передачі, а після знову оцифровується при записі. Якість зображення, що зберігається, погіршується з кожним перетворенням і при великій довжині кабелів. Чим більше дальність передачі аналогового відеосигналу, тим слабкіше він стає.

У повністю цифровій системі охоронного IP-відеоспостереження зображення оцифровується один раз у мережевій камері й потім залишається в цифровому виді, без непотрібних перетворень і втрат якості поза залежністю від дальності передачі мережею. Також, цифрове зображення легше зберігати й одержувати до нього доступ, у порівнянні з аналоговими відеокасетами.

Економічна ефективність

Сукупна вартість володіння в системи IP-відеоспостереження звичайно нижче чим у традиційної аналогової системи відеонагляду.

Часто в організації вже існує й використовується мережева IP-Інфраструктура, яку можна використовувати для мережевої системи відеоспостереження. У цілому дротові й бездротові IP-мережі є менш дорогою альтернативою традиційним коаксіальним і оптичним кабельним мережам для аналогових систем відеоспостереження. Крім того, цифрові відеопотоки можуть передаватися по усьому світі, використовуючи різні канали зв'язку. Застосування серверного встаткування, що відповідає промисловим, відкритим стандартам для запису й зберігання, а не закритого спеціалізованого апаратного забезпечення, як у випадку із цифровими відеореєстраторами в аналогових системах відеоспостереження, також дозволяє знизити витрати на встаткування й керування.

Більше того, у системах мережевого відеоспостереження може бути використана технологія Power over Ethernet (PoE), недоступна для аналогових систем. PoE дозволяє подавати живлення на мережеві пристрої від комутатора або інжектора з підтримкою PoE по кабелю для передачі даних (відео). Технологія PoE дозволяє досягти реальної економії у

витратах на монтаж і збільшити надійність системи. Додаткову інформацію про Power over Ethernet.

Розширюваність і гнучкість

Система мережевого відеоспостереження може бути розширена відповідно до потреб користувача. Системи відеоспостереження на базі IP дозволяють використовувати в одній провідній або бездротовій мережі велика кількість мережевих камер і відеокодерів, тому додавання будь-якого числа додаткових пристроїв мережевого відеоспостереження може здійснюватися без складних або витратних змін у мережевій інфраструктурі.

В аналогових системах подібне неможливо. До кожної станції спостереження/запису в аналоговій системі необхідно підводити коаксіальний кабель від кожної камери. Також потрібні окремі аудіокабелі, якщо необхідно звук. Пристрою мережевого відеоспостереження можуть бути розташовані й доступні практично де завгодно в мережі, а сама система може бути й відкритої, і закритої.

Керування подіями й інтелектуальні відеотехнології

Найчастіше, при великих обсягах записаного відео бракує часу для якісного аналізу записів.

Мережеві камери й відеокодери з убудованими інтелектуальними або аналітичними функціями допомагають вирішувати цю проблему, зменшуючи кількість непотрібних записів і використовуючи заздалегідь певні події. Такі можливості недоступні в аналогових системах.

Мережеві камери й відеокодери Axis мають наступні убудовані функції: детектор руху, детектор звуку, активне оповіщення при несанкціонованих діях, рознімання уведення-виводу, а також можливість керування подіями й оповіщеннями. Ці функції дозволяють мережевим камерам і відеокодерам постійно аналізувати входи для виявлення подій і автоматично реагувати на події різними способами, такими як запис відео або відправлення повідомлень із оповіщенням.

Функції керування подіями можна настроїти як за допомогою користувальницького інтерфейсу пристрою мережевого відеоспостереження, так і за допомогою ПЗ для керування відео. Користувачі можуть задати тип оповіщення або події, набудовуючи час і тип спрацьовувань. Також можна настроїти реакцію на події (наприклад запис на один або трохи локальних або віддалених носіїв; активація зовнішніх пристроїв, таких як звукові й світлові сигнали або двері; відправлення повідомлень користувачам).

Віддалений доступ

Мережеві камери й відеокодери можна набудовувати віддалено, забезпечивши можливість декільком авторизованим користувачам переглядати зображення в режимі реального часу й записувати відео в будь-який час і практично з будь-який, що має доступ у мережу, крапки миру. Дана функція корисна якщо необхідно надати доступ до відео стороннім особам, наприклад представникам.

Проста й надійна установка

Система охоронного IP-відеоспостереження відрізняється швидкістю й простотою установки. У мережевих камерах і відеокодерах Axis передбачена підтримка технології Power over Ethernet, що додатково полегшує процес установки, оскільки один кабель забезпечує й живлення камери, і передачу відео. Використання моделей, підготовлених для зовнішнього застосування у вандалозахищеному виконанні також вносить свій внесок у прискорення процесу установки й гарантує одержання відмінних відеозображень навіть у самих несприятливих умовах.

Цифрове керування панорамуванням, нахилом і зумом, дистанційний зум і фокусування дозволяють зручно регулювати кут огляду камери й фокус із комп'ютера мережею. Коридорний формат Axis дає можливість установникові змонтувати камеру найбільш ефективним образом для наявної ситуації, а лічильник пікселів допомагає перевірити відповідність системи будь-яким нормативним вимогам або конкретним вимогам замовника.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів відеонагляду газового родовища на основі обладнання Axis. В межах України в недостатній мірі представлені вітчизняні розробки в цій області. У роботі наведені теоретичне узагальнення й рішення наукового завдання дослідження методів відеонагляду газового родовища на основі обладнання Axis. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем відеонагляду газового родовища на основі обладнання Axis; Досліджена система відеонагляду газового родовища на основі обладнання Axis; На основі отриманих результатів досліджень створена програмна реалізація системи відеонагляду газового родовища на основі обладнання 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.

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. Пасевич, магістр гр. КІ-19М
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ ІНТЕРНЕТ-ГІПЕРМАРКЕТУ З ВИКОРИСТАННЯМ REACT З ECMASCRIPT 2018

У статті розроблено програмне забезпечення, яке призначено для системи інтернет-гіпермаркету з використанням react з ecmascript 2018. Метою розробки є дослідження та програмна реалізація системи інтернет-гіпермаркету з використанням react з ecmascript 2018. Об'єктом дослідження є процес побудови та програмна реалізація системи інтернет-гіпермаркету. Предметом дослідження є методи побудови та програмна реалізація з застосунку з використанням react з ecmascript 2018. Методи дослідження базуються на методах побудови та програмна реалізація, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи інтернет-гіпермаркету з використанням react з ecmascript 2018. 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 інтернет-гіпермаркету, React, ecmascript 2018

Постановка проблеми. Розробка Інтернет-гіпермаркету та його використання є актуальним питанням на сьогоднішній день, оскільки мільйони людей щодня, не виходячи з дому, купують різні товари в електронних гіпермаркетах. В світі, а зокрема в Україні величезними темпами росте кількість користувачів Інтернет і, як наслідок, кількість «електронних» покупців.

Інтернет зближує, реакція на будь-яку подію поступає практично негайно, а відстані зникають. Інтернет-гіпермаркети істотно зменшують витрати виробника, заощадивши на утриманні звичайного гіпермаркета, розширюють ринки збуту, так само як і розширює можливість покупця - купувати будь-який товар у будь-який час в будь-якій країні, в будь-якому місті, у будь-який час доби. Це дає Інтернет-гіпермаркетам перевагу перед звичайними гіпермаркетами. Цей момент є істотним під час переходу виробників із «звичайної» торгівлі на «електронну».

Інтернет-гіпермаркети, що пережили кризу, укріпили свої позиції на ринку, за рахунок скуповування менш вдалих конкурентів. Гіганти оффлайнового бізнесу, в 1999 році що коштували в десятки разів дешевше за своїх онлайнових побратимів, після кризи теж дістали можливість вийти на ринок Інтернету, запропонувавши вищу якість послуг і гучне ім'я.

В Україні у сфері електронної комерції традиційно працюють фірми по наданню послуг доступу в Інтернет: web-портали, пошукові машини, електронні пошти. Тут немає ні лідерів оффлайнового ринку, ні представництв крупних міжнародних Інтернет-компаній.

Традиційний ринок інтернет-комерції зароджувався як ринок роздрібної торгівлі. Але поступово на ринку стали з'являєтися рішення, орієнтовані не на кінцевих споживачів, а на організації, так званий ринок B2b, або business-to-business.

Спочатку, на ринку B2b пропонувалися продукти, пов'язані власне з організацією роздрібної торгівлі (готові Інтернет-гіпермаркети, послуги з реклами, впровадження Інтернет-торгівлі в традиційні бізнес-процеси і тому подібне). Але поступово через Інтернет почали продаватися рішення, безпосередньо з Інтернет не зв'язані (комерційне програмне забезпечення, послуги з автоматизації, оптова торгівля, брокерські послуги, і тому подібне).

З всього вище сказаного однозначно зрозуміла актуальність питання дослідження Інтернет-гіпермаркету та його розробки з використанням сучасних Internet-технологій. В рамках магістерської дипломної роботи перед нами було поставлено завдання розробити Web-сайт «Інтернет-гіпермаркет».

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи інтернет-гіпермаркету з використанням react з ecmascript 2018.

Мета й завдання дослідження. Проаналізувати специфіку діяльності Інтернет гіпермаркетів, їх відмінності від звичайних гіпермаркетів, розглянути сучасні засоби по розробці Інтернет-гіпермаркетів та розробити web-сайт „Інтернет-гіпермаркет”.

Завдання роботи*:*

1. Здійснити пошук інформації по тематиці магістерської дипломної роботи та провести її аналіз та дослідження.
2. Ознайомитись з особливостями інтернет-гіпермаркети, його позитивними та негативними якостями, та визначити їх класифікацію.
3. Розглянути існуючі інтернет-гіпермакети та вивчити їх принципи побудови та роботи.
4. Розглянути структуру побудови інтернет-гіпермаркетів.
5. Провести маркетингове дослідження.
6. Розглянути сучасні програмні засоби по розробці інтернет-гіпермаркетів.

Розробити інтернет-гіпермаркет з використанням фреймворку React та Ecmascript 2018.

Виклад основного матеріалу. Інтернет-магазин (англ. *Internet shop*, англ. *Online shop*) – місце в інтернеті, де відбувається прямий продаж товарів споживачеві (юридичній або фізичній особі), враховуючи доставку. При цьому розміщення споживацької інформації, замовлення товару і угода відбуваються там само, всередині мережі (на сайті інтернет-магазину).

Електро́нний магази́н (*е-магазин, e-shop*) – сайт, з якого можна вибрати та замовити потрібний товар чи послугу. Інтернет-магазин перш за все передбачає грошові розрахунки на відміну від сайтів, які надають послуги безкоштовно. Для безпечного використання сайту передбачені надійні протоколи – https, та інші системи безпеки.

Інше визначення Internet-магазину характеризує його як реалізоване в мережі Internet представництво шляхом створення Web-сервера для продажу товарів та пов'язаних з ними послуг користувачам Internet. Кількість представлених на сервері видів товарів може коливатися від кількох одиниць до кількох тисяч.

Важливі елементи інтернет-магазину — оновлення наявного асортименту (продукти/товари та їх кількість), можливість додавати товари до «кошику», вхід для зареєстрованих користувачів. У деяких випадках можна використовувати систему оплати через інтернет (електронні гроші), у простішому випадку оплата відбувається звичайними грішми через банк на рахунок, роздрукований з сайту. Оплата через інтернет передбачає необхідність створення кількох облікових записів (принаймні двох), але у деяких випадках системи оплати можуть бути пов'язаними з магазином.

Для того, щоб інтернет-магазин видавав інформацію залежно від запитів, надавав можливості пошуку тощо – на сервер встановлюється підтримка скриптів (наприклад PHP, Perl). У більш комплексному варіанті, програма інтернет-магазину — це система управління вмістом сайту, яка вже має підтримку скриптів, надає можливість в он-лайновому режимі (головним чином через інтернет) і в межах наявного асортименту виконувати купівлю потрібних товарів.

WEB-сайт має бути розміщений на цілодобово функціонуючому сервері з високою пропускною спроможністю каналу. Умови навколишнього середовища повинні відповідати умовам експлуатації серверів, які вказуються в інструкції з експлуатації сервера. Адміністратор WEB-сайту повинен стежити за станом баз даних і їх наповненням. Сайт має

бути розрахований на користувача, не знайомити з програмування, кількість переходів по посиланнях для отримання необхідної інформації, яку необхідно сприйняти і переробити користувачеві для навігації по WEB- сайту, має бути мінімальною. Завантаження WEB-сторінок повинне відбуватися в середньому за 10-15 секунд. Естетичне оформлення WEB-сайту повинне викликати позитиву реакцію користувача. При їх недотриманні розробник сайту не несе відповідальність за коректність роботи сайту та збереження інформаційних ресурсів. У кожного свої особливості й переваги для бізнесу.

Internet-магазини потребують значно менших витрат на утримання та організацію роботи, оскільки у ньому значно обмеженіша матеріально-технічна база (будівлі, споруди, приміщення) та кількість обслуговуючого персоналу.

Проте Internet-магазини мають і недоліки. Основними є невизначеність реального існування товару та відповідність його основним параметрам якості, шахрайства при проведенні грошових трансакцій, проблеми з доставкою.

Основними вимогами, які ставляться користувачами до Internet-магазину є:

– зрозумілий інтерфейс та зручна система навігації по магазину;

– зручна система посилань, що дозволяє оптимальним способом одержати необхідну користувачеві інформацію;

– мінімальна кількість дій користувача для здійснення покупки.

За Інтернет-магазинами – майбутнє. Уже сьогодні тисячі людей при купівлі техніки та інших видів товарів віддають перевагу їм, а не реальним магазинам. Звісно, адже в Інтернеті практично завжди дешевше. Єдиний недолік – може часто прибути не той товар або недоукомплектований. Ну і замовляючи на деяких ресурсах товар, приходиться чекати іноді тижнями. Але чим далі, тим Інтернет-магазини працюють чіткіше, навіть в нашій країні помітно цю позитивну тенденцію.

Створення Інтернет-магазину коштує дешевше; вартість його на декілька порядків нижче за реальний магазин; для обслуговування Інтенет-магазину достатньо 1-2 людей, кількість товару необмежена, переглянути товар можна 24 години на добу.

До того ж, Ви економите свій дорогоцінний час, замовляючи що-небудь в Інтернет-магазині: нікуди не їздите і не шукаєте товари, не «ламаєте» свій щільний графік (адже такі магазини працюють цілодобово і без вихідних), не бігаєте по торговому залу, запам’ятовуючи ціни, моделі та характеристики, не вистоюєте черги в касі, знаходите усе по ключовому слову.

Слід звернути увагу і на такі переваги Інтернет-магазинів як детальна інформація про товари чи послуги (всіх дістає випитувати некомпетентного або лінивого консультанта про характеристики товарів), можливість порівняти оцінки та відгуки інших покупців, ну і найважливіше для більшості батьків – відсутність незручностей, пов’язаних із покупкою товарів чи послуг разом з дітьми.

Оцінивши такі можливості, ви напевне поспішите шукати в Інтернеті потрібні об’єкти, проте не забудьте, що ідеального не існує, і запам’ятайте деякі думки відносно недоліків Інтернет-магазинів. Ними є неможливість відчути товар (картинки, описи не дають повної можливості оцінки) та тривале очікування доставки товару (хоча в цьому є і плюс – здійснивши покупку імпульсивно, Ви можете передумати, поки товар не прийде).

Але в будь-якому випадку спочатку оцініть усі можливі товари, почитайте відгуки покупців, а потім робіть вибір. Є деякі Інтернет-магазини, що дають на вибір декілька моделей товарів, із яких Ви обираєте ту, яка вам підходить.

Взагалі товари, що пропонуються Інтернет-магазинами, є відображенням бажань та потреб покупців. Те, що потрібно Вам часто та у великій кількості – одразу ж з’являється у магазині. Наприклад, найбільш популярними товарами є книжки та канцтовари. Є статистика, за якою 56 % покупців роблять замовлення на даний товар. Побутова техніка потрібна приблизно 40 % покупців, з них – 39 % – купляють комп’ютери та комплектуючі.

Всесвітній розвиток Інтернет-комерції у всій її різноманітті не обійшов стороною й Україну. Незважаючи на ще відносно невелику кількість користувачів Інтернет у нашій країні, розвиток подібних форм бізнесу в нас вважається перспективним.

Міжнародний центр інформаційних технологій, що зайнявся розробкою і впровадженням Інтернет-комерції біля двох років тому, – www.int-coinmerce.com – представляє зараз найбільш відому і реально працюючу систему.

Система Інтернет-комерції або скорочено СІК, а в англійському варіанті SIC (System for InternetCommerce), – це комплекс організаційних, технічних, комунікаційних і програмних засобів, призначених для створення і розвитку середовища взаємодії суб'єктів комерційної діяльності в Інтернет. На основі цієї технології працює декілька сайтів, розрахованих на ведення продажів через Інтернет в основному українським споживачам.

Це електронні магазини – www.bampooh.com і www.duratshop.com, що приймають оплату за замовлення в режимі он-лайн платіжних карток клієнтів із застосуванням системи криптографічного захисту інформації.

У технологічному плані СІК – це інтегрований комплекс підсистем:

– платіжна і торговельна підсистеми (тобто back office продавця для керування складом, вітринами магазину, обробкою замовлень клієнтів);

– підсистема захисту (криптографічний захист інформації, моніторинг, адміністративний контроль);

– підсистема оператора, що підтримує всі підсистеми і виконує адміністративні функції.

Розробка структурної схеми

JavaScript в останні роки розвивається семимильними кроками, що не можна сказати про користувачів. На жаль, ми не можемо підтримувати тільки останні версії браузерів, так як мало хто серед замовників готовий пожертвувати істотною частиною аудиторії на догоду "класним технічним фічам". На щастя, придумані інструменти, які дозволяють програмісту використовувати найбільш сучасні конструкції мови і писати так, як йому зручно, а в результаті буде виходити код, який буде працювати правильно навіть в дуже древніх браузерах

React-розробка полягає в описі того, що потрібно вивести на сторінку (а не в складанні інструкцій для браузера, присвячених тому, як це робити). Це, крім іншого, означає значне скорочення обсягів шаблонного коду.

У складі Angular, з іншого боку, є засоби командного рядка, які генерують шаблонний код компонентів. Чи не здається це трохи не тим, чого можна чекати від сучасних інструментів розробки інтерфейсів? Фактично, мова йде про те, що в Angular так багато шаблонного коду, що для того, щоб його генерувати, навіть створено спеціальний засіб.

У React, приступаючи до розробки, просто починають писати код. Тут немає шаблонного коду компонентів, який потрібно якось генерувати. Звичайно, перед розробкою потрібна деяка підготовка, але, коли справа доходить до компонентів, їх можна описувати у вигляді чистих функцій.

Структурна схема інтернет магазину насправді дуже проста:

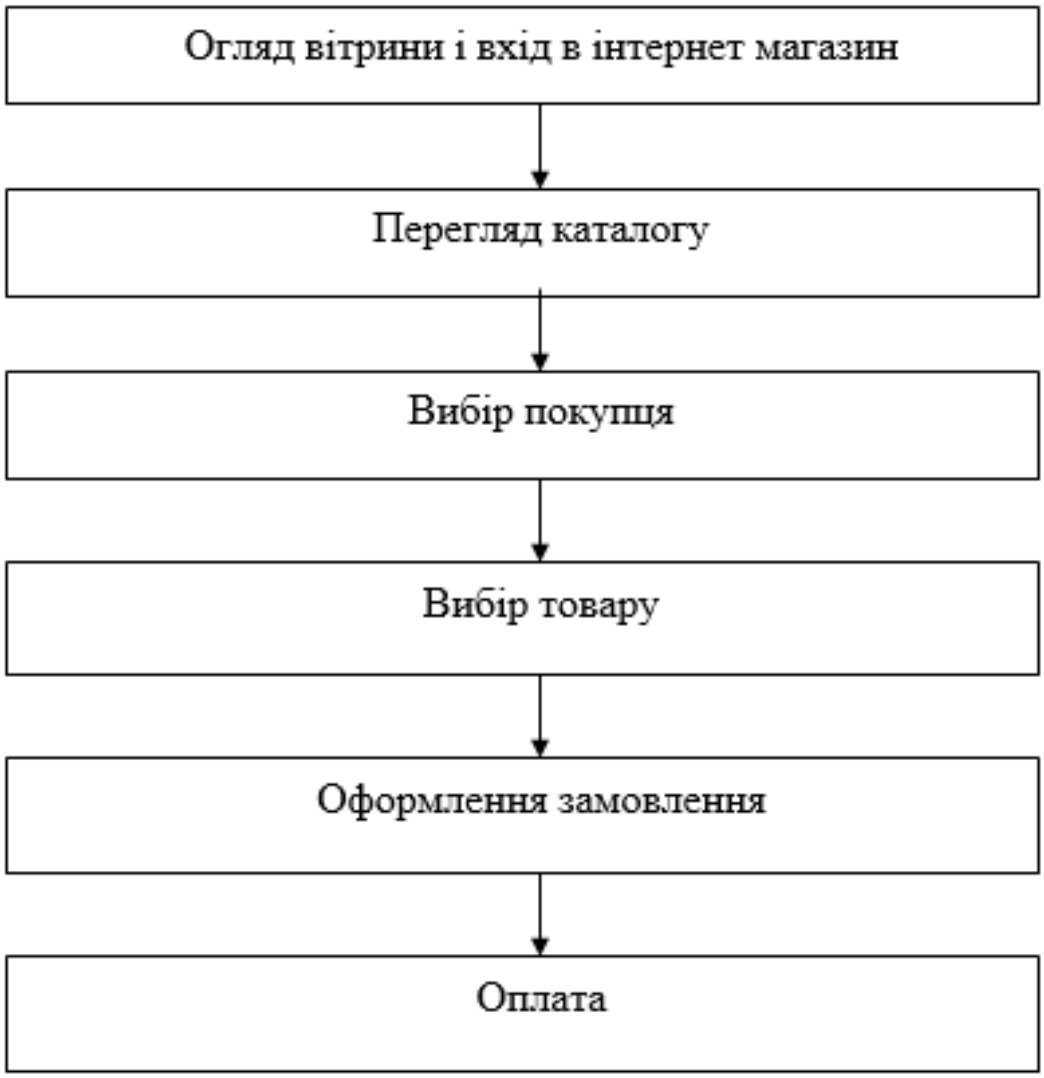


Рисунок 1 – Структурна схема системи

Епоха, яка передувала появі Internet, передбачала наявність стандартного життєвого циклу продукту. На початковому етапі створювався попит на пропоновані товари, і першопрохідники діставали максимальний прибуток за рахунок переважного становища на ринку. Потім формувався масовий попит, і послідовники отримували прибуток за рахунок ефективних способів виробництва.

Internet скоротив часові рамки, протягом яких відбувається засвоєння товару ринком. Новий сценарій життєвого циклу продукту не залишає місця для успішних попутників.

Для виживання в конкурентному середовищі менеджерам електронної комерції необхідні спеціальні інструменти, що допомагають в адмініструванні електронного бізнесу.

Моделі електронного бізнесу і їхня відмінність від традиційного бізнесу, мабуть, є темами електронної комерції, які дискутуються найбільше. У загальному значенні, модель ведення бізнесу – це метод його здійснення, за допомогою якого компанія може існувати й одержувати доход.

Деякі традиційні моделі досить прості. Наприклад, компанія виготовляє товари чи надає послуги, і при позитивному результаті дохід від продажів перевершує витрати, тобто компанія дістає прибуток.

Типова схема взаємодії покупця з Internet-магазином здійснюється наступним чином:

1. Покупець за допомогою браузера заходить на сайт Internet-магазину, який містить електронну вітрину, де представлений каталог товарів та необхідні елементи інтерфейсу для виконання операцій відбору та купівлі товарів.

2. Перегляд товарного каталогу та вибір товарів (формування кошика покупця).

3. Реєстрація покупця.

4. Вибір форми оплати та доставки товару.

5. Підтвердження замовлення.

6. Оплата товару.

7. Доставка придбаного товару покупцеві.

Пошук товарів в Internet-магазині може здійснюватися за допомогою каталогу або через внутрішню пошукову систему.

Каталог товарів повинен містити якнайповнішу інформацію про товар, мати зручну структуру, пошук необхідного товару повинен займати якнайменше часу. Саме за допомогою каталогу можна здійснити огляд товару (найчастіше у вигляді фото), ознайомитися з його споживчими та технічними характеристиками (у вигляді тексту та символів), ціною. Важливу роль в даному випадку можуть відігравати технології 3D (технології тривимірного зображення), завдяки яким товар можна оглянути з усіх боків, відкрити кришку тощо. Проте використання таких технологій висуває додаткові вимоги до технічних можливостей комп'ютера клієнта.

Інформаційна підтримка потенційного покупця полягає в наданні йому в будь-який момент відповіді на питання, що виникають при здійсненні покупки. Найчастіше така інформація стосується умов післяпродажного сервісу, знижок на певні товари, особливостей схем оплати і т. п. У багатьох випадках на сайтах електронних магазинів існують спеціальні сторінки, де подані відповіді на найважливіші питання.

У процесі перегляду і відбору товару покупець формує власний віртуальний кошик. Кошик покупця являє собою список відібраного товару з вказанням його ціни, кількості та загальної вартості (з урахуванням можливих знижок). Такий список постійно доступний покупцеві. За його бажанням у будь-який момент будь-який товар може бути вилучений з кошика з відповідним подальшим перерахуванням вартості, або може відбутися повне очищення кошика.

Коли зроблено остаточний вибір товару, покупцеві слід підтвердити замовлення, зареєструватися за встановленою процедурою з визначенням форми оплати та доставки товару.

Реєстрація полягає у заповненні покупцем спеціальної форми, що включає в себе інформацію про покупця, його поштову і (або)електронну адресу, особистий пароль та деяку іншу. Процедура реєстрації дозволяє Internet-магазинові убезпечити себе від можливих шахрайств та полегшити процедуру покупки для покупця наступного разу.

Реєстрація може здійснюватися до і після вибору товару. В першому випадку створюється спеціальний вхід для постійних клієнтів, для яких реалізується спеціальна система обслуговування та оплати. Реєстрація після вибору товару дозволяє покупцю зберегти анонімність відвідування магазину та заощаджує час, якщо покупець нічого не вибрав.

Під час проведення реєстрації особиста інформація покупця забезпечується шляхом передачі даних з використанням спеціальних методів захисту. Такими засобами можуть виступати протоколи SET або SSL.

Обробка замовлення покупця здійснюється безпосередньо торговою системою Internet-магазину і починається з перевірки наявності товарів на складі та його резервування. Якщо певний товар в даний момент відсутній, то система інформує покупця про можливу затримку виконання замовлення. Пізніше, якщо здійснюється оплата через Internet, виконується запит до визначеної платіжної системи та оформлення замовлення на доставку товару. Покупець в цей час може одержувати інформацію про проходження

замовлення. плата покупцем придбаного товару в Internet-магазинах може здійснюватися шляхом передоплати та при одержанні товару.

До варіанту передоплати можна віднести оплату при передачі інформації через Internet, при доставці звичайної чи експрес-пошти, магістральним транспортом, за допомогою захищених угод (схем, пов'язаних із резервуванням суми покупки на рахунку покупця з дійсним переказом коштів після здійснення поставки).

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів інтернет-гіпермаркету з використанням React з Ecmascript – 2018. В межах України в недостатній мірі представлені вітчизняні розробки в цій області. У роботі наведені теоретичне узагальнення й рішення наукового завдання дослідження методів побудови та реалізація системи інтернет-гіпермаркету з використанням React з Ecmascript – 2018. Рішення даного завдання полягало у вирішенні наступних задач:Був проведений огляд існуючих систем побудови та реалізація системи інтернет-гіпермаркету з використанням React з Ecmascript – 2018; Досліджена система побудови та реалізація системи інтернет-гіпермаркету з використанням React з Ecmascript – 2018; На основі отриманих результатів досліджень створена програмна реалізація системи інтернет-гіпермаркету з використанням React з Ecmascript - 2018. Розроблені під час виконання роботи алгоритми дозволяють успішно вирішувати завдання побудови та реалізації системи інтернет-гіпермаркету з використанням React з Ecmascript – 2018.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. 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.

УДК 004

Б. Підхлібний, магістр гр. КІ-19М-1,4
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ БЕЗПЕЧНОГО ЗБЕРІГАННЯ ДАНИХ У ХМАРІ ЗА РАХУНОК CLOUD CONTROLS MATRIX

У статті розроблено програмне забезпечення, яке призначено для системи системи безпечного зберігання даних у хмарі за рахунок Cloud Controls Matrix. Метою розробки є дослідження та програмна реалізація системи безпечного зберігання даних у хмарі за рахунок Cloud Controls Matrix. Об’єктом дослідження є процес безпечного зберігання даних у хмарі за рахунок Cloud Controls Matrix. Предметом дослідження є методи безпечного зберігання даних у хмарі за рахунок Cloud Controls Matrix. Методи дослідження базуються на методах захисту інформації, методах математичної статистики, методах розробки програмного забезпечення. 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, Cloud Controls Matrix

Постановка проблеми. Проблема безпеки залишається каменем спотикання при переході в хмару. Причини занепокоєння із приводу захищеності й схоронності інформації очевидні, оскільки дані розміщаються на площадці, що перебуває під контролем сторонньої компанії. У цьому зв'язку ключовим стає питання довіри до провайдеру хмарних послуг, але частина відповідальності замовник повинен взяти на себе.

Небезпеки, що підстерігають власників традиційних і хмарних середовищ, багато в чому однакові. Якщо взяти, наприклад, «брудну дюжину» – список головних погроз для хмарних обчислень, що щорічно публікує Cloud Security Alliance, то здебільшого вони актуальні й для корпоративних ЦОДів. І все-таки з переходом у хмару з'являються додаткові ризики й нові види погроз.

У цьому зв'язку дуже важливо зрозуміти, як саме розділяються завдання по забезпеченню безпеки між користувачем і провайдером. Розподіл обов'язків залежить від виду використовуваних послуг. Якщо це інфраструктура як сервіс, то основна відповідальність покладає на користувача, зокрема, він сам відповідає за відновлення програмного забезпечення. А у випадку послуг SaaS своєчасне відновлення ПЗ здійснює провайдер.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи безпечного зберігання даних у хмарі за рахунок Cloud Controls Matrix.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи безпечного зберігання даних у хмарі за рахунок Cloud Controls Matrix.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем безпечного зберігання даних у хмарі за рахунок Cloud Controls Matrix.

– Дослідження системи безпечного зберігання даних у хмарі за рахунок Cloud Controls Matrix.

– Програмна реалізація системи безпечного зберігання даних у хмарі за рахунок Cloud Controls Matrix.

Об'єктом дослідження є процес безпечного зберігання даних у хмарі за рахунок Cloud Controls Matrix.

Предметом дослідження є методи безпечного зберігання даних у хмарі за рахунок Cloud Controls Matrix.

Методи дослідження базуються на методах захисту інформації, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. У хмарі дані найчастіше зберігаються надійніше, ніж у корпоративному ЦОДі. Персонал хмарного провайдеру має більше досвіду в рішенні таких завдань, як резервне копіювання або відновлення програмного забезпечення. Необхідно використовувати компетентність сервісу-провайдеру. Ви як замовник реалізуєте всього один проект, а ми паралельно ведемо 10 проектів з різною специфікою, у реалізації яких беруть участь безліч фахівців різного рівня. В остаточному підсумку ключове завдання технічного персоналу КЦОДа – захист даних клієнтів.

Однак безпека даних у хмарі починається із захисту ресурсів корпоративного ЦОДу. При компрометації мережі компанії хакери можуть використовувати отриману інформацію, наприклад дані про облікові записи, для атаки на її ресурси, розміщені в хмарі. Спочатку кожний повинен розібратися з тим, як у нього обстоять справи із внутрішньою безпекою, а вже потім турбуватися, як вона реалізована десь ще.

Безпека й схоронність даних клієнта в хмарі залежать у першу чергу від нього самого. Досить показовий інцидент, що відбувся з великою виробничою компанією. У результаті вірусної атаки на її бази даних всі файли виявилися зашифровані. За резервування відповідав сам клієнт, але, як виявилося, наявні копії були неактуальними. На запуск активних ВМ треба було три дні, на відновлення працездатності Exchange і «1С» – біля двох тижнів. А відновлення всіх систем, включаючи віртуальні робітники місця, зайняло майже місяць. Це зробило сильний негативний вплив на бізнес, оскільки затримувалася виписка рахунків, накладних і інших важливих документів – бізнес фактично виявився паралізованим.

Щоб не допустити повторення подібної ситуації, фахівці запропонували три можливих рішення. Перше – установка системи зберігання EMC Data Domain (витрати 200 тис. євро), друге – організація другої площадки для аварійного відновлення (120 тис. євро), третє – створення консистентних миттєвих знімків (10 тис. євро). Вибір замовника легко вгадати, тим більше що вся інфраструктура була перенесена в ЦОД провайдеру.

Усе, що треба було, – це придбати додатковий обсяг дискового місця й необхідне програмне забезпечення (якщо миттєві знімки робити засобами сховища, то вони не будуть консистентними, тому що ці зміни не відбиваються в системах Microsoft). Перевага такого рішення – відсутність необхідності зупиняти ВМ і застосунку для створення знімків, тому що вони робляться під час роботи (процесів). Відновлення будь-якого сервера займає до 10 з, а знімки можна робити із частотою до чотирьох у годину.

По-перше, треба змінити свій підхід до резервування, а по-друге, більше довіряти провайдеру й обговорювати з ним виникаючі проблеми. В описаному випадку клієнт повідомив про, що відбувається після атаки тільки на третій день. Якби він не забарився, системи можна було б відновити оперативно з наявних знімків платформи, які робив провайдер.

Як би надійної не був захист ЦОДу, цього недостатньо. При загальній присутності в Інтернеті, основним об'єктом атаки стають Web-застосунки й сервіси. Відповідно до дослідження уразливості дані компанії Verizon (Data Breach Investigation Report, DBIR), слабкою ланкою є саме Web-застосунки: кількість успішних атак на них, які привели до компрометації даних, з 2014 року виросло в чотири рази.

Коли ми будуємо моделі безпеки, те маємо на увазі те, до чого звикли, – безпека інфраструктури. Однак опора на потужну захищену інфраструктуру ЦОДу не привід розслаблюватися й ігнорувати захист на рівні застосунків. Відповідні погрози він розділяє на кілька рівнів: процеси, архітектура, реалізація, налаштування, комунікації, інтерфейси й профілі.

Сервіс може бути неправильно спроектований, тобто в самій процедурі є якась вада. Так, часта проблема інтернет-магазинів – можливість одержати товар, не оплативши його. Зокрема, на одному із сайтів можна було по прямому посиланню відразу перейти на сторінку доставки оплаченого товару. Саме посилання легко генерувалося за прикладом аналогічних сторінок (URL мали типовий формат), при цьому контрольна крапка для перевірки факту оплати товару була відсутня. У результаті зловмисникам удалося викрасти багато дорогої техніки.

Коли процес споконвічно побудований з помилкою, захистити його неможливо. Якщо ж наздогін він має неадекватну архітектуру, не розраховану на високе навантаження й не забезпечує необхідне розпаралелюванні процесів, ніякі ресурси й можливості ЦОДу не допоможуть: сервіс у будь-який момент може виявитися під погрозою. Такі ситуації не можна запобігти зовнішніми засобами, їх можна усунути тільки зсередини. Якщо на кожному етапі процесу не передбачаються необхідні елементи безпеки, навряд чи їх можна захистити «навісними» рішеннями.

Навіть при наявності добре спроектованої архітектури програмісти можуть припуститися помилки. Їхня мотивація – швидко випустити сервіс за мінімальною ціною, особливо якщо замовлення отримане за підсумками електронних закупівель: хто менше запропонував, той його й одержав. До того ж з поширенням принципів адаптивної розробки (agile) частота змін збільшується. Найчастіше застосунки міняються щодня, і тепер ніхто не буде писати низькорівневу документацію на код, як це було прийнято в старожитні часи, коли застосунку мінялися раз у квартал. У результаті часом неможливо зрозуміти, чи помилка це або задум розроблювача.

Трапляються й проблеми в налаштуваннях: по недогляду доступ може бути наданий не тому й не туди. У цій ситуації оператор ЦОДу теж допомогти не зможе, оскільки не знає, що була допущена помилка. Відповідно, необхідно управляти й налаштуваннями. Щораз треба не просто дивитися, що це за налаштування, а з'ясовувати, які погрози вона в собі несе. Якщо в людини є доступ, треба проконтролювати, які дії йому дозволені. Застосунки обробляють дані, що надходять із різних джерел, тому комунікаційні канали й інтерфейси обміну повинні контролюватися так само ретельно.

Однак, навіть якщо всі технічні моменти враховані й необхідної міри захисту передбачені, є ще одна небезпека – людський фактор. Адміністратор, що має легальний доступ, може їм зловжити: наприклад, його можуть шантажувати або в нього може виникнути образа на роботодавця. Таким чином, необхідне профілювання дій користувача. Прикладом погано спланованого профілю може служити відсутність обмежень на кількість паролів, що вводяться, що уможливлює підбор потрібного за допомогою перебору (brute force).

Таким чином, крім захисту інфраструктури, необхідно подбати й про захист самого сервісу. Якщо основний обсяг завдань першої групи може взяти на себе провайдер послуг ЦОДу, то про рішення інших завдань клієнтові прийде подбати по більшій частині самому. Провайдер забезпечить захист від атак DDo, здійснить резервне копіювання даних, допоможе виявити уразливості в системі, але він нічого не знає про архітектуру застосунків, користувальницьких сценаріях, внутрішніх процесах і інших особливостях інфраструктури клієнта.

До того ж, час «навісної» безпеки йде – застосунки й сервіси необхідно захищати не зовні, а зсередини: «Захист повинна бути убудованим – кожний процес повинен перевірятися на безпеку. Це не начіпний процес, а окремий шар у кожному процесі. Безпека давно перетворилася в якийсь імунітет усередині процесу».

Перехід у хмару може дати компанії цілий ряд переваг. Деякі можливості простіше забезпечити на базі хмарного ЦОДу – наприклад, необмежену масштабованість, тобто можливість одержувати будь-які ресурси як у випадку динамічного хмарного ЦОДу. Крім того, хмарні провайдери пропонують і унікальні сервіси. Сервіси Lambda, Kinesis, DynamoDB, Redshift, ви не одержите більше ніде, тільки в конкретного хмарного

провайдеру. Реалізувати ж їх самостійно вам навряд чи вдасться. Однак перехід у хмару часом обривається, так і не почавшись, якщо завдання по захисту даних не вирішені.

Виділено шість стадій впровадження хмарного підходу:

- експериментування;
- забезпечення безпеки;
- використання IaaS, PaaS, SaaS;
- підключення додаткових сервісів;
- додавання унікальних сервісів;
- повне прийняття хмари, коли вся діяльність компанії побудована з урахуванням його використання.

Поекспериментував із хмарою, багато організацій цим і обмежуються. Дуже багато хто на цьому етапі в Україні просто зупиняються, тому що мало хто розуміє, як управляти хмарними сервісами і як захищати їх. Якщо етап забезпечення безпеки не пройдений, ніяких подальших впроваджень і прогресу очікувати не доводиться.

Що ж міняється? Інструменти й технології безпеки майже не відрізняються. Одна з головних особливостей – зміна ролі замовника. Якщо раніше ви захищали всі самі, то тепер частина повноважень треба віддати третій стороні й перевіряти, чи виконуються всі домовленості. Мало хто із провайдерів готовий надати повні дані про те, що він робить із погляду безпеки і як варто взаємодіяти з ним при розслідуванні якоїсь події. До того ж, указує Володимир Маліновський, ви однаково не зможете довідатися всі нюанси захисту хмарної інфраструктури провайдеру. Це вже не стільки питання керування безпекою, скільки питання вибору постачальника, але з погляду безпеки.

Разом з тим безпека не самоцінність. Акцент усе більше зміщається убік економічних показників, тобто ефективність системи безпеки характеризується не числом інцидентів, а кількістю зекономлених засобів у результаті скорочення простоїв, зниження збитку й т.п. Відповідно, особливе значення має співвідношення можливостей і ризиків. Безпека важлива як зворотна сторона можливостей. При переході в хмару краще пробувати те, чого у вас ні, тоді більше уваги будете приділяти можливостям, а не ризикам.

Звичайно, це не означає, що погрози варто ігнорувати (хоча потенційна вигода іноді переважує будь-які ризики). Заходи для їхнього зниження є невід'ємною частиною процесу переходу в хмару. Ухвалюючи рішення щодо переході в хмару, необхідно враховувати чутливість/критичність даних і пропонованого провайдером рівня захисту, але в остаточному підсумку вибір буде залежати від того, чи виявиться користь для бізнесу більше вагомої, чим можливі ризики.

Розробка структурної схеми

Хоча за останні кілька років «хмарні» сервіси придбали величезну популярність у підприємств за свої численні вигоди, вони не позбавлені ризиків у таких областях як безпека, конфіденційність даних і доступність даних. Стало очевидно, що необхідно єдина думка про методи оцінки ризиків хмарних обчислень, але цього важко домогтися, оскільки в галузі відсутній єдина, стандартна, структурована платформа, що могла б допомогти підприємствам в оцінці й зниженні ризиків «хмарних» обчислень.

Сьогодні цілий ряд організацій намагається вирішити цю проблему, і, можливо, найбільше успішно це робить організація CSA (Cloud Security Alliance), що вважає своєю місією просувати використання передових технологій забезпечення безпеки в хмарі, пропонуючи безліч проектів оцінки й сертифікації «хмари» відносно контрольних директив, які CSA уважає важливими для забезпечення безпеки й відповідності «хмари».

Європейське агентство по мережевій і інформаційній безпеці (ENISA) розробило модель забезпечення доступності, цілісності й безпеці інформації (IAF), засновану на широких класах директив зі стандарту ISO/IEC 271101/2 і стандарти BS 2599. За останні кілька років ці й інші групи створили велика кількість документів, що містять інформацію з виявлення ризиків, спеціальних керівництв і контрольних запитальників, з якими необхідно

консультуватися при оцінці ризиків хмарних обчислень. Проте, більшість цих документів по оцінці хмарних ризиків дають докладний опис проблем безпеки і ймовірних ризиків, але не пропонують детальній, всебічній моделі оцінки, що можуть використовувати організації.

Довгий і нудний перелік серйозних відключень і порушень системи безпеки тільки ще більше заплутує організації, коли вони намагаються корелювати свої поточні внутрішні системи керування й пропоновані хмарні системи керування з випадками, що згадуються в пресі. У цій статті розглядаються методи вибору, розробки й початку реалізації заснованої на стандартах платформи для оцінки ризиків хмарних обчислень.

Метод оцінки «хмарних» ризиків безпеки

Як відправна крапка для проведення оцінки 'хмарної' середовища на основі ризиків варто використовувати доступні підприємствам загальні моделі керування ризиками типу інтегрованої моделі керування ризиками організацій Комітету спонсорських організацій Комісії Тредвея (COSO). Є також специфічні для конкретної області платформи, методи й моделі, наприклад, стандарт ISO 27001. Заснована на керуванні IT-ризиками платформа COBIT від ISACA може заповнити пробіл між платформами керування ризиками загального користування й специфічних платформ, заснованими на допущеннях, що IT-ризик не є сугубо технічною проблемою.

Однак для рішення специфічних для даної організації проблем безпеки 'хмарних' обчислень необхідно розробити цільну платформу керування хмарними ризиками безпеки за допомогою використання однієї або більше галузевих рекомендацій. Наприклад, в організації CSA є опитувальник оцінки стану безпеки хмарного середовища, а також «хмарна» матриця керування (CCM). Аналогічно цьому, ENISA пропонує важлива підстава для забезпечення ефективної інтеграції зі сторонніми сертифікаціями й атестаціями, наприклад, ISO 27001/27002, PCI DSS, SOX і SAS 70.

Розуміння безпеки в контексті даного бізнесу

У той час як безліч провайдерів «хмарних» сервісів пропонують можливості забезпечення безпеки корпоративного класу або вище, ризики теж ростуть. Кіберзлочинці все частіше роблять своєю мішенню зростаючу концентрацію, недостатню захищеність і цінність хмарних ресурсів, і нормативи відповідності постійно посилюються. З обліком цього, нижче описані чотири основних етапи використання тої або іншої платформи для визначення й оцінки 'хмарних' ризиків на основі поточного положення речей.

Моделювання профілю ризиків – Моделі ризиків визначають основні терміни, використовувані в оцінці хмарних ризиків, включаючи фактори оцінюваних ризиків і взаємозв'язок цих факторів. Організаціям необхідно виразити ці визначення в писемній формі, перш ніж проводити оцінки ризиків, оскільки ці оцінки повинні бути засновані на добре певних атрибутах погроз, уразливостях і інших факторах ризиків для ефективного визначення ризику. Під час планування й проведення оцінки впливу на бізнес, необхідно змоделювати кожний додаток або бізнес-процес у даному хмарному середовищі. І тут необхідно задати два

Вибір критеріїв оцінки – Критерії для хмарних сервісів повинні вибиратися на основі профілю ризиків організації з метою ідентифікації критичних ресурсів і наступного аналізу потенційних уразливостей і погроз цим ресурсам. Для оцінки ризиків безпеки можна використовувати структурований підхід, використовуючи для цього вибрані галузеві стандарти або рекомендації – ISO 2700x, COBIT, NIST 800-53, і PCI DSS Cloud Computing Guidelines, які застосовні до уразливих місць конкретного хмарного середовища. Організаціям, які зобов'язані мати більше однієї нормативної вимоги відповідності, має сенс пристосовувати вказівки кожного нормативного стандарту або рекомендації до організації у відповідних випадках, а потім розробляти специфічну комбіновану платформу для оцінки бажаних наборів контрольних функцій з метою виконання вимог відповідності, яким підлягає дана організація.

Виконання періодичних оцінок і безперервного моніторингу – Важливо, щоб організації на постійній основі виконували контроль факторів ризиків, ідентифіковані під час

оцінок ризиків, і розуміли наступні зміни цих факторів. Вони також повинні обновляти основні компоненти оцінок ризиків, у результаті періодичних перевірок. Організації можуть зменшувати зусилля й витрати на оцінки й моніторинг шляхом залучення сторонніх організацій, у випадку якщо це є можливим.

Перегляд і відновлення платформи – Організаціям необхідно переглядати й обновляти свої критерії оцінки у випадку появи нових випадків використання, що компенсують засобів або ризиків. Буде необхідно періодично виконувати повторне моделювання й оцінку ризиків, для того щоб знати, не потрібні чи інші схеми використання хмари. Дуже важливо обновляти критерії оцінки з появою нових або оновлених стандартів безпеки хмарних обчислень, керівництв, платформ оцінки відповідності або вимог.

Хмарні обчислення залишаються областю, що розвивається, сильні й слабкі сторони якої ще не повністю вивчені, підтверджені документально або випробувані. Організації повинні починати процес роботи із платформою оцінки ризиків, використовуючи описаних вище рекомендацій. Крім того, ідентифіковані засоби керування повинні регулярно оцінюватися, тестуватися й підтверджуватися в 'хмарному' середовищі, тим самим полегшуючи виконання будь-яких застосовних вимог відповідності.

Програмне забезпечення системи безпечного зберігання даних у хмарі за рахунок Cloud Controls Matrix, що розроблено в даній роботі, забезпечує інтелектуальний захист IT-мереж і корпоративних ресурсів від постійно зростаючих і усе більше витончених погроз і дозволяє відповідати необхідним вимогам і стандартам.

Програмне забезпечення системи безпечного зберігання даних у хмарі за рахунок Cloud Controls Matrix, що розроблено в даній роботі, забезпечує повну видимість усередині мережі, відслідковуючи активність всіх користувачів і застосунків. Це дозволяє виявляти всі існуючі й потенційні погрози для мережевої інфраструктури.

Рішення побудоване на гнучкій платформі, що здатна розвиватися разом з організацією, підбудовуючись під її зростаючу інфраструктуру, і застосовувати досвід взаємодії з конкретним користувачем до цілих груп користувачів у всій організації. Керування балками, передове виявлення погроз і керування політиками по відповідності вимогам і стандартам роблять програмне забезпечення системи безпечного зберігання даних у хмарі за рахунок Cloud Controls Matrix, що розроблено в даній роботі, добре інтегрованим рішенням, що швидко й легко забезпечує моніторинг корпоративної безпеки.

Програмне забезпечення системи безпечного зберігання даних у хмарі за рахунок Cloud Controls Matrix, що розроблено в даній роботі збирає наступну інформацію:

- події системи безпеки – події від брандмауерів, VPNs, IDS/IPS, і т.д.,
- монітор активності мережі – контекстні ідентифікатори протоколів 7-го рівня від мережевого трафіку й застосунків,
- монітор активності користувачів – дані продуктів типу IAM (Identity and Access Management) і сканерів уразливостей,
- події в мережі – події від світчів, роутерів, серверів, хостів і т.д.,
- журнали подій застосунків – ERP, документообіг, бази даних застосунків, адміністративні платформи й т.д.

Програмне забезпечення системи безпечного зберігання даних у хмарі за рахунок Cloud Controls Matrix, що розроблено в даній роботі **–** це рішення, що стане основою безпеки вашої організації: централізований користувальницький інтерфейс, що забезпечує функціональний рольовий доступ і глобальний огляд керування інцидентами й звітністю. Панелі керування доступні як функціонал, а користувачі можуть самі створювати й налаштовувати власні робочі простори. Подібна можливість деталізації дозволяє набагато простіше виявляти й вибирати сплески подій або мережеві потоки, пов'язані з порушеннями. Доступно близько 3 500 шаблонів звітів, що мають відношення до конкретних пристроїв, ролям і відповідностям.

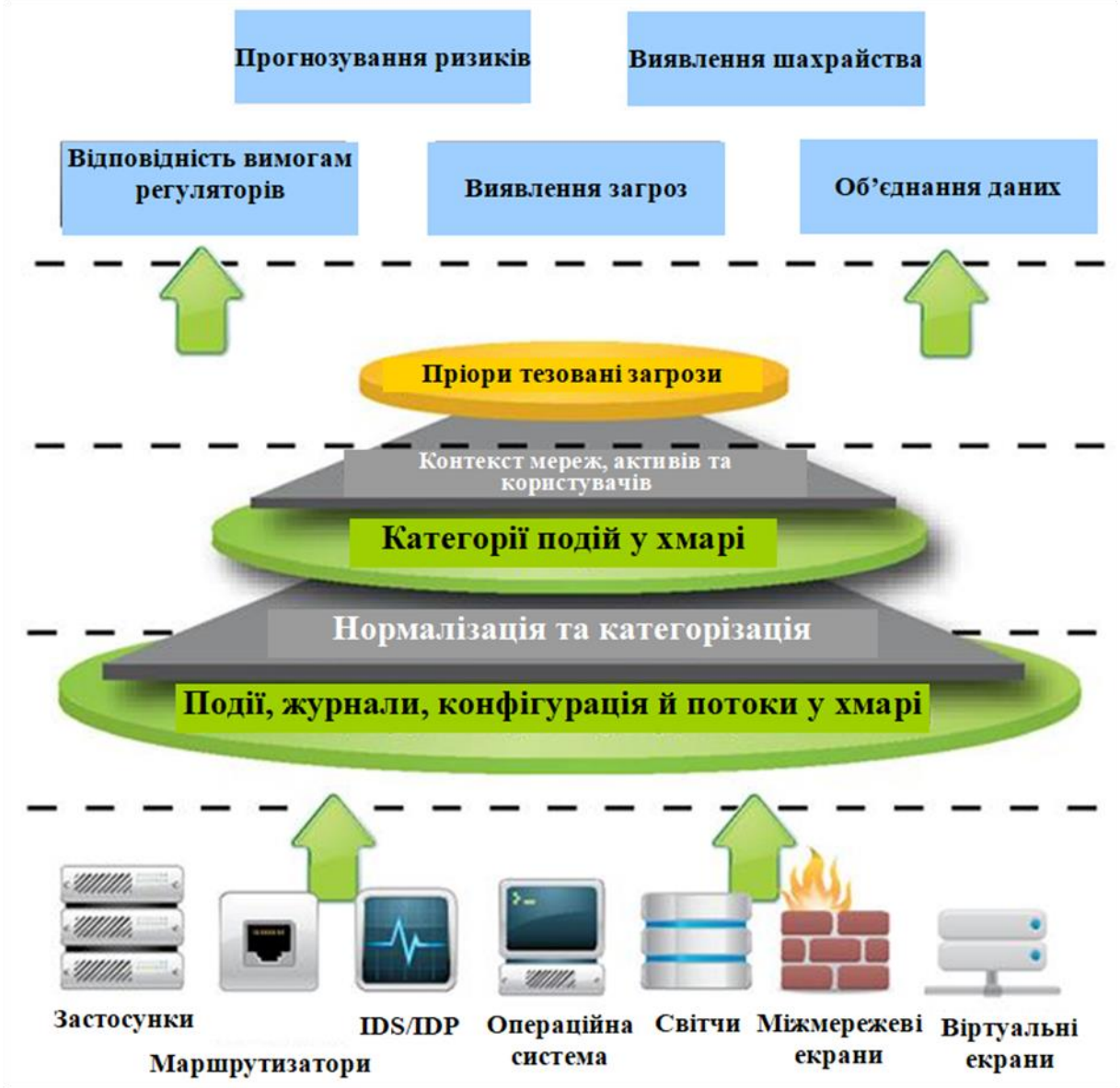


Рисунок 1 – Структурна схема системи

Конкурентною перевагою є можливість автоматизації процесу виявлення джерел подій і профілювання застосунків, що дозволяє максимально адаптувати рішення до вимог замовника. Крім того, програмне забезпечення системи безпечного зберігання даних у хмарі за рахунок Cloud Controls Matrix, що розроблено в даній роботі, підтримує функцію щотижневого автоматичного відновлення контенту, включаючи сторонній. Для початку роботи рішення потрібна мінімальне налаштування.

Надається можливість авто-розгортання, авто-звітності і автоматичного визначення пріоритетів. Дозволяє організаціям істотно поліпшити моніторинг, аналіз і реагування на інциденти інформаційної безпеки.

Програмне забезпечення системи безпечного зберігання даних у хмарі за рахунок Cloud Controls Matrix, що розроблено в даній роботі допомагає службам безпеки:

- виявляти погрози;
- відповідати нормативним вимогам;
- прогнозувати ризики;
- виявляти інсайдерів;
- поєднувати розрізнені дані.

Програмне забезпечення системи безпечного зберігання даних у хмарі за рахунок Cloud Controls Matrix, що розроблено в даній роботі, забезпечує збір, аналіз і кореляцію даних через широкий спектр систем, включаючи мережеві рішення, рішення безпеки, сервери, хости, операційні системи й застосунки. Підтримує більше 200 продуктів практично всіх ведучих вендорів. Крім того, програмне забезпечення системи безпечного зберігання даних у хмарі за рахунок Cloud Controls Matrix, що розроблено в даній роботі, легко налаштовується для підтримки будь-яких пропрієтарних застосунків і нових систем. На сьогоднішній день підтримує пристрою більшості виробників: F5, Cisco, Juniper, Nortel, Checkpoint, Oracle, Sun, Enterasys, Symantec, ISS/IBM, McAfee, Sourcefire, RSA і т.д.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів безпечного зберігання даних у хмарі за рахунок Cloud Controls Matrix. В межах України в недостатній мірі представлені вітчизняні розробки в цій області. У роботі наведені теоретичне узагальнення й рішення наукового завдання дослідження методів безпечного зберігання даних у хмарі за рахунок Cloud Controls Matrix. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем безпечного зберігання даних у хмарі за рахунок Cloud Controls Matrix; Досліджена система безпечного зберігання даних у хмарі за рахунок Cloud Controls Matrix; На основі отриманих результатів досліджень створена програмна реалізація системи безпечного зберігання даних у хмарі за рахунок Cloud Controls Matrix. Розроблені під час виконання роботи алгоритми дозволяють успішно вирішувати завдання безпечного зберігання даних у хмарі за рахунок Cloud Controls Matrix. 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. 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. Прокопенко, магістр гр. КІ-19МЗ
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ МЕРЕЖЕВИХ ПРИКІНЦЕВИХ ПРИСТРОЇВ АВТОМОБІЛЯ

У статті розроблено програмне забезпечення, яке призначено для системи мережевих прикінцевих пристроїв автомобіля. Метою розробки є дослідження та програмна реалізація системи мережевих прикінцевих пристроїв автомобіля. Об’єктом дослідження є процес мережевих прикінцевих пристроїв автомобіля. Предметом дослідження є методи мережевих прикінцевих пристроїв автомобіля. Методи дослідження базуються на методах комп’ютерної електроніки, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи мережевих прикінцевих пристроїв автомобіля.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, мережа, прикінцеві пристрої

Постановка проблеми. Будь-який сучасний автомобіль, оснащений інжекторним двигуном внутрішнього згорання, має «бортовий комп'ютер» для управління й контролю параметрів роботи двигуна. Більш правильно замість «бортовий комп'ютер» застосувати іншу назву – контролер управління двигуном, тому що даний пристрій звичайно виконаний на 8-мі бітному мікроконтролері, або найбільше що часто зустрічається в технічній літературі термін – електронний блок управління двигуном (ЕБУ). Основне завдання ЕБУ – на основі показань датчиків (найбільш важливі – датчик положення колінчатого вала, датчик положення дросельної заслінки, датчик масової витрати повітря, кисневий датчик (лямбда зонд)) формування стехіометричної паливної суміші й своєчасний підпал останньої. Стехіометрична паливна суміш (при якій паливо згоряє повністю) – співвідношення кількості палива до кількості повітря від 12 до 16 залежно від навантаження двигуна. Програма управління двигуном міститься в ПЗУ, звичайно, однократно записуване або з ультрафіолетовим стиранням. Крім того, можливо в ЕБУ наявність Flash пам'яті, що разом з високошвидкісним мікроконтролером С509 і внутрисхемною програмою завантажником дозволяє оперативно змінити прошивання й програму управління двигуном. Властиво програма управління побудована на принципі табличної конвертації. Набагато простіше й швидше виконати кілька програмних переходів, ніж робити якісь обчислення. Тому для зміни режимів роботи двигуна не потрібно міняти програму цілком, досить змінити частину пошивки – дані калібрувань.

Робота з бортовим комп’ютером забезпечується за рахунок використання інтерфейсу обміну даними за стандартом ISO 14230 (ISO9141, OBD-II, KWP2000).

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи мережевих прикінцевих пристроїв автомобіля.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи мережевих прикінцевих пристроїв автомобіля.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем мережевих прикінцевих пристроїв автомобіля.
– Дослідження системи мережевих прикінцевих пристроїв автомобіля.
– Програмна реалізація системи мережевих прикінцевих пристроїв автомобіля.

Об'єктом дослідження є процес мережевих прикінцевих пристроїв автомобіля.

Предметом дослідження є методи мережевих прикінцевих пристроїв автомобіля.

Методи дослідження базуються на методах комп'ютерної електроніки, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Система функціонує наступним чином. Спершу ЕОМ через кабель з стандартом OBDII (ISO 14230) підключається до бортового комп'ютера автомобіля. Після цього завантажуються стандартні тестові послідовності, які або повертають дані, що системи автомобіля є справними, або повертають коди помилок у роботі того, або іншого блоку автомобіля. Цих кодів помилок дуже багато, порядку 2000, тому у даній магістерській роботі, приведемо перелік тільки основних помилок. До них відносяться наступні нижче перераховані коди несправностей стандарту OBDII.

P0 – 1XX – Вимірники палива й повітря.
PO – 100 – Несправність ланцюга датчика витрати повітря.
PO – 101 – Вихід сигналу із припустимого діапазону.
PO – 102 – Низький рівень вихідного сигналу.
PO – 103 – Високий рівень вихідного сигналу.
PO – 105 – Несправність датчика тиску повітря.
PO – 106 – Вихід сигналу із припустимого діапазону.
PO – 107 – Низький рівень вихідного сигналу.
PO – 108 – Високий рівень вихідного сигналу.
PO – 110 – Несправність датчика температури усмоктуваного повітря.
PO – 111 – Вихід сигналу із припустимого діапазону.
PO – 112 – Низький рівень вихідного сигналу.
PO – 113 – Високий рівень вихідного сигналу.
PO – 115 – Несправність датчика температури охолодної рідини.
PO – 116 – Вихід сигналу із припустимого діапазону.
PO – 117 – Низький рівень вихідного сигналу.
PO – 118 – Високий рівень вихідного сигналу.
PO – 120 – Несправність датчика положення дросельної заслінки.
PO – 121 – Вихід сигналу із припустимого діапазону.
PO – 122 – Низький рівень вихідного сигналу.
PO – 123 – Високий рівень вихідного сигналу.
PO – 125 – Низька температури охолодної рідини для управління по замкнутому контуру. .
PO – 130 – Датчик O2 B1 S1 несправний (Банк1).
PO – 131 – Датчик O2 B1 S1 має низький рівень сигналу.
PO – 132 – Датчик O2 B1 S1 має високий рівень сигналу.
PO – 133 – Датчик O2 B1 S1 має повільний відгук на збагачення/збіднiння.
PO – 134 – Ланцюг датчика O2 B1 S1 пасивна.
PO – 135 – Нагрівач датчика O2 B1 S1 несправний.
PO – 136 – Датчик O2 B1 S2 несправний.
PO – 137 – Датчик O2 B1 S2 має низький рівень сигналу.
PO – 138 – Датчик O2 B1 S2 має високий рівень сигналу.
PO – 139 – Датчик O2 B1 S2 має повільний відгук на збагачення/збіднiння.
PO – 140 – Ланцюг датчика O2 B1 S2 пасивна.
PO – 141 – Нагрівач датчика O2 B1 S2 несправний.
PO – 142 – Датчик O2 B1 S3 несправний.

P0 – 143 – Датчик O2 B1 S3 має низький рівень сигналу.
P0 – 144 – Датчик O2 B1 S3 має високий рівень сигналу.
P0 – 145 – Датчик O2 B1 S3 має повільний відгук на збагачення/збідніння.
P0 – 146 – Ланцюг датчика O2 B1 S3 пасивна.
P0 – 147 – Нагрівач датчика O2 B1 S3 несправний.
P0 – 150 – Датчик O2 У2 S1 несправний (Банк2).
P0 – 151 – Датчик O2 У2 S1 має низький рівень сигналу.
P0 – 152 – Датчик O2 У2 S1 має високий рівень сигналу.
P0 – 153 – Датчик O2 У2 S1 має повільний відгук на збагачення/збідніння.
P0 – 154 – Ланцюг датчика O2 У2 S1 пасивна.
P0 – 155 – Нагрівач датчика O2 У2 S1 несправний.
P0 – 156 – Датчик O2 У2 S2 несправний.
P0 – 157 – Датчик O2 У2 S2 має низький рівень сигналу.
P0 – 158 – Датчик O2 У2 S2 має високий рівень сигналу.
P0 – 159 – Датчик O2 У2 S2 має повільний відгук на збагачення/збідніння.
P0 – 160 – Ланцюг датчика O2 У2 S2 пасивна.
P0 – 161 – Нагрівач датчика O2 У2 S2 несправний.
P0 – 162 – Датчик O2 У2 S3 несправний.
P0 – 163 – Датчик O2 У2 S3 має низький рівень сигналу.
P0 – 164 – Датчик O2 У2 S3 має високий рівень сигналу.
P0 – 165 – Датчик O2 У2 S3 має повільний відгук на збагачення/збідніння.
P0 – 166 – Ланцюг датчика O2 У2 S3 пасивна.
P0 – 167 – Нагрівач датчика O2 У2 S3 несправний.
P0 – 170 – Витік палива з паливної системи блоку №1.
P0 – 171 – Блок циліндрів №1 збіднює (можливо підсмоктування повітря).
P0 – 172 – Блок циліндрів №1 збогачує (можливо неповне закриття форсунки).
P0 – 173 – Витік палива з паливної системи блоку №2.
P0 – 174 – Блок циліндрів №2 збіднює (можливо підсмоктування повітря).
P0 – 175 – Блок циліндрів №2 збогачує (можливо неповне закриття форсунки).
P0 – 176 – Датчик викиду CHx несправний.
P0 – 177 – Сигнал датчика виходить із припустимого діапазону.
P0 – 178 – Низький рівень сигналу датчика CHx.
P0 – 179 – Високий рівень сигналу датчика CHx.
P0 – 180 – Ланцюг датчика температури палива «A» несправний.
P0 – 181 – Сигнал датчика «A» виходить із припустимого діапазону.
P0 – 182 – Низький сигнал датчика температури палива «A».
P0 – 183 – Високий сигнал датчика температури палива «A».
P0 – 185 – Ланцюг датчика температури палива «B» несправний.
P0 – 186 – Сигнал датчика «B» виходить із припустимого діапазону.
P0 – 187 – Низький сигнал датчика температури палива «B».
P0 – 188 – Високий сигнал датчика температури палива «B».
P0 – 190 – Ланцюг датчика тиску палива в паливній рампі несправний.
P0 – 191 – Сигнал датчика виходить із припустимого діапазону.
P0 – 192 – Низький сигнал датчика тиску палива .
P0 – 193 – Високий сигнал датчика тиску палива .
P0 – 194 – Сигнал датчика тиску палива перемежований.
P0 – 195 – Ланцюг датчика температури масла у двигуні несправний.
P0 – 196 – Сигнал датчика виходить із припустимого діапазону.
P0 – 197 – Низький сигнал датчика температури масла.
P0 – 198 – Високий сигнал датчика температури масла.
P0 – 199 – Сигнал датчика температури масла перемежований.
P0 – 2XX – .

РО – 200 – Ланцюг управління форсункою несправний.
РО – 201 – Ланцюг управління форсункою циліндра №1 несправний.
РО – 202 – Ланцюг управління форсункою циліндра №2 несправний.
РО – 203 – Ланцюг управління форсункою циліндра №3 несправний.
РО – 204 – Ланцюг управління форсункою циліндра №4 несправний.
РО – 205 – Ланцюг управління форсункою циліндра №5 несправний.
РО – 206 – Ланцюг управління форсункою циліндра №6 несправний.
РО – 207 – Ланцюг управління форсункою циліндра №7 несправний.
РО – 208 – Ланцюг управління форсункою циліндра №8 несправний.
РО – 209 – Ланцюг управління форсункою циліндра №9 несправний.
РО – 210 – Ланцюг управління форсункою циліндра №10 несправний.
РО – 211 – Ланцюг управління форсункою циліндра №11 несправний.
РО – 212 – Ланцюг управління форсункою циліндра №12 несправний.
РО – 213 – Ланцюг управління форсункою холодного старту №1 несправний.
РО – 214 – Ланцюг управління форсункою холодного старту №2 несправний.
РО – 215 – Соленоїд вимикання двигуна несправний.
РО – 216 – Ланцюг контролю часу упорскування несправний.
РО – 217 – Двигун перебуває в перегрітому стані.
РО – 218 – Трансмісія перебуває в перегрітому стані.
РО – 219 – Двигун перекручений.
РО – 220 – Несправність датчика положення дросельної заслінки «В».
РО – 221 – Вихід сигналу із припустимого діапазону.
РО – 222 – Низький рівень вихідного сигналу датчика «В».
РО – 223 – Високий рівень вихідного сигналу датчика «В».
РО – 224 – Сигнал датчика «В» перемежований.
РО – 225 – Несправність датчика положення дросельної заслінки «С».
РО – 226 – Вихід сигналу із припустимого діапазону.
РО – 227 – Низький рівень вихідного сигналу датчика «С».
РО – 228 – Високий рівень вихідного сигналу датчика «С».
РО – 229 – Сигнал датчика «С» перемежований.
РО – 230 – Первинний ланцюг бензонасоса (управління реле бензонасосу) несправний.
РО – 231 – Вторинний ланцюг бензонасоса має постійно низький рівень.
РО – 232 – Вторинний ланцюг бензонасоса має постійно високий рівень.
РО – 233 – Вторинний ланцюг бензонасоса має перемежований рівень.
РО – 235 – Ланцюг датчика тиску турбо-наддування «А» несправний.
РО – 236 – Сигнал з датчика турбіни «А» виходить із припустимого діапазону.
РО – 237 – Сигнал з датчика турбіни «А» має постійно низький рівень .
РО – 238 – Сигнал з датчика турбіни «А» має постійно високий рівень.
РО – 239 – Ланцюг датчика тиску турбо-наддування «Б» несправний.
РО – 240 – Сигнал з датчика турбіни «Б» виходить із припустимого діапазону.
РО – 241 – Сигнал з датчика турбіни «Б» має постійно низький рівень .
РО – 242 – Сигнал з датчика турбіни «Б» має постійно високий рівень.
РО – 243 – Соленоїд затвора вихлопних газів турбіни «А» несправний.
РО – 244 – Сигнал соленоїда турбіни «А» виходить із припустимого діапазону.
РО – 245 – Соленоїд вихлопних газів турбіни «А» завжди закритий.
РО – 246 – Соленоїд вихлопних газів турбіни «А» завжди відкритий.
РО – 247 – Соленоїд вихлопних газів турбіни «В» несправний.
РО – 248 – Сигнал соленоїда турбіни «В» виходить із припустимого діапазону.
РО – 249 – Соленоїд вихлопних газів турбіни «В» завжди закритий.
РО – 250 – Соленоїд вихлопних газів турбіни «В» завжди відкритий.
РО – 251 – Насос упорскування турбіни «А» несправний.

РО – 252 – Сигнал насоса упорскування турбіни «А» виходить із допустимого діапазону.
РО – 253 – Сигнал насоса упорскування турбіни «А» має низький рівень.
РО – 254 – Сигнал насоса упорскування турбіни «А» має високий рівень.
РО – 255 – Сигнал насоса упорскування турбіни «А» перемежований.
РО – 256 – Насос упорскування турбіни «В» несправний.
РО – 257 – Сигнал насоса упорскування турбіни «В» виходить із допустимого діапазону.
РО – 258 – Сигнал насоса упорскування турбіни «В» має низький рівень.
РО – 259 – Сигнал насоса упорскування турбіни «В» має високий рівень.
РО – 260 – Сигнал насоса упорскування турбіни «В» перемежований.
РО – 261 – Форсунка 1-ого циліндра замкнута на землю .
РО – 262 – Форсунка 1-ого циліндра обірвана або замкнута на +12В.
РО – 263 – Драйвер форсунки 1-ого циліндра несправний.
РО – 264 – Форсунка 2-ого циліндри замкнутий на землю .
РО – 265 – Форсунка 2-ого циліндри обірваний або замкнута на +12В.
РО – 266 – Драйвер форсунки 2-ого циліндри несправний.
РО – 267 – Форсунка 3-го циліндри замкнутий на землю .
РО – 268 – Форсунка 3-го циліндри обірваний або замкнута на +12В.
РО – 269 – Драйвер форсунки 3-го циліндри несправний.
РО – 270 – Форсунка 4-ого циліндри замкнутий на землю .
РО – 271 – Форсунка 4-ого циліндри обірваний або замкнута на +12В.
РО – 272 – Драйвер форсунки 4-ого циліндри несправний.
РО – 273 – Форсунка 5-ого циліндра замкнута на землю .
РО – 274 – Форсунка 5-ого циліндра обірвана або замкнута на +12В.
РО – 275 – Драйвер форсунки 5-ого циліндра несправний.
РО – 276 – Форсунка 6-ого циліндра замкнута на землю .
РО – 277 – Форсунка 6-ого циліндра обірвана або замкнута на +12В.
РО – 278 – Драйвер форсунки 6-ого циліндра несправний.
РО – 279 – Форсунка 7-ого циліндра замкнута на землю .
РО – 280 – Форсунка 7-ого циліндра обірвана або замкнута на +12В.
РО – 281 – Драйвер форсунки 7-ого циліндра несправний.
РО – 282 – Форсунка 8-ого циліндра замкнута на землю .
РО – 283 – Форсунка 8-ого циліндра обірвана або замкнута на +12В.
РО – 284 – Драйвер форсунки 8-ого циліндра несправний.
РО – 285 – Форсунка 9-ого циліндра замкнута на землю .
РО – 286 – Форсунка 9-ого циліндра обірвана або замкнута на +12В.
РО – 287 – Драйвер форсунки 9-ого циліндра несправний.
РО – 288 – Форсунка 10-ого циліндра замкнута на землю .
РО – 289 – Форсунка 10-ого циліндра обірвана або замкнута на +12В.
РО – 290 – Драйвер форсунки 10-ого циліндра несправний.
РО – 291 – Форсунка 11-ого циліндра замкнута на землю .
РО – 292 – Форсунка 11-ого циліндра обірвана або замкнута на +12В.
РО – 293 – Драйвер форсунки 11-ого циліндра несправний.
РО – 294 – Форсунка 12-ого циліндра замкнута на землю .
РО – 295 – Форсунка 12-ого циліндра обірвана або замкнута на +12В.
РО – 296 – Драйвер форсунки 12-ого циліндра несправний.
РО – 3ХХ – Система запалювання й пропуски.
РО – 300 – Виявлені випадкові/множинні пропуски запалювання.
РО – 301 – Виявлені пропуски запалювання в 1-ому циліндрі.
РО – 302 – Виявлені пропуски запалювання в 2-ому циліндрі.
РО – 303 – Виявлені пропуски запалювання в 3-ому циліндрі.

РО – 304 – Виявлені пропуски запалювання в 4-ому циліндрі.
РО – 305 – Виявлені пропуски запалювання в 5-ому циліндрі.
РО – 306 – Виявлені пропуски запалювання в 6-ому циліндрі.
РО – 307 – Виявлені пропуски запалювання в 7-ому циліндрі.
РО – 308 – Виявлені пропуски запалювання в 8-ому циліндрі.
РО – 309 – Виявлені пропуски запалювання в 9-ому циліндрі.
РО – 310 – Виявлені пропуски запалювання в 10-ому циліндрі.
РО – 311 – Виявлені пропуски запалювання в 11-ому циліндрі.
РО – 312 – Виявлені пропуски запалювання в 12-ому циліндрі.
РО – 320 – Ланцюг розподільника запалювання несправний.
РО – 321 – Сигнал ланцюга розподільника запалювання виходить за допустимі межі.
РО – 322 – Сигнал ланцюга розподільника запалювання відсутній.
РО – 323 – Сигнал ланцюга розподільника запалювання перемежований.
РО – 325 – Ланцюг датчика детонації №1 несправний.
РО – 326 – Сигнал датчика детонації №1 виходить за припустимі межі.
РО – 327 – Сигнал датчика детонації №1 має низький рівень .
РО – 328 – Сигнал датчика детонації №1 має високий рівень.
РО – 329 – Сигнал датчика детонації №1 перемежований.
РО – 330 – Ланцюг датчика детонації №2 несправний.
РО – 331 – Сигнал датчика детонації №2 виходить за припустимі межі.
РО – 332 – Сигнал датчика детонації №2 має низький рівень .
РО – 333 – Сигнал датчика детонації №2 має високий рівень.
РО – 334 – Сигнал датчика детонації №2 перемежований.
РО – 335 – Датчик положення колінчатого вала «А» несправний.
РО – 336 – Сигнал датчика «А» виходить за припустимі межі.
РО – 337 – Сигнал датчика «А» має низький рівень або замкнуть на масу .
РО – 338 – Сигнал датчика «А» має високий рівень або замкнуть на 12В.
РО – 339 – Сигнал датчика «А» перемежований.
РО – 340 – Датчик положення розподільного вала несправний.
РО – 341 – Сигнал датчика виходить за припустимі межі.
РО – 342 – Сигнал датчика має низький рівень або замкнуть на масу .
РО – 343 – Сигнал датчика має високий рівень.
РО – 344 – Сигнал датчика перемежований.
РО – 350 – Первиний/вториний ланцюг котушки запалювання несправні.
РО – 351 – Первиний/вториний ланцюг котушки запалювання «А» несправні.
РО – 352 – Первиний/вториний ланцюг котушки запалювання «В» несправні.
РО – 353 – Первиний/вториний ланцюг котушки запалювання «С» несправні.
РО – 354 – Первиний/вториний ланцюг котушки запалювання «D» несправні.
РО – 355 – Первиний/вториний ланцюг котушки запалювання «Е» несправні.
РО – 356 – Первиний/вториний ланцюг котушки запалювання «F» несправні.
РО – 357 – Первиний/вториний ланцюг котушки запалювання «G» несправні.
РО – 358 – Первиний/вториний ланцюг котушки запалювання «Н» несправні.
РО – 359 – Первиний/вториний ланцюг котушки запалювання «І» несправні.
РО – 360 – Первиний/вториний ланцюг котушки запалювання «J» несправні.
РО – 361 – Первиний/вториний ланцюг котушки запалювання «К» несправні.
РО – 362 – Первиний/вториний ланцюг котушки запалювання «L» несправні.
РО – 380 – Свіча накалювання або ланцюг нагрівання несправні.
РО – 381 – Свіча накалювання або індикатор нагрівання несправні.
РО – 385 – Ланцюг датчика положення колінчатого вала «В» несправні.
РО – 386 – Сигнал датчика «В» виходить за припустимі межі.
РО – 387 – Ланцюг датчика обірваний або замкнута на масу.
РО – 388 – Ланцюг датчика замкнутий на один із силових виводів.

P0 – 389 – Сигнал датчика «B» перемежований.
P0 – 4XX – .
P0 – 400 – Система рециркуляції відпрацьованих газів несправний.
P0 – 401 – Система рециркуляції відпрацьованих газів неефективна.
P0 – 402 – Система рециркуляції відпрацьованих газів надлишкова.
P0 – 403 – Ланцюг датчика рециркуляції відпрацьованих газів несправний.
P0 – 404 – Сигнал датчика виходить за припустимі межі.
P0 – 405 – Сигнал датчика «A» має низький рівень.
P0 – 406 – Сигнал датчика «A» має високий рівень.
P0 – 407 – Сигнал датчика «B» має низький рівень.
P0 – 408 – Сигнал датчика «B» має високий рівень.
P0 – 410 – Система вторинної подачі (упорскування) повітря несправний.
P0 – 411 – Помилковий потік проходить через систему вторинної подачі повітря.
P0 – 412 – Клапан системи вторинної подачі повітря «A» несправний.
P0 – 413 – Клапан системи вторинної подачі повітря «A» завжди відкритий.
P0 – 414 – Клапан системи вторинної подачі повітря «A» завжди закритий.
P0 – 415 – Клапан системи вторинної подачі повітря «B» несправний.
P0 – 416 – Клапан системи вторинної подачі повітря «B» завжди відкритий.
P0 – 417 – Клапан системи вторинної подачі повітря «B» завжди закритий.
P0 – 420 – Ефективність системи каталізаторів «B1» нижче поріг.
P0 – 421 – Ефективність прогріву каталізатора «B1» нижче поріг.
P0 – 422 – Ефективність головного каталізатора «B1» нижче поріг.
P0 – 423 – Ефективність нагрівача каталізатора «B1» нижче поріг.
P0 – 424 – Температура нагрівача каталізатора «B2» нижче поріг.
P0 – 430 – Ефективність системи каталізаторів «B2» нижче поріг.
P0 – 431 – Ефективність прогріву каталізатора «B2» нижче поріг.
P0 – 432 – Ефективність головного каталізатора «B2» нижче поріг.
P0 – 433 – Ефективність нагрівача каталізатора «B2» нижче поріг.
P0 – 434 – Температура нагрівача каталізатора «B2» нижче поріг.
P0 – 440 – Контроль системи вловлювання пар бензину несправний.
P0 – 441 – Система вловлювання пар бензину погано продувається.
P0 – 442 – Виявлений невеликий витік у системі вловлювання пар.
P0 – 443 – Управління клапаном продувки системи «EVAP» несправний.
P0 – 444 – Клапан продувки системи «EVAP» завжди відкритий.
P0 – 445 – Клапан продувки системи «EVAP» завжди закритий.
P0 – 446 – Управління повітряним клапаном системи «EVAP» несправно.
P0 – 447 – Повітряний клапан системи «EVAP» завжди відкритий.
P0 – 448 – Повітряний клапан системи «EVAP» завжди закритий.
P0 – 450 – Датчик тиску пар бензину несправний.
P0 – 451 – Сигнал датчика тиску пар бензину виходить за допустимі діапазон.
P0 – 452 – Сигнал датчика тиску пар бензину має низький рівень.
P0 – 453 – Сигнал датчика тиску пар бензину має високий рівень.
P0 – 454 – Сигнал датчика тиску пар бензину перемежований.
P0 – 455 – Виявлена грубий витік у системі вловлювання пар.
P0 – 460 – Ланцюг датчика рівня палива несправний.
P0 – 461 – Сигнал датчика рівня палива виходить за припустимі межі.
P0 – 462 – Сигнал датчика рівня палива має низький рівень.
P0 – 463 – Сигнал датчика рівня палива має високий рівень.
P0 – 464 – Сигнал датчика рівня палива перемежований.
P0 – 465 – Ланцюг датчика потоку повітря продувки несправний.
P0 – 466 – Сигнал датчика потоку повітря продувки виходить за допустимі межі.
P0 – 467 – Сигнал датчика потоку повітря продувки має низький рівень.

РО – 468 – Сигнал датчика потоку повітря продувки має високий рівень.
РО – 469 – Сигнал датчика потоку повітря продувки перемежований.
РО – 470 – Датчик тиску вихлопних газів несправний.
РО – 471 – Сигнал датчика тиску виходить за допустимі діапазон.
РО – 472 – Сигнал датчика тиску має низький рівень.
РО – 473 – Сигнал датчика тиску має високий рівень.
РО – 474 – Сигнал датчика тиску перемежований.
РО – 475 – Клапан датчика тиску вихлопних газів несправний.
РО – 476 – Сигнал клапана датчика тиску виходить за допустимі діапазон.
РО – 477 – Сигнал клапана датчика тиску має низький рівень.
РО – 478 – Сигнал клапана датчика тиску має високий рівень.
РО – 479 – Сигнал клапана датчика тиску перемежований.
РО – 500 – Датчик швидкості автомобіля несправний.
РО – 501 – Сигнал датчика швидкості автомобіля виходить за допустимі межі.
РО – 502 – Сигнал датчика швидкості автомобіля має низький рівень.
РО – 503 – Сигнал датчика перемежований або має високий рівень.
РО – 505 – Система підтримки холостого ходу несправний.
РО – 506 – Оберти двигуна під управлінням системи занадто низькі.
РО – 507 – Оберти двигуна під управлінням системи занадто високі.
РО – 510 – Концевик індикації закритого положення дроселя несправний.
РО – 530 – Датчик тиску холодоагенту кондиціонера несправний.
РО – 531 – Сигнал датчика тиску холодоагенту виходить за допустимі діапазон.
РО – 532 – Сигнал датчика тиску холодоагенту має низький рівень.
РО – 533 – Сигнал датчика тиску холодоагенту має високий рівень.
РО – 534 – Більша втрата холодоагенту в кондиціонері.
РО – 550 – Датчик тиску гідропідсилювача керма несправний.
РО – 551 – Сигнал датчика тиску виходить за припустимий діапазон.
РО – 552 – Сигнал датчика тиску має низький рівень.
РО – 553 – Сигнал датчика тиску має високий рівень.
РО – 554 – Сигнал датчика тиску перемежований.
РО – 560 – Датчик бортової напруги несправний.
РО – 561 – Бортова напруга нестабільно.
РО – 562 – Бортова напруга має низький рівень.
РО – 563 – Бортова напруга має високий рівень.
РО – 565 – Ланцюг включення «круїз контролю» несправний.
РО – 566 – Ланцюг вимикання «круїз контролю» несправний.
РО – 567 – Ланцюг продовження роботи «круїз контролю» несправний.
РО – 568 – Ланцюг установки швидкості «круїз контролю» несправний.
РО – 569 – Ланцюг підтримки «накату» «круїз контролю» несправний.
РО – 570 – Ланцюг підтримки «розгону» «круїз контролю» несправний.
РО – 571 – Перемикач включення гальм «круїз контролю» несправний.
РО – 572 – Перемикач завжди замкнуть.
РО – 573 – Перемикач завжди розімкнуть.
РО – 600 – Лінія передачі послідовних даних несправний.
РО – 601 – Помилка контрольної суми внутрішньої пам'яті.
РО – 602 – Програмна помилка контрольного модуля.
РО – 603 – Помилка репрограмуємої пам'яті.
РО – 604 – Помилка оперативного запам'ятовувального пристрою.
РО – 605 – Помилка постійного запам'ятовувального пристрою.
РО – 606 – Помилка модуля управління енергозбереженням.
РО – 700 – Система управління трансмісією несправний.
РО – 701 – Система управління трансмісією працює невірно.

РО – 703 – Перемикач карданний вал/гальма несправний.
РО – 704 – Ланцюг датчика включення зчеплення несправний.
РО – 705 – Датчик діапазону роботи трансмісії несправний.
РО – 706 – Сигнал датчика виходить за припустимі межі.
РО – 707 – Сигнал датчика має низький рівень.
РО – 708 – має високий рівень.
РО – 709 – Сигнал датчика перемежований.
РО – 710 – Датчик температури трансмісійної рідини несправний.
РО – 711 – Сигнал датчика виходить за припустимі межі.
РО – 712 – Сигнал датчика має низький рівень.
РО – 713 – має високий рівень.
РО – 714 – Сигнал датчика перемежований.
РО – 715 – Датчик швидкості турбіни несправний.
РО – 716 – Сигнал датчика виходить за припустимі межі.
РО – 717 – Сигнал датчика відсутній.
РО – 718 – Сигнал датчика перемежований.
РО – 719 – Перемикач карданний вал/гальма замкнуть на масу.
РО – 720 – Ланцюг датчика «Зовнішньої швидкості» несправний.
РО – 721 – Сигнал датчика «Зовнішньої швидкості» виходить за допустимі межі.
РО – 722 – Сигнал датчика «Зовнішньої швидкості» відсутній.
РО – 723 – Сигнал датчика «Зовнішньої швидкості» перемежований.
РО – 724 – Перемикач карданний вал/гальма замкнуть на живлення.
РО – 725 – Ланцюг датчика швидкості обертання двигуна несправний.
РО – 726 – Сигнал датчика виходить за припустимі межі.
РО – 727 – Сигнал датчика відсутній.
РО – 728 – Сигнал датчика перемежований.
РО – 730 – Передаточне число трансмісії невірно.
РО – 731 – Передаточне число трансмісії на 1 передачі невірно.
РО – 732 – Передаточне число трансмісії на 2 передачі невірно.
РО – 733 – Передаточне число трансмісії на 3 передачі невірно.
РО – 734 – Передаточне число трансмісії на 4 передачі невірно.
РО – 735 – Передаточне число трансмісії на 5 передачі невірно.
РО – 736 – Передаточне число трансмісії на передачі заднього ходу невірно.
РО – 740 – Ланцюг управління блокуванням диференціала несправний.
РО – 741 – Диференціал завжди виключений (розблоований).
РО – 742 – Диференціал завжди включений (заблокований).
РО – 743 – Зарезервовано.
РО – 744 – Диференціал стан нестійке.
РО – 745 – Управління стискаючим соленоїдом несправно.
РО – 746 – Соленоїд завжди у виключеному стані.
РО – 747 – Соленоїд завжди у включеному стані.
РО – 749 – Стан соленоїда хитливий.
РО – 750 – Соленоїд «А» включення передачі несправний.
РО – 751 – Соленоїд «А» завжди у виключеному стані.
РО – 752 – Соленоїд «А» завжди у включеному стані.
РО – 754 – Стан соленоїда «А» хитливий.
РО – 755 – Соленоїд «В» включення передачі несправний.
РО – 756 – Соленоїд «В» завжди у виключеному стані.
РО – 757 – Соленоїд «В» завжди у включеному стані.
РО – 759 – Стан соленоїда «В» хитливий.
РО – 760 – Соленоїд «С» включення передачі несправний.
РО – 761 – Соленоїд «С» завжди у виключеному стані.

P0 – 762 – Соленоїд «C» завжди у включеному стані.
P0 – 764 – Стан соленоїда «C» хитливий.
P0 – 765 – Соленоїд «Д» включення передачі несправний.
P0 – 766 – Соленоїд «Д» завжди у виключеному стані.
P0 – 767 – Соленоїд «Д» завжди у включеному стані.
P0 – 769 – Стан соленоїда «Д» хитливий.
P0 – 770 – Соленоїд «E» включення передачі несправний.
P0 – 771 – Соленоїд «E» завжди у виключеному стані.
P0 – 772 – Соленоїд «E» завжди у включеному стані.
P0 – 774 – Стан соленоїда «E» хитливий.
P0 – 780 – Перемикання передач не працює.
P0 – 781 – Перемикання передач із 1-ой на 2-ю не працює.
P0 – 782 – Перемикання передач із 2-й на 3-ю не працює.
P0 – 783 – Перемикання передач із 3-й на 4-ю не працює.
P0 – 784 – Перемикання передач із 4-й на 5-ю не працює.
P0 – 785 – Соленоїд управління синхронізатором несправний.
P0 – 787 – Соленоїд управління синхронізатором завжди виключений.
P0 – 788 – Соленоїд управління синхронізатором завжди включений.
P0 – 789 – Соленоїд управління синхронізатором нестійкий.
P0 – 790 – Ланцюг перемикача режиму руху несправний.
P1 – 291 – На впуску перегріте повітря.
P1 – 292 – Тиск газу (бензину)де те в «CN» високе.
P1 – 293 – Тиск газу (бензину)де те в «CN» низьке.
P1 – 294 – Холостий хід нестабільний.
P1 – 295 – На датчику положення дросельної заслінки немає живлення 5В.
P1 – 296 – На датчику тиску повітря у впускному колекторі немає живлення 5В.
P1 – 297 – Тиск у датчику мало.
P1 – 298 – Широко відкритий дросель збіднює.
P1 – 298 – Виявлена відсутність змін сигналу с.
P1 – 299 – Потік повітря занадто великий.
P1 – 390 – Збій за часом синхронізації колінчатого вала.
P1 – 391 – Провалля сигналу датчика обертання колінчатого вала.
P1 – 391 – Відсутність сигналу «початок відліку» №1 більше половини часу.
P1 – 392 – Відсутність сигналу «початок відліку» №2 більше половини часу.
P1 – 393 – Відсутність сигналу «початок відліку» №3 більше половини часу.
P1 – 394 – Відсутність сигналу «початок відліку» №4 більше половини часу.
P1 – 395 – Відсутність сигналу «початок відліку» №5 більше половини часу.
P1 – 398 – Датчик положення колінчатого вала.
P1 – 486 – Перетиснений випарний рукав.
P1 – 487 – Ланцюг високошвидкісного вентилятора №2.
P1 – 488 – Живлення датчиків 5В відсутнє.
P1 – 489 – Ланцюг реле високошвидкісного вентилятора.
P1 – 490 – Ланцюг реле низькошвидкістного вентилятора.
P1 – 491 – Ланцюг реле радіаторного вентилятора.
P1 – 492 – Сигнал датчика зовнішньої температури завжди високий.
P1 – 493 – Сигнал датчика зовнішньої температури завжди низький.
P1 – 494 – Виявлений витік у ланцюзі перемикача тиску насоса.
P1 – 495 – Виявлений витік у ланцюзі соленоїда насоса.
P1 – 496 – Відсутній 5В вихід.
P1 – 596 – Потужний крововий перемикач має неправильне початкове положення.
P1 – 598 – Сигнал датчика тиску в кондиціонері завжди низький.
P1 – 599 – Сигнал датчика тиску в кондиціонері завжди високий.

P1 – 698 – Немає кодів повідомлень прийнятих в «trans control mode».
P1 – 699 – Немає кодів повідомлень прийнятих в «powertrain control mode».
P1 – 761 – Керуюча контрольна система.
P1 – 762 – Сигнал датчика тиску GOV зміщений.
P1 – 763 – Сигнал датчика тиску GOV завжди високий .
P1 – 764 – Сигнал датчика тиску GOV завжди низький.
P1 – 765 – Зміна напруги в ланцюзі реле.
P1 – 899 – Перемикач паркування/нейтрал перебуває в помилковому положенні.
P1 – 100 – Сигнал датчика витрати повітря перемежований.
P1 – 101 – Сигнал датчика витрати повітря виходить із допустимого діапазону.
P1 – 112 – Сигнал датчика температури повітря на впуску перемежований.
P1 – 116 – Сигнал датчика температури охолоджуючої рідини виходить із допустимого діапазону.

Розробка структурної схеми

Структурна схема системи зображена на рисунку1.

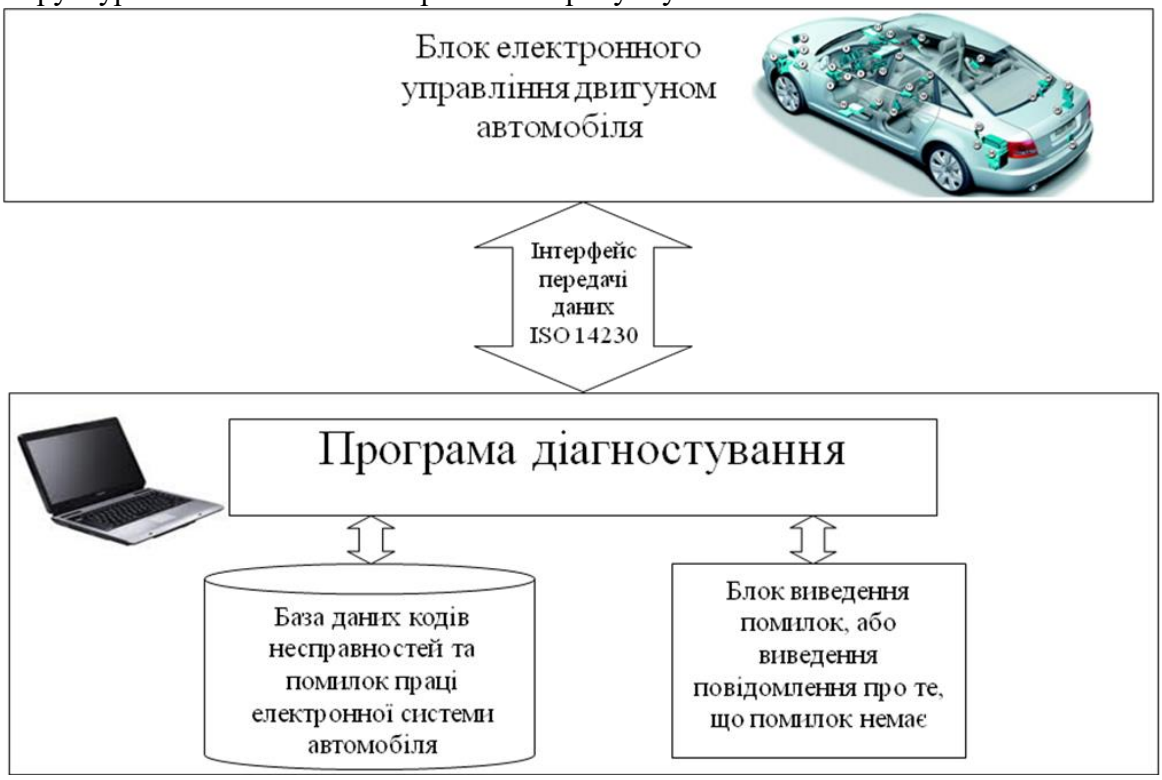


Рисунок 1 – Структурна схема системи

З нього ми бачимо, що основними структурними блоками, які взаємодіють між собою, у ній є наступні:

– Персональній комп’ютер.
– Автомобіль (блок електронного управління двигуном автомобіля).
– Інтерфейс передачі даних ISO 14230.
– Програма діагностування.
– База даних кодів несправностей та помилок праці електронної системи автомобіля.
– Блок виведення помилок, або виведення повідомлення про те, що помилок немає.

Розглянемо як працює розроблена система. Абревіатура E-K-B в автомобільній тематиці має на увазі електронний блок управління або ЕБУ. Тобто ECU це Electronic Control Unit. У сучасному автомобілі є безліч різноманітних ECU. Вони відносяться до гальм, трансмісії, підвісці, системі охорони, кліматичній установці, навігації й іншому.

Найважливіший це блок управління двигуном. У різних джерелах йому можуть відповідати назви як ECU, так і DME (Digital Motor Electronics), ECM (Engine Control Module), PCM (Powertrain Control Module) і деякі ін. Будемо дотримуватися загальноприйнятого терміна ECU як «електронний блок управління», доповнюючи його вказівкою приналежності в міру появи необхідності.

Які можуть бути блоки управління:

– Блок управління автономного нагрівника.
– Блок управління АБС гальм з EDS.
– Блок управління системи підтримки безпечної дистанції.
– Передавач системи контролю тиску в шинах, передній лівий.
– Блок управління бортовою мережею.
– Блок управління у двері водія.
– Блок управління доступом і старту.
– Блок управління в комбінації приладів.
– Блок управління електронними приладами на кермовому стовпчику.
– Блок управління телефоном, системою телематик; приймально-передавач для телефону.
– Блок управління двигуном.
– Блок управління Climatronic.
– Блок управління регулюванням сидіння із запам'ятовувальним пристроєм і регулюванням кермового стовпчика.
– Блок управління регулюванням дорожнього просвіту.
– Блок управління коректором фар.
– Блок управління системою контролю тиску в шинах.
– Блок управління 2 бортовою мережею.
– Блок управління MMI передньої інформаційно-командної панелі.
– Діагностичний інтерфейс для шин даних.
– Модуль, приймаче/зчитування, системи антен для доступу без ключа.
– CD-чейнджер.
– CD-ROM-дисковід.
– Блок управління в задніх лівих дверях.
– Блок управління системою Air-Bag.
– Датчик швидкості обертання автомобіля навколо вертикальної осі.
– Блок управління у двері переднього пасажира.
– Блок управління регулюванням сидіння переднього пасажира із запам'ятовувальним пристроєм.
– Блок управління в задніх правих дверях.
– Передавач системи контролю тиску в шинах, задній лівий.
– Радіоприймач стояночного нагрівника.
– Блок управління системою навігації з CD-дисководом.
– Блок управління голосовим уведенням.
– Блок управління цифровою звуковою системою; радіомодуль; TV-тюнер; цифрове радіо.
– Передавач системи контролю тиску в шинах, задній правий.
– Блок управління системою полегшення паркування.
– Центральний блок управління системою комфорту.
– Блок управління електричним стояночним "ручним" гальмом.
– Блок управління енергопостачанням (менеджер батареї).

Універсальний алгоритм

Спосіб діагностики, що викладається, використовує принцип: якщо немає прямих доказів виходу ECU з ладу, то варто почати пошук причини неполадки в системі в припущенні справності ECU. Прямих доказів дефектності блоку управління існує всього

два. Або ECU має видимі ушкодження, або проблема йде при заміні ECU на свідомо справний (ну, або переноситься на свідомо справний а/м разом з підозрілим блоком; іноді це робити небезпечно, до того ж тут зустрічається виключення, коли блок управління ушкоджений так, що не здатний працювати у всьому діапазоні експлуатаційного розкиду параметрів різних екземплярів однієї й тої ж системи управління, але на одному із двох а/м все-таки працює).

Діагностика повинна розвиватися в напрямку від простого до складного й згідно з логікою роботи системи управління. Саме тому припущення про дефект ECU варто залишити «на потім». Спочатку розглядаються загальні міркування здорового глузду, потім послідовній перевірці підлягають функції системи управління. Ці функції чітко розділяються на забезпечуючі роботу ECU і на функції ECU, що виконуються. Спочатку повинні перевірятися функції забезпечення, потім – функції виконання. У цьому головну відмінність послідовної перевірки від довільної: вона виконується по пріоритеті функцій. Відповідно, кожний із цих двох видів функцій може бути представлений своїм списком у порядку убування значимості для роботи системи управління в цілому.

Діагностика успішна тільки тоді, коли вказує на найважливішу із втрачених або порушених функцій, а не на довільний набір таких. Це істотний момент, тому що втрата однієї функції забезпечення може приводити до неможливості роботи декількох функцій виконання. Останні не будуть працювати, але аж ніяк не будуть втрачені, їхня відмова відбудеться просто в результаті причинно-наслідкових зв'язків. Саме тому такі несправності прийнята називати наведеними.

При непослідовному пошуку наведені несправності маскують справжню причину проблеми (досить характерно для діагностики сканером). Зрозуміло, що спроби боротися з наведеними несправностями «у чоло» ні до чого не приводять, повторне сканування ECU дає колишній результат. Ну а ECU «є предмет темний і науковому дослідженню не підлягає», та й замінити його для проби, як правило, нема чим – от схематичні начерки процесу помилкового вибракування ECU.

Отже, універсальний алгоритм пошуку несправності в системі управління такий:

– візуальний огляд, перевірка найпростіших міркувань здорового глузду;
– сканування ECU, читання кодів несправностей (по можливості);
– огляд ECU або перевірка шляхом заміни (по можливості);
– перевірка функцій забезпечення роботи ECU;
– перевірка функцій виконання ECU.

Важлива роль належить докладному опитуванню власника про те, які зовнішні прояви несправності він спостерігав, як виникла або розвивалася проблема, які дії в цьому зв'язку вже були початі. Якщо проблема в системі управління двигуном, варто приділити увагу питанням про сигналізацію (протиугінну систему), так як електрика додаткових устроїв свідомо менш надійна через спрощені прийоми їхньої установки (наприклад, пайка або стандартні з'єднувачі в призначуваних точках розгалуження й розсічення штатного проведення при підключенні додаткового джгута, як правило, не застосовуються; причому пайка найчастіше не застосовується свідомо через нібито її нестійкість перед вібрацією, що для якісної пайки, звичайно, не так).

Крім того, необхідно точно встановити, який саме а/м перед вами. Усунення скільки-небудь серйозної несправності в системі управління припускає використання електричної схеми останньої. Електросхеми зведені в спеціальні автомобільні комп'ютерні бази по діагностиці й нині досить доступні, треба лише правильно вибрати потрібну. Звичайно, якщо задати саму загальну інформацію з а/м (відзначимо, що бази по електросхемам не оперують VIN-номерами), розвідувач бази знайде кілька різновидів моделі а/м, і буде потрібно додаткова інформація, що може повідомити власник. Наприклад, назву двигуна завжди записано в техпаспорті – букви перед номером двигуна.

Візуальний огляд відіграє роль найпростіших діагностичних затрат. Нерідко досить прості несправності приводять до складних зовнішніх проявів і змушують

вважати складною просту проблему. Тому в процесі попереднього огляду повинно перевірятися:

– наявність палива в бензобаку (якщо підозра на систему управління двигуном);

– відсутність затички у вихлопній трубі (якщо підозра на систему управління двигуном);

– чи затягнуті клеми акумуляторної батареї (АКБ) і їхній стан;

– відсутність видимого ушкодження електропроводки;

– чи добре вставлені (повинні бути защелкнуті й не переплутані) роз'єми проведення системи управління;

– попередні чужі дії по подоланню проблеми;

– дійсність ключа запалювання – для автомобіля зі штатним іммобілайзером (якщо підозра на систему управління двигуном);

Іноді буває корисно оглянути місце установки ECU. Не так уже рідко воно виявляється залито водою, наприклад, після мийки двигуна установкою високого тиску. Вода згубна для ECU негерметичного виконання. Помітимо, що роз'єми ECU також бувають як герметичного, так і простого виконання. Роз'єм повинен бути сухим (припустимо застосовувати як водовідштовхувальні кошти, наприклад, WD-40).

Читання кодів несправностей

Якщо для читання кодів несправностей застосовується сканер або комп'ютер з адаптером, важливо, щоб їхнє з'єднання із цифровою шиною ECU було виконано правильно. Ранні ECU не встановлюють зв'язок з діагностикою, поки не приєднані обидві лінії K і L.

Сканування ECU, або активація самодіагностики автомобіля дозволять швидко визначити нескладні проблеми, наприклад, із числа виявлення несправних датчиків. Причому для ECU однаково, несправні сам датчик або його дроти.

Завжди варто пам'ятати, що формування ECU діагностичних повідомлень, зчитувальних сканером, значно формалізоване й підлегле закладеній програмі самодіагностики. Остання видає найбільш імовірну на думку розроблювача, що написав програму, причину несправності. Але очевидно, що найбільш імовірна причина буде реалізовуватися не щораз.

Ще гірше, коли найбільш імовірну причину алгоритм самодіагностики ігнорує (очевидно, у чинність великої віри розроблювача в надійність того або іншого вузла). Так, наприклад, самодіагностика деяких французьких автомобілів при відсутності пуску двигуна через обрив ланцюга датчика положення коленвала не передбачає тестування цього датчика. І тому навіть дилерський прилад DIAG-2000 у цілому ряді випадків при перевірці системи управління двигуном не знаходить придбаний обрив зазначеного ланцюга.

Виконавчі механізми, наприклад, реле, керовані ECU, перевіряються сканером у режимі примусового включення навантажень. Цей режим називається тестом виконавчих механізмів. Тут знов-таки важливо відрізняти дефект у навантаженні від дефекту в її проведенні.

По-справжньому повинна насторожувати ситуація, коли спостерігається сканування множинних кодів несправностей. При цьому досить велика ймовірність того, що частина з них відноситься до наведених несправностей. Така вказівка на несправність ECU, як «немає зв'язку», – означає, швидше за все, що ECU знеструмлено або відсутній яке-небудь одне його живлення або заземлення.

Якщо немає у своєму розпорядженні сканер або його еквівалент у вигляді комп'ютера з адаптером ліній K і L, більшу частину перевірок можна зробити вручну (див. розділи «Перевірка функцій...»). Звичайно, це буде повільніше, але при послідовному пошуку й обсяг роботи може бути невеликий.

Огляд і перевірка ECU

У тих випадках, коли доступ до ECU простий, а сам блок може бути легко розкритий, варто оглянути його. От що може спостерігатися в несправному ECU:

– обриви, відшарування струмоведучих доріжок, часто з характерними підпалинами;
– спучені або тріснуті електронні компоненти;
– прогари друкованої плати аж до наскрізних;
– вода;
– окисли білий, синьо-зелений або коричневий кольори;

Як уже було сказано, вірогідно перевірити ECU можна шляхом заміни на свідомо справний. Дуже добре, якщо діагност розташовує перевірочним ECU. Однак варто зважати на ризик вивести цей блок з ладу, адже часто першопричина проблеми – несправність зовнішніх ланцюгів. Тому необхідність мати перевірочні ECU не очевидна, а сам прийом варто застосовувати з великою обачністю. На практиці набагато продуктивніше в початковій фазі пошуку вважати ECU справним уже тільки тому, що його огляд не переконує у зворотному. Буває нешкідливо просто переконатися, що ECU на місці.

Перевірка функцій забезпечення

До функцій забезпечення роботи ECU системи управління двигуном відносяться:
– живлення ECU як електронного устрою;
– обмін з керуючим блоком іммобілайзера – якщо є штатний іммобілайзер;
– запуск і синхронізація ECU від датчиків положення коленвала й/або розподільчого вала;
– інформація з інших датчиків.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів мережевих прикінцевих пристроїв автомобіля. В межах України в недостатній мірі представлені вітчизняні розробки в цій області. У роботі наведені теоретичне узагальнення й рішення наукового завдання дослідження методів мережевих прикінцевих пристроїв автомобіля. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем мережевих прикінцевих пристроїв автомобіля; Досліджена система мережевих прикінцевих пристроїв автомобіля; На основі отриманих результатів досліджень створена програмна реалізація системи мережевих прикінцевих пристроїв автомобіля. Розроблені під час виконання роботи алгоритми дозволяють успішно вирішувати завдання мережевих прикінцевих пристроїв автомобіля. 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. 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 комп'ютерної електроніки: 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 (ІТ & І): 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

Р. Рудяк, магістр гр. КІ-19М-1,4,
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ КІБЕРБЕЗПЕКИ ДЛЯ АВТОМАТИЗОВАНОГО ЗАХИСТУ КОРПОРАТИВНОЇ МЕРЕЖІ

У статті розроблено програмне забезпечення, яке призначено для системи кібербезпеки для автоматизованого захисту корпоративної мережі. Метою розробки є дослідження та програмна реалізація системи кібербезпеки для автоматизованого захисту корпоративної мережі. Об'єктом дослідження є процес кібербезпеки для автоматизованого захисту корпоративної мережі. Предметом дослідження є методи кібербезпеки для автоматизованого захисту корпоративної мережі. Методи дослідження базуються на методах захисту інформації, методах математичної статистики, методах розробки програмного забезпечення. 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 доступу, корпоративна мережа

Постановка проблеми. Для деяких процесів удалося радикально підвищити точність визначення атак, причому настільки, що досягнута точність перевищила показники людини. Процеси легко автоматизують, коли вони однозначні й повторювані. Наприклад антивіруси – їх треба було тільки встановити, інше вони робили самі: скачували відновлення баз даних, визначали й блокували віруси, іноді запитуючи підтвердження. Визначення вірусів, сигнатури атак і інших простих методів захисту працювали безвідмовно доти, поки атаки не стали персоніфікованими. Інакше кажучи, зловмисники стали враховувати особливості конкретного об'єкта захисту й саму систему захисту. Виявляти віруси й атаки за допомогою вже відомих зразків тепер вдавалося не завжди, що змусило вдатися до набагато менш точного способу – поведінкового аналізу: ні на один відомий вірус це не схоже, але веде воно себе як вірус. Перші системи такого роду викликали протести користувачів: кількість помилкових спрацьовувань у порівнянні зі старими технологіями було неприйнятним, користувачеві доводилося постійно відволікатися від роботи, щоб розбиратися з повідомленнями антивірусу.

Поступово всі зійшлися на тому, що заради захисту прийде упокоритися з помилковими спрацьовуваннями, але відрізнити фіктивну тривогу від реальної атаки може не кожний. Так з'явилися професійні оператори систем захисту, які аналізували повідомлення систем безпеки й дозволяли колізії. «Системи захисту» – устояний, але неправильний термін, адже по суті мова йде про системи моніторингу, оскільки така система лише повідомляє оператора про підозрілу активність, а ті або інші міри приймає людина, від кваліфікації якого багато в чому залежить їхня ефективність.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи кібербезпеки для автоматизованого захисту корпоративної мережі.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи кібербезпеки для автоматизованого захисту корпоративної мережі.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

- Огляд існуючих систем кібербезпеки для автоматизованого захисту корпоративної мережі.
- Дослідження системи кібербезпеки для автоматизованого захисту корпоративної мережі.
- Програмна реалізація системи кібербезпеки для автоматизованого захисту корпоративної мережі.

Об'єктом дослідження є процес кібербезпеки для автоматизованого захисту корпоративної мережі.

Предметом дослідження є методи кібербезпеки для автоматизованого захисту корпоративної мережі.

Методи дослідження базуються на методах захисту інформації, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. У Безпека даних – одне з головних завдань, розв'язуваних IT-відділами компаній. Причому мова йде не тільки про запобігання витоку корпоративної інформації, зниженні обсягів паразитного трафіку й відбитті атак на ресурси компанії, але й про оптимізацію роботи системи в цілому. Знайти універсальне рішення в даному питанні практично неможливо: неоднорідність сфер діяльності й структур організацій переводить завдання в категорію потребуючого індивідуального підходу. Однак для грамотних фахівців нерозв'язних проблем не існує. У цій роботі ми поговоримо про ключові підходи, методи й засоби інформаційної безпеки, а також оцінимо вартість конкретних рішень.

Особливості й завдання корпоративних систем захисту інформації

Забезпечення інформаційної безпеки актуально насамперед для корпорацій зі складною, територіально-розподіленою, багаторівневою структурою: великих банків, транснаціональних і державних компаній.

Найчастіше корпоративні мережі подібних організацій побудовані з використанням устаткування різних поколінь і від різних виробників, що помітно ускладнює процес керування IT-системою.

Крім того, інформаційні структури корпорацій відрізняються різнорідністю, вони складаються з різних баз, наборів розподілених і локальних систем. Це робить ресурси корпоративного рівня особливо уразливими.

У процесі обміну даними між користувачами організації й зовнішнім миром мережі можуть бути уражені шкідливими програмами, які руйнують бази даних і здійснюють передачу відомостей третім особам.

Однак сказати, що завдання забезпечення інформаційної безпеки неактуальна для середнього й малого бізнесу, теж було б невірно.

Особливо сьогодні, коли бізнес-процеси активно переходять у віртуальний простір: оплата товарів і послуг через Інтернет, електронна пошта, IP-Телефонія, хмарні сховища, віртуальні сервера – все це стало типово для сучасних фірм середньої руки, як і атаки хакерів, витік конфіденційних даних, у тому числі фінансових і т.д.

Отже, що ж ставиться до головних погроз корпоративної мережі? На думку фахівців, найбільш серйозну небезпеку для IT-інфраструктури сьогодні представляють віруси (троянське ПЗ, хробаки), шпигунське й рекламне програмне забезпечення, спам і фішинг-атаки типу «відмова в обслуговуванні», підміна головної сторінки інтернет-ресурсу й соціальний інжиніринг. Причому джерелом погроз можуть бути як зовнішні користувачі, так і співробітники (часто ненавмисно).

Реалізація шкідливих алгоритмів може привести як до паралізації системи і її збоїв, так і до втрати, підміні або витоку інформації.

Все це чревате величезними іміджевими, часовими й фінансовими втратами для компанії.

Таким чином, головними завданнями будь-якої системи інформаційної безпеки є:

– забезпечення доступності даних для авторизованих користувачів – можливості оперативного одержання інформаційних послуг;

– гарантія цілісності інформації – її актуальності й захищеності від несанкціонованої зміни або знищення;

– забезпечення конфіденційності відомостей.

Для рішення позначених цілей сьогодні застосовуються такі методи захисту інформації, як реєстрація й протоколювання, ідентифікація й автентифікація, керування доступом, створення міжмережевих екранів і криптографія.

Регуляторами висуваються наступні вимоги до захисту даних у комп'ютерних мережах:

– використання ліцензійних технічних засобів і ПЗ;

– проведення перевірки об'єктів інформації на відповідність нормативним вимогам по захищеності;

– складання списку припустимих до застосування програмних засобів і заборона на використання засобів, що не входять у цей перелік;

– використання й своєчасне відновлення антивірусних програм, проведення регулярних перевірок комп'ютерів на предмет зараження шкідливими ПЗ;

– розробка способів профілактики по недопущенню влучення вірусів у мережу;

– розробка методів зберігання й відновлення зараженого ПЗ.

У банківських структурах також необхідно забезпечувати розмежування доступу до даних для запобігання злочинних дій з боку співробітників і впроваджувати методи шифрування даних з метою забезпечення безпеки проведення електронних грошових операцій.

Комплексний підхід при побудові системи інформаційної безпеки й захисти інформації

Надійний захист інформації може забезпечити тільки комплексний підхід, що припускає одночасне використання апаратних, програмних і криптографічних засобів (жодне із цих засобів окремо не є досить надійним).

Подібний підхід передбачає аналіз і оптимізацію всієї системи, а не окремих її частин, що дозволяє забезпечити баланс характеристик, тоді як поліпшення одних параметрів нерідко приводить до погіршення інших.

Стандартом побудови системи безпеки є ISO 17799, що передбачає впровадження комплексного підходу до рішення поставлених завдань.

Дотримання даного стандарту дозволяє вирішити завдання по забезпеченню конфіденційності, цілісності, вірогідності й доступності даних.

Організаційні міри, прийняті при комплексному підході, є самостійним інструментом і поєднують всі використовувані методи в єдиний цілісний захисний механізм. Такий підхід забезпечує безпека даних на всіх етапах їхньої обробки. При цьому правильно організована система не створює користувачам серйозних незручностей у процесі роботи.

Комплексний підхід включає детальний аналіз впроваджуваної системи, оцінку погроз безпеки, вивчення засобів, використовуваних при побудові системи, і їхніх можливостей, аналіз співвідношення внутрішніх і зовнішніх погроз і оцінку можливості внесення змін у систему.

Методи й засоби захисту інформації

Таким чином, для забезпечення захисту інформації необхідно вживати наступних заходів:

- формування політики безпеки й складання відповідної документації;
- впровадження захисних технічних засобів.

І хоча 60-80% зусиль по забезпеченню безпеки у великих компаніях спрямовано на реалізацію першого пункту, другий є не менш, а можливо й більше, важливим.

До основних програмно-апаратних засобів ставляться наступні.

Міжмережеві екрани

Вони забезпечують поділ мереж і запобігають порушенню користувачами встановлених правил безпеки. Сучасні міжмережеві екрани відрізняються зручним керуванням і більшим функціоналом (можливістю організації VPN, інтеграції з антивірусами й ін.).

У цей час спостерігаються тенденції:

- до реалізації міжмережевих екранів апаратними, а не програмними засобами (це дозволяє знизити витрати на додаткове устаткування й ПЗ й підвищити ступінь захищеності);
- до впровадження персональних міжмережевих екранів;
- до орієнтації на сегмент SOHO, що приводить до розширення функціонала даних засобів.

Антивірусний захист інформації

Зусилля найбільших виробників спрямовані на забезпечення ешелонованого захисту корпоративних мереж. Розроблювальні системи захищають робочі станції, а також закривають поштові шлюзи, проксі-сервери й інші шляхи проникнення вірусів. Ефективним рішенням є паралельне використання двох і більше антивірусів, у яких реалізовані різні методи виявлення шкідливого ПЗ.

Системи виявлення атак

Подібні системи тісно інтегровані із засобами блокування шкідливих впливів і із системами аналізу захищеності. Система кореляції подій акцентує увагу адміністратора тільки на тих подіях, які можуть завдати реальної шкоди інфраструктурі компанії. Виробники IDS прагнуть до підвищення швидкісних показників своїх розробок.

Контроль доступу й засобу захисту інформації усередині мережі

З метою забезпечення безпеки даних великими компаніями проводиться автоматизація керування інформаційною безпекою або створення загальної консолі керування, а також розмежування доступу між співробітниками відповідно до їх функціонала.

В області засобів створення VPN відзначається прагнення до підвищення продуктивності процесів шифрування й забезпечення мобільності клієнтів (тобто доступу до відомостей з будь-якого пристрою).

Розроблювачі систем контролю вмісту прагнуть домогтися того, щоб створені ними системи не створювали дискомфорту користувачам.

Тенденції в сфері комплексного захисту інформації

Комплексні засоби захисту інформації міняються згодом і визначаються насамперед поточними економічними умовами й існуючими погрозами. Так, збільшення кількості шкідливих атак і економічну кризу змушують українські компанії й держструктури вибирати тільки реально працюючі рішення. Цим пояснюється зміна орієнтирів.

Якщо раніше корпорації були націлені в першу чергу на виконання вимог регуляторів, то тепер їм не менш важливо забезпечити реальну безпеку бізнесу шляхом впровадження відповідних програмних і апаратних засобів.

Усе більше компаній прагне інтегрувати захисні засоби з іншими системами IT-структур, зокрема, SIEM, які в режимі реального часу аналізують події безпеки, що приходять від мережних пристроїв і додатків.

Функція адміністрування засобів захисту передається від підрозділів безпеки в IT-відділи.

Останнім часом керівниками компаній і IT-директорами приділяється особлива увага технологічності застосування, сумісності й керованості засобів захисту.

Відзначається перехід від простого пошуку уразливостей (чисто технічного підходу) до ризик-орієнтованому менеджменту (до комплексного підходу).

Усе більше важливими для клієнтів стають наочність звітності, зручність інтерфейсу, забезпечення безпеки віртуальних середовищ при роботі з мобільними пристроями.

У зв'язку зі збільшенням частки цільових атак росте попит на рішення в області захищеності критичних об'єктів і інфраструктури (розслідування комп'ютерних інцидентів, запобігання DDoS-атак).

Вартість рішень по захисту інформації

Ціна організації корпоративної системи захисту відомостей складається з безлічі складових. Зокрема, вона залежить від сфери діяльності компанії, кількості співробітників і користувачів, територіальної розподіленості системи, необхідного рівня захищеності й ін.

На вартість робіт впливає ціна устаткування, що здобувається, і ПЗ, обсяг виконуваних робіт, наявність додаткових сервісів і інші фактори. Так, вартість програмно-апаратного комплексу Cisco WebSecurity варіюється від $170 (при кількості користувачів до 1000) до $670 (5000-10 000 користувачів). пристрій, що розгортається Локально, McAfee WebGateway коштує від $2000 до $27 000. Ціна веб-фільтра Websense WebSecurity може досягати $40 000. Вартість Barracuda WebFilter стартує від $1500 за устаткування, що обслуговує до 100 користувачів одночасно (апарат для обслуговування 300-8000 користувачів обійдеться в $4000). При цьому щорічне відновлення ПЗ обійдеться ще в $400-1100. Придбати GFI WebMonitor для 100 користувачів на один рік можна за $2600.

Отже, сучасна інформаційна безпека компанії базується на концепції комплексного захисту інформації, що припускає одночасне використання багатьох взаємозалежних програмно-апаратних рішень і мер соціального характеру, які підтримують і доповнюють один одного. У тому числі безпека компанії допомагають забезпечити й системи корпоративного керування паролями.

Розробка структурної схеми

Розглянемо які атаки можуть бути початі зловмисником, що працює з-під облікового запису звичайного користувача без привілеїв локального адміністратора. Зокрема, ми наводили приклад того, як спрощене спадкування привілеїв у рамках доменної авторизації (Single-Sign-On) дозволяє зловмисникові одержати доступ до різних мережних ресурсів і сервісів, діючи з-під обмеженого облікового запису звичайного користувача. У цьому розділі ми детально розглянемо можливі вектори атаки на корпоративну мережу зсередини, тобто із зараженого комп'ютера.

Після того, як зловмисник одержав контроль над якою-небудь користувальницькою системою в корпоративній мережі, всі подальші події укладаються в три послідовних етапи: закріплення в системі, аналіз оточення й поширення. Є безліч варіантів реалізації кожного з описаних етапів, що розрізняються технічними методами, стратегією й тактикою. Можливі

варіанти дій зловмисника, спрямованих на закріплення, аналіз і поширення в корпоративній мережі, зображені на структурній схемі нижче.

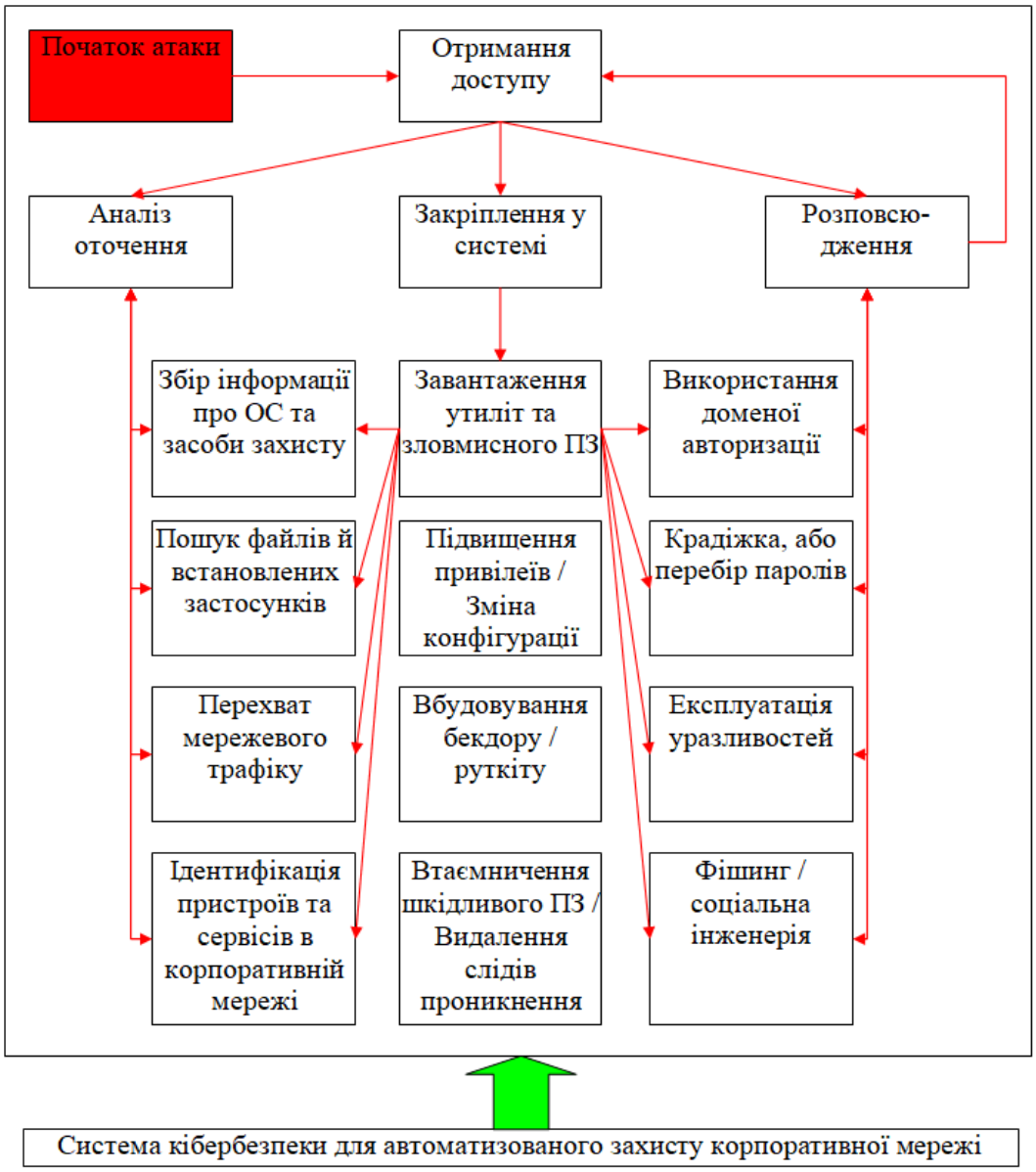


Рисунок 1 – Структурна схема системи

Для фахівців ІБ важливо знати ознаки, по яких та або інша атака може бути вчасно виявлена. Так, використовуючи запропоновану «карту дій», фахівці ІБ можу виявити атаку, зіставляючи події, що відбуваються в мережі, з різними шаблонами поводження зловмисника.

Закріплення в системі

Звичайно в перші мінути або годинники після проникнення в корпоративну мережу хакер завантажує на атакований комп'ютер утиліти (у т.ч. шкідливі), необхідні для збору інформації про систему й установленому ПЗ, пошуку файлів і даних, установлення зв'язку із центром керування (C&C), крадіжки облікових даних, перебору паролів, злому облікових записів, підвищення привілеїв, зараження системи, перехоплення мережного трафіку, сканування пристроїв у мережі й т.і.

Щоб сховати завантаження всіх необхідних інструментів від очей мережних адміністраторів і фахівців ІБ і уникнути спрацьовування всіляких систем захисту, хакери прибігають до маневрів різного ступеня складності:

– Файли передаються по мережних протоколах/портам загального призначення (HTTP, FTP, HTTPS, SFTP), розчиняючись у величезному потоці щоденного користувальницького трафіку.

– Файли завантажуються зі зламаних серверів, з використанням Fast Flux мереж або через Tor.

– Файли передаються вроздріб, в обфускованому і/або зашифрованому виді.

– Іноді для передачі використовуються різні види стеганографії, наприклад, приховання даних усередині аудіо/відео файлів, зображень або заголовків інтернет-протоколів (особливо якщо порти загального призначення закриті мережним екраном).

Після завантаження необхідних інструментів зловмисники намагається одержати доступ до облікового запису локального адміністратора або системи. У першому випадку звичайно використовується ПЗ для перехоплення уведення із клавіатури, перебору паролів, злому облікових записів або фішінг. У другому випадку для одержань доступу до системного облікового запису (тобто привілеїв рівня ядра) звичайно використовуються експлойти уразливостей у системних сервісах.

Використовуючи отримані привілеї, зловмисники зможе глибоко закріпитися в системі, впровадивши в ОС руткіт або буткіт, очистити систему від слідів проникнення, сховати свої інструменти й сліди активного зараження від локальних засобів захисту. Якщо зловмисникові не вдалося закріпитися в системі «класичним» способом, він може настроїти автоматичне зараження системи, наприклад, використовуючи стандартний планувальник завдань.

Зрозуміло, у кожному конкретному випадку сценарій «закріплення в системі» може значно відрізнятися від запропонованого вище опису. Але, як ми говорили на початку статті, для фахівця ІБ важливо розуміти принципи проведення атаки й уміти уявляти собі завдання, які вирішує зловмисник. Так, на етапі закріплення основне завдання зловмисника – організувати надійний довгостроковий доступ до атакованої системи. У загальному випадку, рішення завдання віддаленого доступу складається із двох частин: створення каналу передачі даних і впровадження засобу віддаленого керування (бекдору).

Аналіз оточення

До, після або одночасно із закріпленням у системі зловмисникові необхідно зібрати інформацію про ОС і її конфігурацію, установлених відновленнях, програмах і засобах захисту. Ця інформацію не тільки придасться для оцінки поточної ситуації й планування наступних кроків атаки, але й украй корисна для точного підбора необхідних утиліт і експлойтів.

Для збору інформації про систему звичайно цілком достатньо наявних під рукою засобів:

– cmd, regedit, vbs, powershell в ОС Windows;

– bash, grep, python, perl в Unix/Linux і Mac OS.

З погляду хакеру, є маса плюсів у тім, щоб використовувати перераховані утиліти – вони є в кожній системі, доступні навіть із обмеженими правами користувача, а їхня робота не контролюється більшістю засобів захисту. Для рішення більше складних завдань зловмисники використовують як широко відомі, так і власні утиліти, що дозволяють перехоплювати мережний трафік, сканувати пристрою в мережі, підключатися до різних мережних служб, використовуючи доменну авторизацію, і т.д. При цьому, якщо хакерські утиліти написані, скажемо, на python, те зловмисники напевно встановлять необхідне ПЗ на заражений комп'ютер. У цьому випадку, python (і т.п.) швидше за все не буде схований у системі за допомогою руткіта, оскільки це може викликати проблеми в роботі інтерпретатора.

Для пошуку й аналізу інших пристроїв у корпоративній мережі, зловмисники застосовують методи пасивного й активного сканування. Зокрема, використовуючи сніффер для прослуховування трафіку з локального мережного інтерфейсу, можна легко виявити різні

пристрої по ARP-Пакетах або активних підключеннях, визначити адреси серверів, на яких розташовані корпоративні додатки, такі як ActiveDirectory, Outlook, бази даних, корпоративні вебсайти й багато хто інші. Для одержання детальної інформації про конкретний вузол мережі зловмисники використовують мережні сканери (наприклад, nmap), що дозволяють визначити доступні мережні служби, угадати назву й версію ПЗ, виявити присутність мережного екрана, IDS/IPS.

Поширення

Після того, як зловмисники закріпився в системі, організував надійний канал для віддаленого доступу й зібрав досить інформації про корпоративну мережу, його подальше дії звичайно спрямовані на досягнення вихідної мети – це може бути крадіжка конфіденційної інформації, атака на інфраструктуру компанії,одержання контролю над критичними системами з метою шантажу або ж власні потреби. За винятком випадків, коли споконвічно атакована система, є кінцевою метою (наприклад, ноутбук CEO, центральний сервер або вебсайт), зловмисникові необхідно захопити контроль над іншими системами усередині корпоративної мережі – залежно від обраної мети зараження може бути крапковим або масовим.

Наприклад, для атаки на інфраструктуру швидше за все буде потрібно масове зараження як серверів, що забезпечують виконання різних бізнес-процесів, так і робітників станцій операторів і адміністраторів. З іншого боку, для крадіжки конфіденційної інформації або шпигунства зловмисникові прийде діяти з великою обережністю, атакуючи тільки самі пріоритетні системи.

Поширення усередині корпоративної мережі може бути реалізовано безліччю способів. Так само, як у випадку із закріпленням у системі й аналізом оточення, зловмисники вибирають найбільш прості рішення, зокрема – використання існуючих облікових записів. Наприклад, запускаючи шкідливий код з-під доменного облікового запису користувача зараженої системи, зловмисник може вільно підключатися до різних мережних сервісів (до яких у користувача є доступ) використовуючи доменну авторизацію (Single Sign-On), тобто без вказівки логіна/пароля. З іншого боку, використовуючи перехоплювач уведення із клавіатури, зловмисник легко може одержати логін/пароль як від доменного облікового запису, так і від інших сервісів, що не підтримують доменну авторизацію. Також зловмисник може спробувати використовувати уразливості в механізмах зберігання й перевірки облікових даних або використовувати перебір пароля.

Найбільш ефективним способом поширення усередині корпоративних мереж є експлуатація уразливостей, оскільки більша частина захисту корпоративної мережі зосереджена на запобіганні зовнішніх атак. Як наслідок, усередині мережі можна зустріти безліч різноманітних уразливостей, незахищених корпоративних сервісів, тестових серверів, систем керування/віртуалізації й т.п. Практика показує, що навіть якщо фахівцям ІБ і інженерам ІТ відомо про всі уразливості у корпоративній мережі, їхнє усунення триває роками, оскільки вимагає великої кількості ресурсів (людино-годин). Проте, досвідчені хакери з обережністю використовують експлойти для відомих уразливостей, воліючи атакувати незахищені корпоративні сервіси – у випадку, якщо в мережі все-таки використовується IDS/IPS (локальне або мережний), використання експлойтів для відомих уразливостей може привести до виявлення зловмисника.

Виявлення атаки

На кожному етапі атаки зловмисники часто використовують оточення й наявні під рукою засоби у власних цілях, залишаючись непомітними на тлі активності звичайних користувачів. Для рішення цієї проблеми необхідно зменшувати надмірність оточення й бізнес-процесів там, де це можливо, а у всіх інших випадках необхідно стежити за тим, що відбувається, виявляти аномалії й реагувати на них.

Наочним прикладом надмірності в бізнес-процесах є вільний доступ до бізнес-активам (конфіденційним документам, критичним додаткам, устаткуванню й т.д.), права локального адміністратора й можливість віддаленого підключення до корпоративної мережі

для тих, кому такі права й доступ не потрібні. Сказане ставиться не тільки до поділів прав на рівні домену, але й на рівні прикладного ПЗ – звичайно браузерах не потрібний доступ до пам'яті інших процесів, а MS Office нема чого встановлювати драйвера.

Як приклад надмірності оточення можна привести наявність на комп'ютері рядового співробітника (не є розроблювачем, тестувальником, адміністратором або фахівцем ІБ) ПЗ для перехоплення мережного трафіку, сканування мережі, віддаленого доступу, створення локального HTTP/FTP сервера, використання стороннього мережного устаткування (Wi-Fi і 3G модемів), засобів розробки ПЗ й т.д.

Ефективна стратегія по запобіганню атак усередині корпоративної мережі полягає в тому, щоб не дати зловмисникові діяти потай, змусити його вживати складні й ризиковані кроки, які дозволять фахівцям ІБ виявити факт атаки й вчасно нейтралізувати погрозу. Для цього в корпоративній мережі необхідно мати дві речі: розумний захист і систему керування інформаційною безпекою (СУІБ). Інформаційна безпека корпоративної мережі, побудована на основі інтеграції цих двох технологій, принципово відрізняється від устояної моделі захисту, а саме – може бачити все, що відбувається в мережі, і негайно реагувати на погрози.

Розумні засоби захисту – це ті ж антивіруси, мережні екрани, IDS/IPS/HIPS, Application Control, Device Control і т.д., але здатні взаємодіяти із СУІБ. Такі засоби захисту повинні не тільки збирати й передавати в СУІБ усіляку інформацію, але й виконувати команди по блокуванню спроб доступу, створення підключень, передачі даних по мережі, запуску додатків, читання й записи файлів і т.д. Звичайно, щоб все це працювало, фахівцеві ІБ необхідно вміти відрізняти легітимну активність від шкідливої.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів кібербезпеки для автоматизованого захисту корпоративної мережі. В межах України в недостатній мірі представлені вітчизняні розробки в цій області. У роботі наведені теоретичне узагальнення й рішення наукового завдання дослідження методів кібербезпеки для автоматизованого захисту корпоративної мережі. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем кібербезпеки для автоматизованого захисту корпоративної мережі; Досліджена система кібербезпеки для автоматизованого захисту корпоративної мережі; На основі отриманих результатів досліджень створена програмна реалізація системи кібербезпеки для автоматизованого захисту корпоративної мережі. Розроблені під час виконання роботи алгоритми дозволяють успішно вирішувати завдання кібербезпеки для автоматизованого захисту корпоративної 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.

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.Рудяк Р.А. Дослідження та програмна реалізація системи кібербезпеки для автоматизованого захисту корпоративної мережі // Збірник праць молодих науковців ЦНТУ. – Вип. 11. – Кропивницький: ЦНТУ, 2021.

5. "Официальное руководство Cisco по подготовке к сертификационным экзаменам CCENT/CCNA ICND1 100-101" Уэнделл Одом (Cisco CCENT/CCNA ICND1 100-101: Official Cert Guide) 978-5-8459-1906-9
6. "Официальное руководство Cisco по подготовке к сертификационным экзаменам CCNA ICND2 200-101. Маршрутизация и коммутация" Уэнделл Одом(Cisco CCNA Routing and Switching ICND2 200-101 Official Cert Guide) 978-5-8459-1907-6
7. Официальное руководство по подготовке к сертификационным экзаменам CCNA ICND2 = CCNA ICND2 Official Exam Certification Guide (CCNA Exams 640-816 and 640-802). – 2-изд. – М.: Вильямс, 2009. – 736 с. – ISBN 978-5-8459-1442-2. ,Официальное руководство Cisco по подготовке к сертификационным экзаменам CCNA ICND2 640-816 = CCNA ICND2 640-816 Official Cert Guide. – 3-изд. – М.: Вильямс, 2012. – 752 с. – ISBN 978-5-8459-1811-6.
8. Программа сетевой академии Cisco CCNA 1 и 2. Вспомогательное руководство = Cisco Networking Academy Program CCNA 1 and 2 Companion Guide. – 3-изд. – М.: Вильямс, 2007. – 1168 с. – ISBN 1-58713-150-1.
9. Программа сетевой академии Cisco CCNA 3 и 4. Вспомогательное руководство = Cisco Networking Academy Program CCNA 3 and 4 Companion Guide. – М.: Вильямс, 2006. – 944 с. – ISBN 1-58713-113-7.
10. Рудяк Р.А. Дослідження та програмна реалізація системи кібербезпеки для автоматизованого захисту корпоративної мережі // Збірник праць молодих науковців ЦНТУ. – Вип. 11. – Кропивницький: ЦНТУ, 2021.

УДК 004

Б. Савич, магістр гр. КІ-19М-1,4
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ КОМПЛЕКСНОГО ЗАСОБУ ВІДЕОНАГЛЯДУ ДЛЯ ЗАХИСТУ ПЕРИМЕТРУ ПІДПРИЄМСТВА

У статті розроблено програмне забезпечення, яке призначено для системи комплексного засобу відеонагляду для захисту периметру підприємства. Метою розробки є дослідження та програмна реалізація системи комплексного засобу відеонагляду для захисту периметру підприємства. Об’єктом дослідження є процес комплексного засобу відеонагляду для захисту периметру підприємства. Предметом дослідження є методи комплексного засобу відеонагляду для захисту периметру підприємства. Методи дослідження базуються на методах теорії кодування, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи комплексного засобу відеонагляду для захисту периметру підприємства. 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, кодування

Постановка проблеми. Захист периметра – комплекс інженерно-технічних заходів, спрямованих на запобігання проникнення зловмисників на територію й несанкціонований вихід або виносу матеріальних цінностей з охоронюваного об'єкта. Створити перешкоду у вигляді забору – це частина робіт із захисту периметра. Але будь-яку перешкоду можна перебороти: вирити підкоп, перелізти, зробити проріз. Вся справа в підготовці зловмисника й часу, який він має.

Системи сигналізації й відеоспостереження на периметрі дозволяють попередити й запобігти проникненню на територію об'єкта, захистити матеріальні цінності, життя й здоров'я людей.

Найбільші переваги інтеграції охоронної сигналізації й системи відеоспостереження проявляються в периметральних системах охорони.

Алгоритми автоматичної взаємодії систем периметральної сигналізації й відеоспостереження на периметрі дозволяють:

– підвищити оперативність реагування – охоронна служба, оперативно впевнившись про реальну небезпеку або тривожну ситуацію, негайно вживає адекватних заходів реагування.

– заощадити, підвищивши при цьому ефективність роботи охорони – щоденний обхід території, цілодобовий режим роботи, реагування на помилкові спрацьовування, – все це вимагає чималих витрат на підтримку на належному рівні роботи служби охорони . Інтеграція охоронного відеоспостереження й сигналізації дозволяють скоротити кількість співробітників служби охорони.

– підвищити адекватність реакції – є різні ситуації, наприклад, через забір перелазять хлопчиська, щоб забрати свій м'яч, або два чоловіки в камуфляжній формі намагаються зробити проріз у заборі. Погодитеся, що реакція повинна бути різною. Відеоспостереження дозволяє застосувати міри адекватні погрозі.

– захистити працівників служби охорони – співробітникам охорони не потрібно виходити один на один з порушниками й збройними злочинцями тільки для того, щоб переконатися, чи дійсно на об'єкт зроблені напад або ж відбулося помилкове спрацьовування системи.

Украй ефективна робота купольних поворотних камер у взаємодії із системою захисту периметра.

Система працює в такий спосіб: при надходженні сигналу про проникнення з ділянки периметра, високошвидкісна поворотна камера виводить ділянку периметра операторові на екран. Таким чином, можна однією поворотною камерою охопити периметр у кілька кілометрів, за умови установки її на вишку.

Такий спосіб охорони заощаджує значні засоби при розгортанні дорогої системи відеоспостереження на периметрі, де доводиться встановлювати камери, мінімум, через кожні 50 метрів.

Активний розвиток відеоаналітики приводить до появи зручних інструментів, які підвищують якісні характеристики систем охорони й зручність роботи оператора. Нерідко робота відеоаналітики істотно впливає на тактику охорони. Робота детекторів руху по зображенню з камер, детекторів перетинання лінії, трекерів об'єктів, дозволяє автоматизувати роботу оператора й зняти з його навантаження за цілодобовим спостереженням за відеокамерами й аналізу зображень. При спрацьовуванні детектора увагу оператора буде автоматично притягнуто до тривожної камери. Використання функцій відеоаналітики істотно знімає навантаження з оператора системи відеоспостереження й дозволяє підвищити ефективність роботи служби охорони!

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи комплексного засобу відеонагляду для захисту периметру підприємства.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи комплексного засобу відеонагляду для захисту периметру підприємства.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем комплексного засобу відеонагляду для захисту периметру підприємства.

– Дослідження системи комплексного засобу відеонагляду для захисту периметру підприємства.

– Програмна реалізація системи комплексного засобу відеонагляду для захисту периметру підприємства.

Об’єктом дослідження є процес комплексного засобу відеонагляду для захисту периметру підприємства.

Предметом дослідження є методи комплексного засобу відеонагляду для захисту периметру підприємства.

Методи дослідження базуються на методах теорії кодування, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. У Одна з основних цілей відеоспостереження – це охорона периметра об'єкта**.** Периметр відеоспостереження може бути організований на базі, як аналогових відеокамер, так і цифрових. Система відеоспостереження, як правило, передбачає цілодобове функціонування, тому при проектуванні й монтажі системи відеоспостереження використовують камери з підвищеною розв'язною здатністю, найчастіше використовуються камери з розв'язною здатністю 570 тб – ліній. Використання таких камер для периметра, дозволяє чітко розпізнавати особи людей і номери машин на досить великій відстані. Також необхідними опціями, для камер, використовуваних для охорони периметра, є низьке енергоспоживання, компенсація засвітлення тла й кілька режимів електронного затвора. При монтажі системи відеоспостереження можливе використання, як кольорових, так і чорно – білих камер.

Для підвищення ефективності системи, при установці камер відеоспостереження, використовуються поворотні пристрої. Поворотні пристрої для камер, дозволяють значно розширити кут огляду камери, стежити за більшими площами охоронюваного об'єкта. Камери з поворотним механізмом мають можливість спостереження за об'єктом у русі. Відеокамери, при установці яких використовуються поворотні механізми, як правило, можуть переміщатися у двох площинах – горизонтально й вертикально. Так, при захисті периметра прямокутної форми, можна використовувати чотири стаціонарні відеокамери, або дві камери на поворотних механізмах. У першому випадку, буде проглядатися весь периметр відеоспостереження одночасно, у другому – одночасно буде проглядатися тільки одна сторона об'єкта, після повороту камер – друга.

Конструкція поворотного пристрою – це дві платформи, одна йз яких приводитися в рух маленькими двигунами, установленими на другій платформі, що залишається нерухомої. У рух поворотні механізми відеокамер приводяться дистанційно за допомогою пультів. Поворотні пристрої, використовувані для охорони периметра, повинні нормально функціонувати в різних погодних умовах, тому радимо вибирати ті моделі, у яких діапазон робочих температур варіюється від -40 до +60 С. У стандартній комплектації для вулиці, камери оснащуються захисним кожухом на поворотний механізм і трансфокатором на об'єктиві. Також поворотні пристрої відрізняються кількістю скануючих площин (горизонтальним і вертикальна, або одним єдина – вертикальна) і максимальним кутом повороту камери. Так, у горизонтальній площині зона огляду може становити максимально 360 градусів, у вертикальній площині – 120 градусів. Крім того, поворотні механізми характеризуються різною швидкістю обертання камери. Швидкість повороту більшості моделей становить 5-7 град/сек. При проектуванні систем відеоспостереження, насамперед, потрібно визначити мети установки периметральної охорони, і визначитися, що саме повинен бачити оператор на моніторі. Цілком достатнім може виявитися загальний огляд, при якому можливо встановити сам факт проникнення на охоронюваний об'єкт. Однак загальний огляд не надає можливості визначити особистість правопорушника, можна лише із упевненістю говорити, що на територію проникнула стороння людина, а не, приміром, тварина. При докладному огляді на зображенні з камер можна пізнати людини, і згодом ідентифікувати його особистість. Від можливостей огляду в цілому залежить вартість системи відеоспостереження. Після визначення цілей установки системи відеоспостереження, варто визначити безпосередній периметр відеоспостереження. Як варіант, можна встановити камери уздовж огородження або встановити камери з поворотними механізмами й трансфокаторами, на високому спорудженні усередині охоронюваної території. Рішення питання залежить від того, яким образом буде здійснюватися відеоспостереження: уздовж або поперек периметра.

Варіанти охорони периметра

Перший варіант передбачає використання відео-детекторів руху, у другому варіанті передбачена додаткова апаратура, для визначення можливої погрози й налаштування огляду камер.

Перший варіант (установлення камер відеоспостереження уздовж огородження) – економія на поворотних механізмах. Крім того, ці камери не мають потреби в керуванні, без особливих проблем можна вести постійний відеозапис всієї площі охоронюваного об'єкта й контролювати невелику смугу відчуження навколо периметра. Така система охоронного телебачення малоуразлива, при поломці однієї камери, не проглядатися буде лише не велика ділянка периметра, не залежить від кількості дерев і будинків на охоронюваній території. При такому варіанті немає необхідності ставити зовнішні датчики тривоги. Недоліки системи – велика кількість камер, відповідно велика кількість необхідного кабелю, низька частота опитування камер, складність монтажу й обслуговування системи відеоспостереження.

Другий варіант, що передбачає установку невеликої кількості відеокамер, значно спрощується монтаж системи відеоспостереження і її сервісне обслуговування. Подібна система організації охорони території набагато швидше адаптується до периметрів складної форми. До того ж вона менш піддана впливам зовнішніх факторів, тому що розташовується усередині охоронюваного об'єкта, дозволяє більш якісно контролювати територію й далекі підступи до огородження. Зрозуміло, таке рішення зажадає установки додаткового устаткування (зовнішні датчики, тривожні інтерфейси). Керування такою системою вимагає певних навичок, але рішення всіх цих питань візьмуть на себе фахівці нашої компанії. Варто врахувати, що наявність дерев і споруджень усередині охоронюваного об'єкта ускладнює роботу всієї системи CCTV.

Охорона периметра об'єкта, що складає з охоронної сигналізація й відеоспостереження, більш успішно справляється з поставленим завданням. Установлені променеві охоронні датчики можуть перекрити досить протяжна ділянка огородження, і при спрацювання охороною сигналізації залучити до даної області увага оператора. Особливо ефективна система, де зроблена інтеграція ОПС і відеоспостереження.

Вибір і проектування необхідної, конкретно для ваших цілей, системи відеоспостереження – справа професіоналів. Наша компанія допоможе вам підібрати саме той варіант відеоспостереження периметра, що буде відповідати вашим вимогам. Ми не тільки якісно встановимо все необхідне устаткування, навчимо навичкам роботи, але й здійснимо постійну підтримку й періодичне обслуговування будь-якою охороною системи.

Для захисту периметра тої або іншої території потрібно щось більше, ніж високий забір з колючим дротом нагорі. Успішно протистояти погрозам можна тільки в тому випадку, коли є безліч рівнів захисту, оснащених надійними системами безпеки. Однак чимало підприємств як і раніше зазнають труднощів з розробкою й впровадженням такого комплексного рішення.

Сьогодні організації гостріше, ніж коли-або раніше, відчувають важливість блокування дій зловмисників, перш ніж ті встигнуть завдати шкоди майну й нашкодити клієнтам або співробітникам. Експерти IFSEC Global, посилаючись на дані провідного центра дослідження ринків Research and Markets, прогнозують, що до 2020 року обсяг продажів на глобальному ринку засобів безпеки для захисту периметра досягне 21 млрд доларів.

Незважаючи на це, існує одна фундаментальна проблема: багато хто як і раніше зазнають труднощів з розробкою й впровадженням всеосяжного плану захисту периметра. От шість питань, які варто задати собі при підготовці такого проекту.

1. Що розуміється під периметром?

Периметр – це будь-яка границя, що відокремлює одну область від іншої. Ціль захисту полягає в забезпеченні безпеки уразливих місць, що перебувають усередині його, і структур.

При розробці плану захисту периметра в першу чергу треба оцінити його довжину. Як правило, для довгих периметрів буде потрібно більше огороджень і засобів безпеки.

Візьмемо, приміром, міжнародний аеропорт. За повідомленням, тільки за останні десять років на охоронювану територію площею 137 км2, навколо якої вибудуваний забір довжиною 48 км, проникнули вісім чоловік. Інші великі аеропорти мають огородження аналогічної або навіть більшої довжини.

А тепер представте, що вам потрібно розробити й реалізувати план, у якому рівна увага приділяється кожному квадратному метру усередині багатокілометрового периметра. Домогтися цього нелегко, але можна виконати наступні дії:

Визначите всі входи й виходи. Як правило, зловмисники проникають через зазначені зони, тому що зробити це легше всього.

Вивчите фізичний периметр: він може складатися зі стін, заборів, якоїсь іншої інфраструктури й природних перешкод, таких як живоплоти з кущів і дерев.

Оцініте наслідки проникнення. Потрібно чи подавати сигнал тривоги, як тільки порушник почне перелазити через забір, або важливіше визначити напрямок його руху й пройдена відстань? Важливість охоронюваної власності можна описати концентричними колами: у центрі перебуває сама коштовна його частина, а на границі – найменш значима.

2. Наскільки актуальна використовувана технологія?

Доцільність застосування найсучасніших рішень безпеки обґрунтовується цілим рядом причин.

Дотримання вимог регуляторів. Організації, що працюють у сфері охорони здоров'я, а також підприємства, що виконують замовлення урядових структур, змушені підтримувати свої рішення в області безпеки в актуальному стані, для того щоб уникнути штрафів.

Наприклад, у США медичні організації повинні дотримувати вимог Закону про звітність і безпеку медичного страхування (HIPAA) і інші приписання штатів і федеральних структур. У числі іншого їм необхідно регулярно обновляти свої рішення безпеки, що дозволяє гарантувати кращий захист фізичної інфраструктури й даних.

Підвищення ефективності продуктів. Технології, що дозволяють розпізнавати рух на відео, постійно вдосконалюються, і на зміну аналізу пікселів приходять інтелектуальне розпізнавання об'єктів і видача попереджень із урахуванням розмірів порушника й швидкості його руху. Обчислювальна потужність IP-пристроїв на границях мережі росте, і з їхньою допомогою можна виконувати більше складний аналіз, що дозволяє зменшити число помилкових спрацьовувань. Це обіцяє відразу кілька переваг. Переміщення обчислень на границю мережі означає, що обчислювальна потужність, що звільнилася, центрального сервера може бути спрямована на рішення інших завдань. Найчастіше це дає можливість знизити витрати на устаткування й скоротити ресурси, виділювані на виконання тих же самих операцій.

Крім того, використання розподілених кінцевих пристроїв для виконання різних завдань дозволяє ізолювати системні збої. Представте, що відбудеться при відмові центрального сервера, що виконує складний аналіз. Аналітика буде недоступна для всіх підключених пристроїв. Завдяки розподіленій системі її не можна буде одержати тільки від тих пристроїв, на яких безпосередньо відбуваються збої.

Захист від кібератак. Підключені до мережі пристрої Інтернету речей (IP-камери й інше устаткування) потенційно уразливі. У новому звіті Deloitte говориться, що число й масштаби розподілених атак, націлених на відмову в обслуговуванні (DDoS-атаки), також ростуть. Це може привести до виводу з ладу систем безпеки або як мінімум до блокування доступу до відеоматеріалів. Установка останніх відновлень допомагає краще захистити компанії від подібних погроз.

Перш ніж обновляти рішення, уточните, як інші методи захисту й виявлення (електричні огородження й контури заземлення, пасивне інфрачервоне устаткування, радари, подвійні датчики, тепловізійні камери, гучномовці й освітлення) уписуються в загальний

план захисту периметра. З'ясуєте, чи відкрита використовувана технологія для інтеграції або ж вона доступна через загальну платформу у вигляді окремого блоку.

3. Чи впливають на точність виявлення клімат і особливості навколишнього середовища?

Клімат і особливості навколишнього середовища здатні зробити серйозний вплив на устаткування систем безпеки і якість розпізнавання погроз. Коли освітлення занадто яскраве, об'єктив захоплює промені висхідного або західного сонця або зйомка проводиться вночі, аналогові камери навряд чи зуміють видати чітке зображення. Для таких ситуацій краще підходять IP-камери із широким динамічним діапазоном або тепловізійні технології.

Освітлення – не єдина потенційна проблема для фахівців з безпеки. При сильному вітрі й різному ступені вібрації виникає ефект тремтіння, позбутися від якого допоможуть електронні стабілізатори зображення.

В екстремальних умовах операторам потрібно враховувати не тільки функціональні можливості рішень безпеки. Необхідно взяти до уваги й інших факторів, що впливають на якість відео:

Вологість. Конденсат, що утвориться усередині об'єктива, розмиває зображення й руйнує електронні компоненти. У камер, що піддаються змінному тиску повітря й впливу дощу, може порушитися ізоляція, і волога проникне усередину. Для запобігання збоїв камери оснащуються внутрішніми вентиляторами й системою швидкого сушіння.

Умови навколишнього середовища. Через високий зміст солі в повітрі устаткування, установлене на морському узбережжі, піддається корозії. Те ж саме відбувається в цехах підприємств, де виробляються харчові продукти, медичні компоненти, що чистять засоби й застосовуються агресивні хімічні сполуки. У такому середовищі варто використовувати камери для зовнішнього спостереження, виготовлені з нержавіючої сталі й полікарбонату й які володіють стійкістю до впливу морської води й реагентів, що чистять.

Температура. Коли устаткування експлуатується при екстремально низьких температурах, його нормальне функціонування порушується. Якщо не підтримуються технологія швидкого сушіння й температурний контроль, то об'єктив покривається льодом, що приводить до размиттю зображення. А при порушеннях у роботі системи електроживлення камера й зовсім перестає працювати.

Монтаж. Не всі поверхні однакові. Камери, установлені на пористі або стінах, що володіють високою теплопровідністю, піддаються додатковому впливу вологи. Заздалегідь вивчивши всі особливості розміщення устаткування, ви зможете краще захистити його від руйнівного впливу навколишнього середовища й сильних перепадів температури.

4. Хто і як приймає сигнали тривоги?

Для постійного контролю за всім периметром часто використовується технологія віддаленого IP-відеоспостереження. Установлені в декількох місцях камери дозволяють співробітникам служби безпеки постійно бути в курсі подій, коли вони стежать за тим, що відображається на моніторах, роблять обхід об'єкта й віддалено спостерігають за, що відбувається з допомогою мобільних пристроїв.

Системи захисту периметра аналізують ситуації й повідомляють персонал тільки при виникненні реальної погрози. Будучи врятовані від необхідності стежити за суб'єктами й подіями, що не представляють якої-небудь небезпеки, співробітники здатні краще оцінити природу ризику й відреагувати відповідним чином.

Такий рівень безпеки допомагає підприємствам вирішити відразу три завдання:

Зменшення числа штрафів. В 2018 році поліція й пожежні служби Канзаса зареєстрували просто неймовірну кількість викликів у місті Уичито. Усього надійшло 18 461 повідомлення, і тільки 659 з них інформували про реальну погрозу. При цьому перше помилкове повідомлення не передбачало ніякого покарання, а от наступні загрожували штрафом у розмірі від 40 до 350 доларів. Сума максимального штрафу склала 750 доларів, у цілому в міську скарбницю надійшло 700 тис. доларів.

Таким чином, фіктивні тривоги обходяться підприємствам у сотні, а те й у тисячі доларів. Кращі рішення для моніторингу дозволяють зменшити число помилкових спрацьовувань за рахунок ідентифікації тільки щирих погроз.

Мінімізація збитку й збитків. Оперативна реакція на порушення периметра допомагає значно скоротити збитки, у тому числі від збитку, нанесеного майну. Але, як уже говорилося раніше, у масштабі країни кількість фіктивних тривог перевищує всі розумні межі. Візьмемо, приміром, Остін. В 2018 році міська поліція щодня виїжджала на термінові виклики в середньому 80 разів. При цьому, за свідченням myStatesman, дев'ять сигналів з десяти виявилися помилковими.

У деяких містах спецслужби відмовилися виїжджати по тривозі в ті місця, звідки надходило найбільшу кількість помилкових сигналів. Об'єкти, де відсутні належні засоби й протоколи захисту периметра, піддаються підвищеному ризику несанкціонованого проникнення й завдання матеріальних збитків.

Зниження числа збоїв у роботі підприємств, викликаних помилковими сигналами тривоги. Особливо важливе значення це має в аеропортах, де будь-яке порушення периметра може привести до затримок рейсів, що чревате багатотисячними збитками від загублених доходів і накладених штрафів.

Згадаємо випадок, що відбувся в міжнародному аеропорті Філадельфії в березні 2012 року. За повідомленням New York Daily News, чоловік, що управляв позашляховиком, проїхав через ворота й виїхав на злітну смугу, куди саме збирався приземлитися літак, на борті якого перебували 43 чоловік. У результаті була затримана посадка не тільки цього рейса, але й ще 75 літаків, що пішли на додаткове коло на вимогу диспетчера. Крім того, 80 літаків, що готувалися до зльоту, протягом півгодини залишалися на своїх місцях.

Системи безпеки, оснащені засобами дистанційного оповіщення, допомагають оперативно попереджати персонал аеропорту, сприяючи блокуванню таких проникнень ще до несанкціонованого перетинання границі периметра або, у крайньому випадку, відразу після його виявлення.

5. Як визначити, що стало причиною тривоги?

Сучасні засоби захисту периметра спрощують виявлення причини тривоги.

Наприклад, у тепловізійних камер, наділених засобами інтелектуального відеоаналізу, не тільки набагато менше, у порівнянні з оптичними, помилкових спрацьовувань, але вони краще підходять для роботи в умовах дощу, снігу й туману. Деякі такі пристрої оснащуються електронними стабілізаторами зображень, які роблять їх більше стійкими при впливі вітру.

Звичайно, можливості тепловізійних камер обмежені. Але якщо вони доповнюються засобами віддаленого моніторингу, співробітники служби безпеки оперативно одержать повідомлення про потенційно небезпечну ситуацію й зможуть перевірити наявність погрози особисто або за допомогою візуальних камер.

В умовах слабкої освітленості або при дуже яскравому світлі ідентифікація порушників утруднена. Як приклад можна привести ситуацію, коли камера спрямована на автомобіль із потужними фарами. Рішення з підтримкою широкого динамічного діапазону дозволяють міняти структуру сцени таким чином, щоб при більших перепадах освітлення об'єкти були видні краще.

Інша ідея полягає у використанні камер, оснащених інфрачервоним підсвічуванням з довжиною хвилі 950 нм і що дозволяють розглянути затемнені місця. Хоча інфрачервоні прилади не відображають природні кольори, вони відмінно підходять для схованого спостереження, оскільки інфрачервоне випромінювання невидимо для людського ока.

Однак, як і в будь-якого іншого рішення, в інфрачервоних камер є слабкі місця:

1. Вони менш ефективні в сиру погоду, тому що точлі води відбивають і переломлюють світло, погіршуючи якість зображення.

2. Як правило, інфрачервоні камери ефективно реєструють відбиття випромінювання від безлічі об'єктів, але, якщо якісь об'єкти занадто темні або, навпаки, яскраві, є ймовірність того, що інфрачервоні промені не будуть відбиватися належним чином.

3. Злочинці можуть побачити тьмяне червоне світіння камер з малою довжиною хвилі й спробувати зламати камеру або її кріплення.

Варто відзначити, що простої додавання джерел освітлення в темних зонах допомагає краще розпізнавати порушників, але в довгостроковій перспективі може привести до збільшення загальних витрат на забезпечення безпеки периметра.

6. Яка дальність виявлення?

Персонал служби безпеки повинен насамперед усунути так звані сліпі зони по периметрі. Якщо виявлення погрози на відстані 3 і 300 метрів однаково важливо, то ознайомлення лише зі специфікаціями системи недостатньо – необхідно оцінити ситуацію в цілому.

Впровадження будь-якого продукту може завершитися невдачею, якщо його розгортання здійснюється неналежним чином. Практичні навички використання технологій захисту периметра й знання обмежень на дальність розпізнавання допоможуть персоналу одержати більше високу віддачу від впровадження рішень безпеки.

Приміром, тепловізійна камера з дальністю дії 300 м відмінно підходить для установки уздовж лінії забору. Але що, якщо операторові потрібно знати, хто порушник – людина або тварина? Ці параметри накладають додаткові обмеження й звужують діапазон залежно від конкретних потреб, умов навколишнього середовища й особливостей території.

Розробка структурної схеми

Відеоспостереження на периметрі покликано ефективно вирішувати завдання виявлення об'єктів на підході до периметра, а так само у внутрішньої сторони забору. Пропонована система дозволяє операторові здійснювати моніторинг протяжного периметра й записувати все що відбувається на диск для наступного аналізу записаного архіву.

Опис системи

Аналогове відеоспостереження надійно й простої в експлуатації. Вам не буде потрібно наймати фахівця з мереж, що б обслуговувати систему. Будь-який рядовий технік розбереться з будь-яким завданням маючи в руках звичайний тестер.

Центром системи є відеосервер з розробленим у даній роботі ПЗ. Програмне забезпечення має потужні аналітичні функції, які попередять оператора у випадку пропажі сигналу з камери, засвітлення, розфокусування, закриття й т.п. Система сама себе охороняє.

Обробка зображення для виявлення потенційно небезпечних цілей знизить навантаження з оператора й не дозволить пропустити проникнення на територію в ситуації, коли оператор відволікся від екрана монітора. У той же час спеціальний алгоритм відстеження наявності оператора на пості дозволяє контролювати роботу охорони й одержувати повідомлення про відсутність оператора понад заданий час.

Відеосервер установлюється в спеціалізованому приміщенні (серверної), а на пості охорони встановлюється ПЕОМ і два монітори для спостереження. Це дозволяє убезпечити системи від випадкового або навмисного (по змові зі зловмисниками) псування сервера або його вимикання. Відеоархів із глибиною зберігання два тижні дозволить швидко розібратися при виникненні будь-якого інциденту.

Відеокамери Panasonic – визнаного лідера в CCTV відеоспостереженні, забезпечують виняткова якість зображення й передачу кольору. Для роботи в нічний час буде потрібно додаткове освітлення. Відеокамери встановлюються в термокожухах, що забезпечує функціонування системи від -52 град. Для в'їзної групи пропонується використання топової версії камери із широким динамічним діапазоном, що забезпечить відмінну якість при будь-якому висвітленні й ефективно бореться із засвітленням від зустрічний фар.

Спеціальні кабелі стійкі до зовнішніх впливів прокладаються в підготовлених траншеях у гладких ПНД трубах. Всі роботи виконуються "під ключ". Відеокамери розміщаються на стовпах замовника.

Робота системи

На сервер системи надходить інформація з периметральних відеокамер в аналоговому виді. Плати відеовводу оцифровують дані й передають у ПЗ для обробки. Дані

обробляються, записуються на HDD і передаються на ПЕОМ установленому на пості охорони. Оператор може перемикати види з камерами на двох моніторах за своїм розсудом у рамах своїх прав, а так само передивлятися архів. Доступ до відеозображення можливий на віддалених клієнтах, у тому числі через розроблений мобільний застосунок.

Рисунок 1 – Структурна схема системи

Для захисту в ситуації короткочасних відключень електрики ми передбачили UPS. Для захисту камер і дорогого серверного устаткування використовується комутаційна панель із функцією грозозахисту.

Оператор у режимі реального часу відслідковує ситуацію на периметрі, приймає оперативні рішення, аналізує архів і проводить розслідування з використанням записаного зображення з відеокамер.

Модифікації й додаткові можливості

Для спостереження в темний час доби при повній відсутності зовнішніх джерел світла необхідно дооснастити систему інфрачервоними прожекторами, або прожекторами на основі світлодіодов. Можлива організація автоматичного включення прожекторів при наявності руху й використання спрацювання датчика руху для автоматичного інформування оператора про підозрілу активність на периметрі.

Необхідно встановити додатково відеокамеру й мікрофон на робочому місці оператора системи для контролю за діями охорони.

Економічний ефект

Для будь-якого власника важлива безпека його об'єкта, людей проживаючих або працюючих на довіреній йому території, матеріальні цінності й погрози об'єктам життєзабезпечення. Убезпечити себе від ризиків покликана система безпеки. Відеоспостереження підвищує привабливість об'єкта й вартість послуг надаваних власником. Якісна система відеоспостереження збільшує цей ефект багаторазово.

1. Устаткування

Відеокамера WV-CP304E

Професійна аналогова відеокамера стандартного дизайну для установки усередині приміщень і на вулиці в термокожусі, день/ніч, 1/3", АРД, висока чутливість, 650 ТВЛ, цифрова обробка зображення, об'єктив окремо, 12/24 В, виробник Panasonic.

Об'єктив 13VG2811ASIR

Професійний об'єктив Tamron зі змінною фокусною відстанню (варіофокальний), для матриці 1/3", для камер з АРД, фокусна відстань 2, 8-11,0 мм, кут огляду 97 – 26 град

Термокожух для відеокамери SVS26

Термокожух для розміщення корпусних відеокамер, живлення 24 В змінної напруги, споживання з камерою до 17 ВА, кронштейн у комплекті, температура -52...40 град, виробник WIZEBOX

Відеокамера WV-CW314LE

Професійна аналогова відеокамера для установки на вулиці, краща камера в сегменті вуличних 3 в 1, день/ніч ІЧ-фільтр, 1/3", АРД, висока чутливість, 650 ТВЛ, цифрова обробка

зображення, широкий динамічний діапазон WDR, убудований об'єктив з регулюванням кута огляду 100-27 град, фокусна відстань 5-40 мм, 24AC/12 В, виробник Panasonic

Джерело живлення SKAT-VN.24/27AC

Блок живлення для камер відеоспостереження 24 В AC змінного струму. Не безперебійний. До 5А

Відеосервер 25-10000-19"-4CIF

PC-based відеосервер на 16 камер. Архів на 14 днів по детектування в середньому 8 ч/доба постійного запису. OS Windows 7. Виконання 19". Гарантія 2 роки.

Панель VIDEOMAX-УЗВ-01

Комутаційна панель 19", 1U, із захистом відеосигналу, 16BNC входів, 2 виходи DB25.

ПЕОМ для віддаленого робочого місця оператора або адміністратора системи VIDEOMAX-URM-INTLT(U1)-2M-ID2

ПЕОМ для віддаленого робочого місця оператора або адміністратора системи, кількість моніторів, що підключаються – 2, конфігурація ID2, робота в цілодобовому режимі 24/7, корпус minitower, настільне виконання, оригінальний захист ОС від втручання оператора, у комплекті з розробленим у даній роботі ЗД.

Монітор AOC E2070SWN 19.5

Монітор 19,5, LED широкоформатний, 1600x900, LED-підсвічування, 200 кд/м2, 600:1, 5 мс, 90/60°°, VGA.

Джерело безперебійного живлення SMART UPS 1500VA LCD RM 2U (SMT1500RMI2U)

Професійне джерело безперебійного живлення серверного устаткування (UPS), потужність 1500VA (1000Вт), для установки в стійку 19", висота 2U, синусоїдальний сигнал, LCD дисплей для контролю режимів роботи.

2. Видаткові матеріали

Коаксіальний кабель RG6 с ПНД оболонкою, силовий кабель ВВГ-НГ для живлення камер, гофровані й гладкі ПНД труби, комутаційні коробки IP65, кріпильні й ізоляційні матеріали.

3. Роботи

- Монтажні роботи.
- Пусконалагоджувальні роботи.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів комплексного засобу відеонагляду для захисту периметру підприємства. В межах України в недостатній мірі представлені вітчизняні розробки в цій області. У роботі наведені теоретичне узагальнення й рішення наукового завдання дослідження методів комплексного засобу відеонагляду для захисту периметру підприємства. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем комплексного засобу відеонагляду для захисту периметру підприємства; Досліджена система комплексного засобу відеонагляду для захисту периметру підприємства; На основі отриманих результатів досліджень створена програмна реалізація системи комплексного засобу відеонагляду для захисту периметру підприємства. Розроблені під час виконання роботи алгоритми дозволяють успішно вирішувати завдання комплексного засобу відеонагляду для захисту периметру 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.

Список літератури

1. Савич Б.О. Дослідження та програмна реалізація системи комплексного засобу відеонагляду для захисту периметру підприємства // Збірник праць молодих науковців ЦНТУ. – Вип. 11. – Кропивницький: ЦНТУ, 2021.

2. 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.
3. 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.
4. 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.
5. 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.
6. 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.
7. 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.
8. 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.
9. 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.
10. 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.

УДК 004

А. Сароян, магістр гр. КН-19МЗ
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ АНАЛІЗУ ДОДАТКІВ РІВНЯ L7 У FIREWALL

У статті розроблено програмне забезпечення, яке призначено для системи аналізу додатків рівня L7 у Firewall. Метою розробки є дослідження та програмна реалізація системи аналізу додатків рівня L7 у Firewall. Об'єктом дослідження є процес аналізу додатків рівня L7 у Firewall. Предметом дослідження є методи аналізу додатків рівня L7 у Firewall. Методи дослідження базуються на методах захисту інформації, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи аналізу додатків рівня L7 у 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 доступу, WEB ресурси

Постановка проблеми. Skype, TOR, Ultrasurf, TCP-over-DNS і ще кілька сотень застосунків і тунелів спокійно проходять крізь statefull inspection firewall і HTTP проксі. Багато засобів захисту відкривають з'єднання, але не перевіряють, що ходить усередині них. Пропоную розібратися, як контрольовано дозволяти з'єднання застосунків у новому поколінні firewall, де правила пишуться по іменах застосунків, що відповідає 7 рівню моделі OSI ISO. Такі міжмережеві екрани мають назву Next Generation Firewall –

міжмережевий екран нового покоління або просто NGFW.

Адміністраторові міжмережевого екрана потрібно не тільки дозволити з'єднання, а ще гарантувати, що усередині дозволеного з'єднання ходить те, що ви хотіли, включаючи перевірки переданих файлів. Це називається безпечний дозвіл застосунків.

Існує кілька важливих відмінностей у роботі із трафіком, які розумієш лише коли переходиш на реальне використання правил, де критерієм є застосунок 7 рівня моделі ISO OSI:

– IT адміністратор бачить, що NGFW зручніше у візуалізації мережевого трафіку й показує вміст поля даних пакетів по кожному користувачі й сервісу: який застосунок працюють і які файли передає.

– IT безпека бачить, що NGFW забезпечують безпечний дозвіл застосунків, оскільки більше глибокий аналіз даних у пакеті дозволяє побачити віруси, підключити відправлення невідомих файлів у пісочницю, перевірити тип файлу, ключові слова для DLP, перевірити категорію URL, перевірити що йде усередині SSL і SSH, зрівняти із уже відомими усьому світу індикаторами компрометації, включити DNS фільтр і інші сучасні техніки.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи аналізу додатків рівня L7 у Firewall.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи аналізу додатків рівня L7 у Firewall.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем аналізу додатків рівня L7 у Firewall.
– Дослідження системи аналізу додатків рівня L7 у Firewall.
– Програмна реалізація системи аналізу додатків рівня L7 у Firewall.

Об'єктом дослідження є процес аналізу додатків рівня L7 у Firewall.

Предметом дослідження є методи аналізу додатків рівня L7 у Firewall.

Методи дослідження базуються на методах захисту інформації, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Семирівнева модель OSI/ISO – це модель взаємодії між мережевими пристроями, що говорить, що існує 7 рівнів абстракції взаємодії: перший – фізичний, потім канальний, мережевий, четвертий – транспортні, сесійний, подання й сьомий рівень – застосунків.

Кожний мережевий пристрій працює на своєму рівні абстракції: веб сервер і браузер – на рівні застосунків, маршрутизатори – спілкуються один з одним на канальному й мережевому рівні, коли передають один одному фрейми й пакети.

Міжмережеві екрани теж є мережевими пристроями, також можуть бути світчами й роутерами й навіть бути «віртуальним кабелем» з погляду мережевої топології, але на них лягає додаткове навантаження: вони повинні аналізувати вміст пакетів і от глибина аналізу мережевих пакетів може відрізнятися. Чи аналізують вони 4 або 7 рівень, у цьому є важливу відмінність.

Firewall

Міжмережевий екран (MME), Firewall, NetworkFirewall – це мережевий пристрій, що ділить мережу на сегменти з різними політиками безпеки й контролюють ці політики. Наприклад, сегмент Інтернет – там можна всі що завгодно. І сегмент вашого ЦОД – там можна працювати тільки виділеному списку співробітників по дозволених застосунках. Усередині одного хоста VMware може бути кілька віртуальних мереж з віртуальними машинами й різними політиками доступу до них.

Політика безпеки firewall містить правила, які пускає в хід програмний код пристрою, аналізуючи кожний фрейм і пакет що прийшов і виходить із firewall. У правилах firewall задаються критерії перевірки (кваліфікатори), по яких приймається рішення

пропускати або блокувати трафік. Прикладами кваліфікаторів у правилах є: адреса, порт, застосунок, користувач, зона. Міжмережевий екран послідовно, правило за правилом, зверху внизу за списком переглядає критерії і якщо вхідний трафік відповідає всім критеріям правила, (логічна операція «И» між критеріями) те застосовується зазначена дія: заблокувати або пропустити. Дія виконується як для першого пакета, так і для всіх наступних пакетів одного TCP/IP з'єднання.

Існують різні типи й реалізації firewall. Ми розглянемо класифікацію по ступені використовуваної глибини аналізу трафіку: L3, L4 і L7.

L3 Firewall

L3 firewall – це міжмережевий екран, що пропускає через себе IP трафік мережі й аналізує тільки заголовки IP протоколу, тобто адресу звідки й куди йде трафік. Такі міжмережеві екрани називають пакетний фільтр. Правила мають назва «список доступу» або access-list і цей функціонал на сьогодні працює практично в будь-якому маршрутизаторі й операційній системі. Такий аналіз не вимагає серйозного навантаження на процесори й пам'ять firewall.

L4 Firewall

L4 firewall – це міжмережевий екран, що пропускає через себе IP трафік мережі й перевіряє заголовки протоколів 4 рівні: TCP, UDP, ICMP, тобто основними критеріями перевірки для пропуску трафіку є IP адреси й порти TCP/UDP.

Також в L4 firewall з'являється поняття stateful inspection, коли кожне минаюче з'єднання запам'ятовується й контролюється стан з'єднання для того, щоб дозволяти необхідні відповідні з'єднання. Тобто з'являється поняття ініціатора з'єднання, що логічно в мережах, побудованих на клієнт-серверної технології. Такий міжмережевий екран витрачає пам'ять на зберігання даних про кожне з'єднання, тобто з'являється обмеження на максимальну кількість збережених одночасних сесій у пам'яті. В L4 firewall уже не потрібно писати відповідне правило для зворотного з'єднання, як це потрібно в L3 firewall, тому що на основі стану з'єднання, міжмережевий екран автоматично дозволяє зворотні з'єднання. Тобто L4 firewall зручніше, ніж пакетний фільтр.

Сучасні L4 firewall зберігають стан не тільки TCP, UDP і ICMP, але й відслідковують взаємодія деяких L7 застосунків. Наприклад, стан FTP, HTTP, SIP, і інші застосунки, що вже залежить від конкретної реалізації firewall. Потрібно задавати виробникові L4 firewall питання: які конкретно застосунки підтримує їхній движок stateful inspection firewall.

L7 Firewall

L7firewall – це міжмережевий екран, що пропускає через себе IP трафік мережі й перевіряє й заголовки 4 рівні й сегмент даних кожного IP пакета, тобто розуміє L7 трафік рівня застосунків, аж до того які файли передаються й у якому напрямку. Оскільки аналізується більше даних, те й критеріїв перевірки в правилах L7 firewall більше: ім'я користувача, застосунок, URL категорія, стан софта на комп'ютері користувача. Навантаження на L7 firewall набагато вище, оскільки його процесор повинен постійно аналізувати мегабайтів даних, які передає застосунок, у той час як L4 firewall перевіряє тільки трохи байт заголовка з адресами джерела й одержувача й портами. Розмір буфера для зберігання стану кожного застосунку потрібно набагато більше, оскільки даних на L7 передається більше, ніж просто в заголовку TCP/IP. Через виросли розмір буфера при використанні аналізу застосунків, кількість одночасно збережених у пам'яті сесій в L7 firewall менше L4 firewall при тім же обсязі пам'яті. Оскільки L7 firewall бачить по контенту що за застосунок йде мережею, то номер порту не несе особливого змісту й правила можна писати за іменем застосунку L7. Крім того сучасні застосунки генерують багато з'єднань і всіх цих з'єднань є частиною одного застосунку. Цей вид firewall дозволяє повернути контроль за сучасними динамічними застосунками, що працюють по будь-якому порту, наприклад, teamviewer, bittorent, tor, про які L4 firewall нічого не знає. Тобто L7 firewall у сучасних реаліях потрібний, якщо в мережі потрібна безпека.

Якщо після прочитання даної статті ви продовжите використовувати L4 firewall те, це значить, що на безпеку вам наплювати.

UTM

UTM – це мережевий пристрій, усередині якого встановлено кілька різних компонентів захисту, які послідовно аналізують минаючий через пристрій трафік. Ядром UTM є L4 firewall, система запобігання атак (IPS), антивірус, аналіз категорій URL в HTTP і HTTPS. Часто UTM ще реалізують функції VPN шлюзу. Керування всіма цими компонентами як правило здійснюється з декількох різних систем керування. Трафік усередині UTM послідовно проходить через модулі фільтрації й на виході залишається чистий трафік, що дозволений політиками безпеки кожного модуля. UTM може бути використаний як платформа для інших функцій: захист від вірусів, IPS, DDoS, QoS, DLP, DNS фільтр, бази індикаторів компрометації Threat Intelligence, захист від фішингу й так далі (залежить від виробника).

Притча про людину, що замовив сім шапочок з однієї шкіри, написана в тому числі для покупців UTM: чим більше функцій ви захочете після покупки включити, тим більше навантаження будуть нести процесора UTM для аналізу того самого обсягу трафіку. Більше функцій – менше швидкість пристрою.

Ідея UTM – навантажити один процесор як можна більшою кількістю функцій стала еволюційним тупиком, тому що число функцій рослася й витримувати все це навантаження процесори не могли. Сьогодні, незважаючи на заявлені гарні функції, ніхто не включає в UTM весь функціонал, щоб виключити затримки трафіку.

Ціль UTM: реалізувати на одному сервері якнайбільше функцій, щоб здешевити пристрій для користувача.

Зараз виробники UTM стали ставити движки аналізу застосунків 7 рівня, щоб говорити, що вони NGFW, чим спантеличують споживача. Однак це легко розпізнати, якщо подивитися в політику безпеки: правила як і раніше базуються на критеріях перевірки полів L4. А для фільтрації L7 застосунків використовується окремий розділ налаштувань, тобто застосунок L7 не є кваліфікатором, як повинне бути в L7 firewall. Розпізнавати застосунок L7 і використовувати застосунок L7 як критерій політики безпеки – це «дві більші різниці».

NGFW

NGFW – це мережевий пристрій, усередині якого реалізований L7 firewall. Оскільки кваліфікатором основним стає ім'я застосунку L7, те в такий спосіб правила пишуться по-іншому. В NGFW працює динамічне зіставлення IP адрес користувачі мережі, тому ім'я користувача теж стає кваліфікатором. NGFW містить у собі функції розшифрування SSL і SSH для розпізнавання застосунків і атак усередині них, IPS, антивірусу, URL фільтрації.

Через те, що NGFW виконує кілька функцій одночасно, іноді вважають NGFW підкласом пристроїв UTM. Відмінність у тім, що в NGFW функції безпеки контенту застосунків (IPS, антивірус, URL фільтрація) прискорені на спеціалізованих апаратних чипах: тобто IPS працює на своєму чипі, антивірус на своєму, розшифровані SSL на своєму й так далі. Поділ функцій по різних процесорах дає можливість запускати їх паралельно й не чекати, коли закінчить працювати попередня функція, як в UTM. Також NGFW містять єдиний програмний інтерфейс керування всіма функціями одночасно.

Ідея NGFW на відміну від UTM – реалізувати кожну функцію на окремому процесорі, які спеціалізований під необхідного функціонала. По тій же схемі колись пішли виробники комп'ютерів, які винесли функції математики й графіки в окремі математичні й графічні процесори. Тому в NGFW коштують окремі процесори під розпізнавання застосунків L7, під розшифровані SSL/SSH, під перевірку сигнатур антивірусу, перевірку сигнатур IPS і так далі. Це дозволяє включити всі функції одночасно, без деградації й затримки трафіку в пристрої на час перевірки.

Ціль пристрою NGFW: дати можливість безпечно працювати застосункам у компанії, тобто постійно перевіряти, що застосунку передають безпечний контент, для цього й реалізується паралельна робота движків захисту з одним потоком трафіку, щоб гарантувати

задану продуктивність при всіх включених функціях безпеки й мінімальну затримку трафіку.

Приклад політики L7 в Palo Alto Networks NGFW

Навіщо може знадобитися URL категорія, як кваліфікатор? Наприклад, ви можете частини співробітників дозволити все-таки відвідувати шкідливі сайти браузером, але заблокувати їм завантаження файлів.

Приклад політики Palo Alto Networks з використанням перевірок Host Information Profile і URL категорій. У цій політиці також задіяна перевірка наявності хостового захисту TRAPS у колонку HIP Profile, що не дасть зайти на сайт зі шкідливим кодом і експлойтами, без установленого захисту на комп'ютері. TRAPS це агент захисту від шкідливого коду й експлойтів.

Блокування завантаження файлів виробляються в налаштуваннях колонки Profile, де застосований профіль блокування передачі всіх файлів по будь-якому додатку. От так виглядає його налаштування.

Проксі-сервер

Проксі-сервер – це пристрій, що терминує на собі трафік якогось застосунку, перевіряє це трафік різними методиками й відправляє цей трафік далі. Найчастіше використовуються в мережах проксі сервера для протоколів HTTP і HTTPS. Оскільки UTM і NGFW аналізують потоки HTTP і HTTPS прозоро, не вимагаючи явно вказувати налаштування проксі-сервера в клієнтів, то HTTP проксі поступово зникають із компаній.

Омани про Stateful Inspection

Окремий параграф я повинен присвятити цьому знайомому кожному мережевому інженерові й безпечнику поняттю. Потрібно підкреслити й доповнити важливі речі, які часто упускають на курсах по міжмережевим екранах. Якщо ви вже вивчали основи stateful inspection, то швидше за все у вас є кілька оман.

Stateful inspection – це не тільки про стан з'єднання TCP, UDP або ICMP! Це ще й про стан інших більше складних протоколів і застосунків: FTP, SIP, RPC, SMTP, SMB і так далі!

Протокол FTP – це протокол рівня застосунків. І в ньому є команда PORT, що може призначати нове TCP підключення. Будь-який firewall, що позиціонує себе як stateful inspection firewall, повинен контролювати команди FTP і бачити команду PORT і дозволяти з'єднання на порт і адресу, що там запитаний. І це ще не все: firewall ще й повинен підмінювати параметри команди PORT і вставляти правильну адресу, якщо FTP сервер працює за NAT.

Тобто в будь-якому сучасному L4 firewall є компонент, що підглядає за L7 рівнем. І такий протокол не один: ще є HTTP, RPC, і інші... І такі аналізатори протоколів 7 рівня називаються Application Layer Gateway (ALG).

Самий «улюблений» одночасно в мережевиків і безпечників – це ALG для SIP, з яким багато хто, хто налаштовує SIP ALG на L4 firewall наїлися проблем, і часто закінчується його відключенням.

Тобто вже в L4 firewall є зачатки аналізу протоколів 7 рівня. L4 firewall відрізняються друг від друга кількістю реалізованих ALG. Коли ви порівнюєте звичайні L4 firewall, те справедливе питання системному інженерові виробника буде: скільки протоколів і застосунків підтримує ваш движок Stateful Inspection? Як правило ніхто не відповідає.

Виходить, що L7 firewall – це теж stateful inspection firewall, але який аналізує й зберігає статус ВСІХ застосунків, а не тільки вибірково, як L4 firewall.

Другу оману вносять самі виробники firewall. Візьміть будь-який datasheet, де виробник пише такий параметр, як «число одночасних сесій». Питання до виробника наступний: сесії яких саме протоколів і застосунків вимірялися й чи був включений хоча б stateful для TCP, не говорячи вже чи минулого перевірки для L7 рівня?

Ми знаємо, що в кожного протоколу або застосунку є стан, що пам'ятає firewall. І для зберігання цього стану потрібно виділити буфер у пам'яті пристрою. По суті, параметр «число одночасних сесій» означає скільки буферів для зберігання станів можна вмістити в

пам'яті пристрою. Потрібно розуміти, що для L4 firewall найчастіше вимірюють цей параметр для голого TCP або навіть UDP. Тобто для TCP потрібний буфер, у який уміщається тільки IP і порт з'єднання. Однак у тесті для L7 застосунків, наприклад, HTTP цей буфер буде значно більшого розміру, адже зберігати, наприклад, параметри запиту GET усередині HTTP потрібно більше пам'яті. А пам'ять не гумова. Відповідно, якщо виробник пише такий параметр як «число одночасних сесій», те він повинен писати:

– чи був це просто тест роботи в режимі світча/роутера, с виключеним stateful inspection,

– чи був це режим L4, де він запам'ятовував тільки заголовки TCP/IP,

– чи був якийсь застосунок L7 рівня взято для тесту.

Правильно L7 firewall вимірювати на числі одночасних сесій HTTP, на пакетах різної довжини: 64Кб, 44Кб, 16Кб, 1.5Кб. Зрозуміло, що якщо якимось виробником всі виміри були зроблені на UDP 1518 байт, те швидше за все у вашу мережу такий пристрій не підійде, оскільки змусити ваших користувачів посилати тільки UDP пакети довжиною 1518 байт – не вийде, а вуж тим більше змусити відповідати такими пакетами сервера HTTP. Потрібно сказати такому виробникові, що продуктивність L7 firewall потрібно виміряти хоча б на трафіку із протоколом HTTP. З відомих компаній, які проводять такі тести привселюдно: компанія NSS Labs.

Самі виробники firewall проводять тести на замовлення у своїх лабораторіях, яким можна замовити свій профіль трафіку, наприклад: 30% трафіку HTTPS, 10% трафіку SMB, 10% трафіку FTP і так далі.

Після перевірки на генераторі трафіку IXIA пристрою одного з виробників UTM:

– у режимі L4 firewall – 4 000 000 одночасних сесій,

– у режимі L7 firewall – 200 000 одночасних сесій.

Це показник того, що буферів для сесій L7 у пам'яті пристрою менше через їхній великий розмір.

І, до речі кажучи, також буде й із загальною продуктивністю пристрою: з виключеними перевірками контенту застосунків міжмережевий екран працює в 10 разів швидше, ніж із включеними. Використовувати тільки аналіз заголовків 4 рівні для прискорення пристрою можна, але безпеки вже ніякий.

Третій важливий момент – робота в кластері. Всі міжмережеві екрани повинні працювати в кластері, тому що якщо один міжмережевий екран перестає працювати, то його завдання «лягти грудьми» і заблокувати весь трафік – така теорія побудови захисту на базі міжмережевих екранів. Поки «зламаний» firewall блокує трафік, завдання по пропуску легітимного трафіку повинен взяти на себе сусідній firewall. А що ж буде із з'єднаннями, які йшли через перший? Швидше за все перший firewall передавав стан всіх з'єднань другому, але от чи передавав він сусідові тільки стан IP заголовків або повністю стан всіх застосунків L7 рівня: але ж там були якісь SSL з'єднання які були розшифровані й над ними трудився IPS і антивірус – вони збирали пакети в буфери, щоб перевіряти вміст. І отут виявляється теж L4 і L7 firewall відрізняються: передати стан L4 не те ж саме, що передати стан L7. Це теж важливо розуміти.

Існує ще одна омана, що L7 firewall можуть працювати в кластерах більше двох пристроїв – це невірно, оскільки обсяг переданих даних L7 росте експоненційно з кожним новим вузлом у кластері й обробка даних навіть двох сусідок перевищує витрати по обробці даних свого ж пристрою. Саме тому кластери більше двох пристроїв працюють тільки обмінюючись заголовками L4, і при перемиканні кластерів всі функції аналізу застосунків і захисти перезапускаються.

Тому потрібно грамотно порівнювати L4 і L7 firewall, також як коли ви порівнюєте чи підходить вам легковий автомобіль і танк на війні. L7 firewall для підвищення безпеки вашої мережі проробляє більше складну роботу, набагато більше роботи йде на його процесорах і йому потрібно більше пам'яті для зберігання стану ваших за стосунків. Все це потрібно робити для безпеки.

Розробка структурної схеми

L7 firewall перевіряє вміст поля даних, L4 firewall ні

Основна проблема, з якої ми боремося, що зараз програми відразу пишуть так, щоб вони обходили захист L4 firewall.

Якщо людина ставить Skype, то він не хоче дзвонити мережевому адміністратору й просити відкрити потрібний йому порт на firewall – він хоче, щоб, Skype відразу засвітився «зелененьким». Програмісти знають, що в мережі часто є HTTP проксі або відкритий порт 80 для роботи HTTP, порт 53 для роботи DNS, порт 123 для роботи NTP, а буває для співробітників зсередини назовні в Інтернет взагалі всі відкрито й відповідно цими дозволеними з'єднаннями можна користуватися.

У розроблювачів є термін User Experience – у клієнта після установки зайнявся Skype зелененьким = клієнт щасливий. А те, що Skype пройшов по з'єднанню, що було відкрито для роботи браузера TCP/80 або 443 – L4 firewall ігнорує, тому що він не дивиться у вміст пакетів, а лише в їхні заголовки.

Проблема L4firewall: port-hopping (тунелювання)

Тунелювання застосунків усередині дозволених з'єднань, які потрібні для інших цілей – це стандартна картина в сучасних мережах навіть для легітимних застосунків. Природно, хакери користуються тим же прийомом: вони створюють тунелі в дозволених з'єднаннях.

Приклад тунелю TCP-Over-DNS

По зібраних пакетах трафіку на картинці видно, що йдуть з'єднання по 53 порту TCP, що звичайно розглядається як робота протоколу DNS. Однак, якщо придивитися, то видно, що в поле Text протоколу DNS перебуває якийсь зашифрований текст. Це реалізація тунелю TCP-Over-DNS, що я часто зустрічаю в корпоративних сітках. Ліворуч список інших тунелів, якими можуть скористатися й ваші користувачі або хакери. Чи дає таку інформацію L4 firewall? Немає. Тому, якщо потрібно убезпечити компанію від несанкціонованих тунелів, то потрібно аналізувати вміст переданих даних і саме по них розбирати який же застосунок у цей момент використовує це TCP з'єднання.

Застосунки змінилися – чи змінився ваш firewall. Світ змінився й сьогодні визначати застосунок за номером порту недостатньо. Так, 20 років тому домовилися, що якщо в поле Port прописано 80, те це HTTP, якщо 53, те це DNS, але тепер це вже не так.

Потрібно аналізувати вміст переданих даних і саме по них розбирати який же застосунок у цей момент використовує це TCP з'єднання.

Зайдіть у базу даних застосунків applipedia.paloaltonetworks.com. Подивитеся скільки застосунків використовує 80 і 443 порт.

Застосунки, що використовують порт 80

Проблема багатьох засобів захисту – ігнорування застосунків на нестандартних портах

Переміщення стандартного застосунку на нестандартний порт, теж дозволяє зловмисникові піти з-під контролю. Цей контроль відновлює тільки пристрій, що аналізує вміст усього трафіку, а не тільки заголовки.

Виявлення застосунків у трафіку

Одним із завдань аналізу застосунків є виявлення трафіку застосунків, які спеціально створені, щоб їхнього з'єднання не бачили. Візьмемо для приклада Skype. Люди, які навчилися відрізняти зашифровані UDP пакети Skype від інших зашифрованих UDP пакетів – дуже великі молодці.

Є ще клас пристроїв, які так уміють: Deep Packet Inspection (далі DPI). Такі пристрої стоять зараз у великих провайдерів і дозволяють маніпулювати трафіком застосунків: застосовувати QoS або перенаправляти в потрібному напрямку.

Іноді NGFW і DPI порівнюють. Різниця: DPI призначена для керування якістю трафіку, а NGFW безпекою, хоча в NGFW теж є функції QoS:

– Якщо потрібно виявити застосунок, що не приховує себе в трафіку, наприклад

HTTP, то досить користуватися звичайними пошуками відповідних паттернів або сигнатур. І це активно застосовують виробники. Це простіше всього.

– Якщо потрібно виявити застосунок, що навмисно приховує себе, наприклад, TOR, то отут потрібний набір методик аналізу статистики пакетів і поводження пакетів. Мої спроби змусити хоч одного розроблювача розповісти, як же ці алгоритми працюють, натикаються на відповідь, що це все інтелектуальна власність.

Буває, що застосунок уже поміняв алгоритм роботи, а движок DPI або NGFW ще не встиг змінитися. Наприклад, Telegram іноді міняє, тому що за ним ведуть полювання. Виникають помилкові спрацьовування. Це важливо перевіряти. Відповідно пристрої й NGFW і DPI відрізняються насамперед кількістю і якістю детектирования застосунків. Тут єдиний метод: поставити їх на свій трафік і подивитися. Якщо говорити про периметр, то самий складний трафік, що я бачив, містив 417 різних застосунків за місяць. У середньому ж через периметр ходить 200-300 застосунків різного роду.

У базі даних застосунків перебувають тисячі застосунків, тому по суті розбір форматів і алгоритмів кожного застосунку – це довга й кропітка робота аналітиків. Після того як зрозуміли як застосунок працює, починають працювати програмісти, які реалізують виявлення застосунку по трафіку. І ці кілька тисяч застосунків постійно міняються. Відповідно, продукт повинен постійно підтримуватися, вивчати нові застосунки й контролювати зміни в старі й додавати в базу змінені детектори. Базу всіх можливих застосунків що генерують трафік можна подивитися отут: https://applipedia.paloaltonetworks.com/

Ви повинні розуміти, що вам потрібно детектувати тільки ваші застосунки на периметрі (300 штук), у ЦОД (10-15 штук), в ICS/SCADA мережах (2-3 застосунки) і інші тисячі це всього лише маркетинг і детект якихось незрозумілих нікому застосунків, якими ніхто не користується. Але ж внутрішня сегментація усередині компанії – це постійна вимога стандартів ІБ, що майже ніхто не виконує. Між сегментами, де сидять програмісти, фінансисти, HR і бухгалтерія теж ходять застосунки, як мінімум мережа Windows (протокол SMB), які тільки почали контролювати після епідемії криптолокера WannaCry, що поширювався по SMB. Тобто у внутрішніх мережах теж потрібний аналіз застосунків 7 рівня й супутні методики пошуку шкідливого коду пісочницею й IPS.

Найчастіша проблема, що помітна в мережах: міжмережевий екран нібито 7 рівня детектує застосунки по портах. Для тесту повісьте FTP сервер на 25 порт. Якщо пристрій говорить, що це протокол SMTP, то це точно не L7 firewall. Або просто спробуйте написати правила для двох застосунків різних, які використовують той самий порт.

Ще один цікавий тест для NGFW, коли потрібно зробити два кастомних L7 застосунки з різними властивостями на одному IP адресі. Цього не може L4 firewall, але може L7 firewall. Повний опис і сам тест тут:http://basic.ngfw-test.com/

L7 Firewall зручніше

Якщо подивитися на процес навчання мережевих інженерів, то найчастіше це люди, які закінчили курси якоїсь відомої компанії, виробника мережевого встаткування й звідси в них таке гарне знання технологій роботи мереж.

Як правило, після вивчення семирівневої моделі OSI ISO детально вивчаються лише перші 4 рівні. Тобто всі тонкості інформаційної безпеки мережеві інженери пізнають лише до рівня TCP/UDP/ICMP. З рівня застосунків розглядається лише трохи основних: HTTP, DNS, SSH, Telnet, NTP, FTP. Який результат? І в мережевого адміністратора створюється відчуття, що управляти прикладним рівнем легко із транспортного рівня.

Свіжоспеченому мережевому фахівцеві може здатися, що все можна зробити правилами на транспортному рівні, де потрібно лише дозволити потрібний протокол і порт. Потрібно дозволити браузер в Інтернет? Відкриваємо TCP/80. Потрібно відкрити DNS? Відкриваємо TCP/53 або UDP/53. Потрібно відкрити RDP? Відкриваємо TCP/3389. І написання правил на L4 firewall стає стандартом у компанії.

Треба сказати, що багато які IT фахівці в курсі про поняття statefull inspection. Але одночасно для багатьох є одкровенням, що різні firewall підтримує satefull inspection для різного набору застосунків. Хтось думає, що statefull inspection – це тільки про дозвіл приймати назад відповіді TCP/UDP/ICMP. А як бути із двома з'єднаннями, які робить FTP на 21 і 20 порти? Там потрібно не просто приймати відповідь, так ще й друге з'єднання дозволяти. А скільки ще команд на відкриття нових з'єднань усередині себе дають застосунку? Резюмуючи, у мережах зараз використовуються й звичайні access list, які не розуміють команду PORT усередині FTP протоколу, і є L4 firewall, які розбирають команду PORT і автоматично відкривають потрібний порт, їсти хто пішов далі й дивиться в більше складні команди протоколів MS RPC або ICS/SCADA протоколів. Але всі можливі застосунки L4 firewall не дивиться й ці firewall теж у загальному-те відрізняються кількістю реалізованих усередині Application Layer Gateway (ALG).

До чого я хилю? Переконаність, що досить пам'ятати основні порти TCP/UDP – не працює. У світі вже кілька тисяч застосунків і всі вони користуються комп'ютерними мережами. І ніякий мережевий інженер не в змозі пам'ятати всі ці порти.

Одкровенням для мережевих інженерів є завдання відкрити порти для застосунку більш складніші, наприклад, VNC. Ніхто не пам'ятає які там порти й доводиться вже використовувати google.

Наступним прикладом можна привести Lync він же Skype for Business. Якщо ви заглянете в Microsoft TechNet, де описано, які порти потрібно відкрити, то хочеться написати правило permit any to any, тому що там порядку 40 портів і частина з них повинні відкриватися динамічно. А це катастрофічно незручно прописувати в L4 firewall.

Виходить, що мережевому інженерові зручніше писати в правилах застосунку L7 і потрібно, щоб firewall сам автоматично відкривав потрібні порти.

Потрібно відкрити VNC? Пишеш у правилі слово VNC і вже firewall розуміє які протоколи нижчележачі потрібно відкрити. Це адже зручно.

Звіт NGFW по окремих категоріях трафіку

У середньому доступом в Інтернет з корпоративної мережі користується 200-300 застосунків. Міжмережевий екран рівня застосунків показує які це застосунку й може ці застосунки фільтрувати для всіх або для конкретних користувачів і фільтрувати файли по типах або контенту, які йдуть у дозволених застосунках у всіх користувачів корпоративної мережі. Також не забуваємо що в NGFW, паралельно працюють функції безпеки: IPS, антивірус, anti-spyware, URL фільтр, DNS фільтр, Threat Intelligence і так далі. Тобто ми не просто дозволяємо застосунки, а робимо це безпечно.

L7 Firewall безпечніше

У мене під рукою є Palo Alto Networks NGFW. Я написав на ньому три різні правила. Давайте розберемо чим вони відрізняються.

Якщо ви налаштовували коли-або firewall, то ви бачите, що для різних груп користувачів: vip, marketing і programmers я дозволив SSL трьома різними способами.

– vip користувачі зможуть ходити по порту 443 і зможуть користуватися SSL усередині нього, оскільки він є портом по-умовчанню для SSL. Якщо вони спробують піти по 443 порту, наприклад звичайним telnet, то в них не вийде – міжмережевий екран перевірить що це не SSL і заблокує.

– marketing може ходити по будь-якому порту додатком SSL, тому що в поле Service, де вказуються порти дозволений будь-який порт. Питання, чи хотів я щоб маркетинг використовував SSL по нестандартних портах або помилка налаштування.

– programmers можуть ходити по порту 443 будь-яким додатком, що взагалі-те є діркою. Тому що я споконвічно хотів відкрити тільки SSL. І саме так і працюють L4 firewall – він відкриває порт і далі йому вже однаково що там і які застосунки цим портом користуються. Будь-який програміст із групи programmers може скористатися будь-яким тунелем.

Взагалі, налаштування application-default дозволяє ще й скоротити кількість правил:

ви можете вказати потрібні застосунки в колонку Application і міжмережевий екран сам відкриє потрібні порти для потрібних застосунків і пропустять по цих портах тільки ті застосунки, які там повинні ходити.

Наприклад, для правила нижче, де всім співробітникам дозволено ходити в Інтернет тільки по портах по-умовчанню, NGFW буде постійно перевірятися, що вони хочуть по 53 порту тільки DNS клієнтом, а ніяк не TCP-over-DNS. І звичайно ж це підвищує безпека, адже ви не просто дозволяєте застосунки, а контролюєте, що по відкритих каналах ходять тільки не застосунку, які ви дозволили.

Які нові проблеми створює новий підхід до написання правил по L7

Потрібно розуміти, що визначення застосунку по контенту пакета дуже навантажує процесора L7 firewall. Якщо звичайний L4 firewall перевіряв тільки трохи байт заголовка TCP пакета й потім інші мегабайти flash ролика пропускав без перевірки, то L7 firewall повинен зчитувати всі що зберігається в поле даних TCP/IP і постійно перевіряти що за контент перебуває усередині з'єднання TCP/IP, раптом воно змінилося або несе погрозу для компанії. Тому, коли з'явився такий функціонал, як аналіз контента, те всі пристрої стали гальмувати.

Обмеження технології аналізу 7 рівня

L7 firewall потрібно більше пам'яті для зберігання стану одного з'єднання, тому параметр «число одночасних з'єднань» в L7 firewall завжди нижче ніж в L4 Firewall при однаковій кількості оперативної пам'яті в обох пристроях, причому значно, раз в 10. Це вже пояснювалося вище. І це ціна за безпеку ваших застосунків. Тому якщо ви порівнюєте L4 і L7 інспекцію, то ставте запитання виробникові як він вимірював параметр «число одночасних сесій»: із включеною безпекою на 7 рівні або з виключеною.

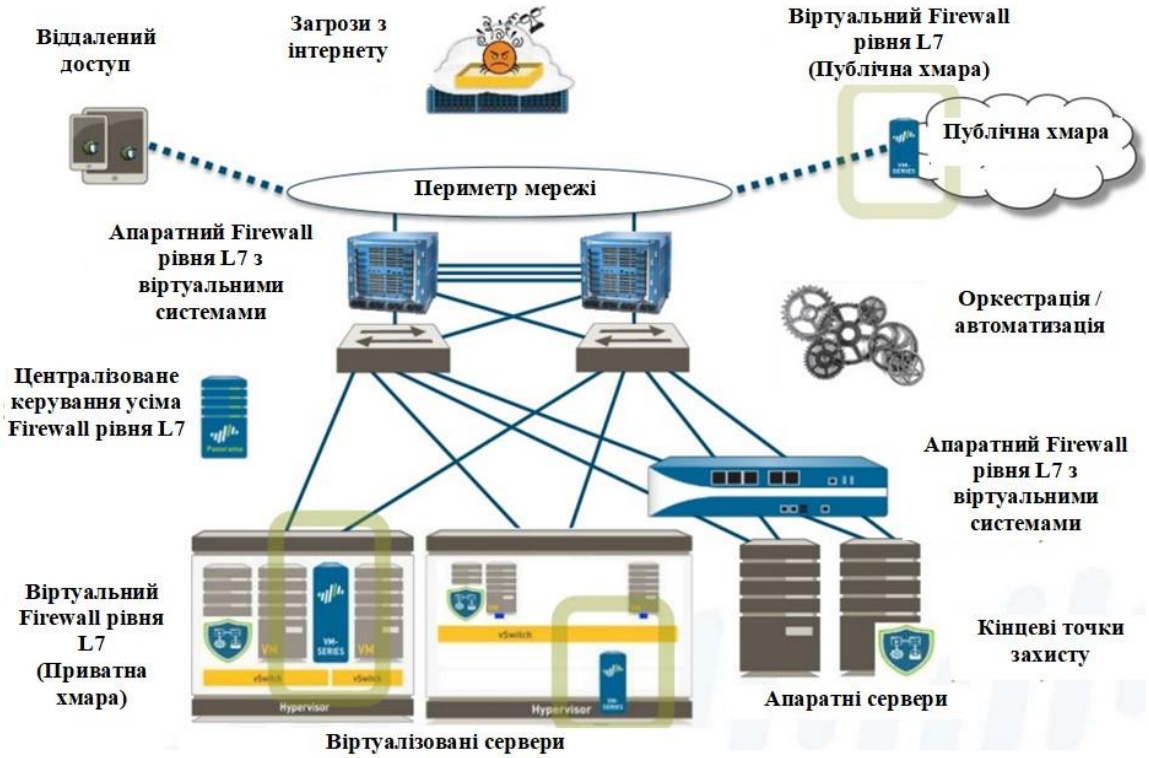


Рисунок 1 – Структурна схема системи

Те ж саме й із продуктивністю: процесор L4 firewall перевіряє лише декілька байт заголовка пакета й потім уже самі дані передає на швидкості маршрутизації без перевірки, а L7 firewall перевірять і заголовок і всі ті мегабайти даних, які утримуються в наступних пакетах з'єднання. А це вже зовсім інша робота. Тому таку роботу потрібно робити на спеціалізовані для цього апаратних платформах, де прискорений аналіз застосунків,

прискорена робота потокового антивірусу, прискорена робота IPS і інших функцій безпеки. Краще всіх у створенні чипів для прискорення безпеки представлена компанія Cavium, чипами якої, наприклад, користується компанія Palo Alto Networks. Крім того використання спеціалізованих чипів FPGA (ПЛІС) дозволяє прошивати сигнатури антивірусу й IPS у сам чип і перевірка сигнатур йде на апаратній швидкості чипа FPGA. Зараз навіть в особистих комп'ютерів є прискорення графічних функцій на виділених графічних процесорах, так що використання чипів для прискорення безпеки – логічний розвиток технологій.

Таким чином:

По-перше, управляти безпекою на L7 firewall простіше. Раніше ви довго читали документацію виробника застосунку й відкривали порти, що там перераховані. Тепер просто: указуєте назву застосунку в правилі NGFW і потрібні порти будуть дозволятися автоматично залежно від стану з'єднань даного застосунку.

По-друге, ви зможете виявити й заблокувати тунелювання, оскільки L7 firewall безпечно дозволяє тільки явно зазначений застосунок і якщо хтось спробує туннелювати інший застосунок по відкритому порту, то відразу буде виявлений і заблокований.

По-третє, ви можете дозволити потрібний застосунок по будь-якому потрібному порту й по цьому порту буде ходити тільки потрібний застосунок, а не всі відразу. Наприклад, тільки веб-браузер буде використовувати 80 порт.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів аналізу додатків рівня L7 у Firewall. В межах України в недостатній мірі представлені вітчизняні розробки в цій області. У роботі наведені теоретичне узагальнення й рішення наукового завдання дослідження методів аналізу додатків рівня L7 у Firewall. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем аналізу додатків рівня L7 у Firewall; Досліджена система аналізу додатків рівня L7 у Firewall; На основі отриманих результатів досліджень створена програмна реалізація системи аналізу додатків рівня L7 у Firewall. Розроблені під час виконання роботи алгоритми дозволяють успішно вирішувати завдання аналізу додатків рівня L7 у 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.

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

Т. Смірнова, магістр гр. КН-19М-1,4
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ ПОШУКУ ЗОБРАЖЕННЯ ЗА ЗМІСТОМ ЗА ДОПОМОГОЮ AR/VR/MR

У статті розроблено програмне забезпечення, яке призначено для системи пошуку зображення за змістом за допомогою AR/VR/MR. Метою розробки є дослідження та програмна реалізація системи пошуку зображення за змістом за допомогою AR/VR/MR. Об'єктом дослідження є процес пошуку зображення за змістом за допомогою AR/VR/MR.Предметом дослідження є методи пошуку зображення за змістом за допомогою AR/VR/MR. Методи дослідження базуються на методах розпізнання зображень, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи пошуку зображення за змістом за допомогою AR/VR/MR. 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, пошук зображення, AR/VR/MR

Постановка проблеми. Рішення з використанням AR ближче до практичного впровадження, причому різноманітних варіантів застосування набагато більше, чим у випадку VR. Втім, поки в компаніях їх просуванням займаються окремі ентузіасти, а впровадження обмежуються переважно пілотними проектами.

Яка сама гаряча тема в IT? Блокчейн, штучний інтелект, AR/VR? Давайте переформулюємо питання по-іншому. Який із трьох ринків самий перспективний? За прогнозами експертів Research And Markets, обсяг ринку блокчейна досягне 7,6 млрд доларів до 2024 року. Аналітики Global Market Insights називають куди більш значну цифру – 16 млрд доларів – до того ж строку.

Штучний інтелект, він же нейронна мережа, має потенційно більш широку область застосування. Відповідно, і цифри більше: KBV Research прогнозує, що обсяг ринку ШІ досягне 32 млрд доларів до 2024 року, а Grand View Research дає схожу оцінку в 36 млрд доларів, але для 2025 року.

А що ж AR/VR? Якщо вірити Омарові Ахтару, аналітикові Altimeter, уже через якихось два роки, в 2022-м, ринок імерсійних технологій складе 215 млрд доларів. Так що відповідь на запитання про найбільш перспективний напрямок, здається, очевидний. У дійсності, звичайно, розкид оцінок для ринку AR/VR нітрохи не менше, чим для двох інших.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-25] було виявлено певні прогалини у забезпеченні системи пошуку зображення за змістом за допомогою AR/VR/MR.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи пошуку зображення за змістом за допомогою AR/VR/MR.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем пошуку зображення за змістом за допомогою AR/VR/MR.

– Дослідження системи пошуку зображення за змістом за допомогою AR/VR/MR.

– Програмна реалізація системи пошуку зображення за змістом за допомогою AR/VR/MR.

Об'єктом дослідження є процес пошуку зображення за змістом за допомогою AR/VR/MR.

Предметом дослідження є методи пошуку зображення за змістом за допомогою AR/VR/MR.

Методи дослідження базуються на методах розпізнання зображень, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. У галузі не існує чіткого загальноприйнятого розмежування між віртуальною, доповненою або змішаною реальностями. Особливо це стосується двох останніх понять: що віднести до AR, а що до змішаної реальності? Умовно, AR – це розумні окуляри, на поверхню яких проектується контекстна (звичайно текстова) інформація. А в окулярах MR реальні об'єкти доповнюються віртуальними. Як приклад останніх можна привести окуляри Hololens компанії Microsoft, які багато експертів уважають найбільш просунутим на даний момент рішенням.

Окуляри Hololens використовують, наприклад, для контролю над будівельними роботами. Вони дозволяють накласти віртуальну 3D-модель на споруджуваний об'єкт і зрівняти досягнутий результат з очікуваним. На одному з об'єктів це дозволило, зокрема, з'ясувати, що протягом місяця ніхто не обертав уваги на допущені при побудові трапа помилки (його неправильну орієнтацію), хоча звірення з паперовою документацією проводилися.

У нафтогазовій компанії Chevron за допомогою Hololens реалізується функціональність віддаленого помічника. Відрядження висококваліфікованого фахівця для проведення технічного обслуговування устаткування обходиться дорого. Для проведення ремонту місцевий співробітник надягає окуляри, через які фахівець, що перебуває в центрі керування, бачить реальну картину. Він може не тільки на словах пояснити, що потрібно зробити, але й наочно показати необхідні дії – наприклад, обвести на екрані вимикач, на який слід нажати.

У компанії BAE, що робить акумулятори, розумні окуляри виконують функції віртуального наставника для великої кількості збирачів. В Hololens послідовно відображаються голографічні інструкції, на яких показується, що робити в конкретний момент: установити деталь, закріпити її і т.д. Такий підхід дозволяє швидко перетворити молодого співробітника без досвіду в майстра. У результаті процес складання вдалося прискорити на 30-50%.

Зараз ведеться пілотний проект, де були об'єднано два рішення, що реалізують покрокові інструкції для експлуатації електрощитового устаткування. Інженерові виводиться контекстна інформація, коли й що йому потрібно зробити. У цьому випадку важлива не стільки швидкість роботи, скільки мінімізація потенційно небезпечних помилок. Після завершення робіт і одержання підтвердження від диспетчера інформація про операції заноситься в електронний журнал заявок.

Однак часто навіть фахівці змішують поняття AR і MR (не просто так MR назвали змішаною реальністю). Втім, віртуальна й доповнена реальності – це не устаткування, а

методологія. У якості ж устаткування можуть застосовуватися будь-які підходящі пристрої, навіть звичайні планшети й монітори.

У рамках даної роботи ми не станемо проводити строгої відмінності між AR і MR, а будемо дотримуватися термінології. Відмінність між ними не настільки істотна, як між VR і AR.

На відміну від віртуальної реальності, при використанні розумних окулярів не потрібно створювати складний контент – найчастіше досить підготувати текстові інструкції й ілюстрації. До того ж на ринку є готові платформи, такі як Vuforia, за допомогою яких підготовка контенту значно спрощується – це може зробити людина без технічної освіти. У результаті пілотний проект можна реалізувати за 1-3 місяця.

Практичне застосування AR

Рішення з використанням AR більш підготовлені до практичного впровадження, причому в безлічі різноманітних варіантів. Як показало недавнє спільне дослідження VR Intelligence і Superdata Research, 46% галузевих експертів і професіоналів уважають, що AR одержить широке поширення вже протягом найближчих трьох років, тоді як в аналогічних перспективах для VR певен тільки 33%.

Ще рік-два назад багато хто вважали, що VR ближче до впровадження, адже концептуально ця технологія не відрізняється від візуалізації на екрані. А для AR, видалося, буде потрібно вічність, щоб такі рішення, як Hololens компанії Microsoft, можна було застосовувати для практичних завдань. Зараз же самі успішні проекти зв'язані саме з доповненою реальністю.

«Розумні окуляри» (Google Glass, Realware, Vuzix, ODG) дозволяють робити просту роботу більш ефективно. Вони не здатні візуалізувати 3D-моделі, як Microsoft Hololens, але найчастіше цього й не потрібно. Їх можна з успіхом використовувати для таких завдань, як інспекція устаткування, щоб інженерові не доводилося витрачати час на заповнення різних бланків.

Рятування співробітника від необхідності пошуку або записи інформації дозволяє підвищити продуктивність праці. Одержувану вигоду легко виміряти. Якщо раніше на інспекцію вантажівки йшло 2 хв 15 з, то зараз 1 хв 45 с. Інспекторові не треба відволікатися, щоб занести інформацію в iPad. Завдяки сучасним потужним технологіям розпізнавання мови, його зауваження відразу можуть бути перетворені в текст і занесені до протоколу.

Був реалізований пілотний проект по використанню смарт-окулярів для складського обліку. Традиційні термінали для зчитування даних важкі й незручні, до того ж у них не самий дружелюбний інтерфейс. При використанні розумних окулярів, крім скорочення часу на виконання основних операцій, зменшується число помилок. Перевага використання окулярів – не в підказках комірникам (вони й без того знають, що їм робити), а в автоматичному обліку зроблених дій.

У багатьох завданнях можна обійтися взагалі без окулярів – досить звичайного смартфону із установленим на ньому додатком. Правда повноцінну доповнену реальність реалізувати непросто: при роботі з більшим об'єктом виникають труднощі із прив'язкою інформації – нелегко зрозуміти, до чого ставляться конкретні дані. Тому для ідентифікації об'єкта найчастіше використовується звичайний QR-код, при зчитуванні якого відображаються всі необхідні дані: характеристики, історія обслуговування і т.д.

У нафтогазової галузі вже є досвід роботи з VR-розв'язками, правда невдалий. Ще в 1999 році був створений міжнародний консорціум для вивчення можливості використання рішень віртуальної реальності. Нафтові компанії стали створювати в себе «VR-печери», візуалізаційні центри на базі проекційних систем (CAVE, англ. «печера», рекурсивний акронім від Cave Automatic Virtual Environment).

Однак вони виявилися занадто складними й дорогими в реалізації й обслуговуванні (середня вартість проекту становила 20 млн доларів), і при цьому реально ними мало хто користувався – технології тоді не були готові. Попередній негативний досвід підсилює

скептицизм відносно пропонованих рішень, які й без того непросто впроваджуються на виробництві.

В Schlumberger інструменти віртуальної реальності використовуються для навчання співробітників нафтогазових компаній.

І висока ціна – далеко не єдина проблема. Мінімальний комплект для знайомства з віртуальною реальністю, включаючи програмне забезпечення й шолом, обійдеться всього в 5000 доларів. Однак це навіть не початкові витрати, особливо якщо передбачається масштабне впровадження розширеної реальності. Для шоломів змішаної реальності, таких як Hololens, середня ціна становить близько 3000 доларів, так що для масового використання на виробництві вони поки дороги.

Компанія General VR підготувала фінансове обґрунтування для 10 різних проектів. Як можна було очікувати, впровадження VR/AR виявилося доцільним не у всіх випадках. Більше того, залежно від того, що створився IT-ландшафту й інших факторів те саме рішення на одному підприємстві може виявитися економічно вигідним, а на іншому ні.

Розрахункова віддача AR виявилася більше, чим можна було припустити до підготовки обґрунтування. У випадку ж VR ситуація протилежна. На жаль, посилаючись на NDA, він не привів ніяких цифр, щоб можна було оцінити економічний ефект.

Найбільший ефект досягається при інтеграції рішень AR/VR з існуючими IT-системами. Віддача залежить від того, наскільки легко/складно це зробити. Швидше за все, через новизну рішень і відсутності стандартизованих механізмів, зробити це буде непросто. Відзначимо складність їх інтеграції в існуюче середовище, підкреслюючи, що це одна із проблем, які ще має бути подоланою на шляху широкого поширення AR/VR.

Як і у випадку мультимедійних рішень, на початкових етапах поширення AR/VR позначається нестача контенту, наприклад, відсутні готові цифрові двійники для реальних об'єктів.

Рішення віртуальної/доповненої реальності відразу залучають до себе увагу. Однак від цікавості до реальних проектів, як говориться, дистанція величезного розміру. Проекти в компаніях просуваються переважно зусиллями окремих ентузіастів, а впровадження в російських компаніях поки обмежуються переважно пілотними проектами.

Для широкомасштабного впровадження ще має бути подолати масу труднощів), однак представники цієї ще молодої галузі певен у її глобальних перспективах. Якщо не в середньостроковій, то в довгостроковій перспективі фізичні екрани й проектори підуть у небуття. Навіщо вони будуть потрібні, якщо ми станемо користуватися маленькими окулярами, вбудовані засоби яких можуть проектувати цифровий контент безпосередньо в очі.

У даному розділі зосередилися в основному на потенційних застосуваннях VR/AR/MR у промисловості. Але розглянуті технології затребувані й в інших галузях економіки – у роздрібній торгівлі для презентації товарів, у ріелторському сегменті для продажу елітної нерухомості, у маркетингу для проведення промокампаній, в охороні здоров'я для діагностики й т.п. І звичайно, в індустрії розваг.

Розробка структурної схеми

Розпізнавання образів – розділ кібернетики, що розробляє принципи й методи класифікації, а також ідентифікації предметів, явищ, процесів, сигналів, ситуацій – усіх тих об'єктів, які можуть бути описані кінцевим набором деяких ознак або властивостей, що характеризують об'єкт.

Образ являє собою опис об'єкта. Образи мають характерну властивість, що проявляються в тому, що ознайомлення з кінцевим числом явищ із того самого безлічі дає можливість пізнавати як завгодно велике число його представників.

У теорії розпізнавання образів можна виділити два основні напрямки:

– вивчення здатностей до розпізнавання, якими мають людські істоти й інші живі організми;

– розвиток теорії й методів побудови пристроїв, призначених для рішення окремих завдань розпізнавання образів у певних прикладних областях.

Далі в статті описуються проблеми, принципи й методи реалізації систем розпізнавання образів, пов'язані з розвитком другого напрямку. У другій частині статті розглядаються нейромережеві методи розпізнавання образів, які можуть бути віднесені до першого напрямку теорії розпізнавання образів.

Проблеми побудови систем розпізнавання образів

Завдання, що виникають при побудові автоматичних систем розпізнавання образів, можна звичайно віднести до декільком основним областям. Перша з них пов'язана з виставою вихідних даних, отриманих як результати вимірів для підлягаючого розпізнаванню об'єкта. Це проблема чутливості. Кожна обмірювана величина є деякою характеристикою образа або об'єкта. Допустимо, наприклад, що образами є буквено-цифрові символи. В такому випадку, у датчику може бути успішно використана вимірювальна сітківка). Якщо сітківка складається з n-елементів, то результати вимірів можна представити у вигляді вектора вимірів або вектора образа, де кожний елемент x_i, ухвалює, наприклад, значення 1, якщо через і-е гніздо сітківки проходить зображення символу, і значення 0 а якщо ні, то.

Друга проблема розпізнавання образів пов'язана з виділенням характерних ознак або властивостей з отриманих вихідних даних і зниженням розмірності векторів образів. Цю проблему часто визначають як проблему попередньої обробки й вибору ознак.

Ознаки класу образів являють собою характерні властивості, загальні для всіх образів даного класу. Ознаки, що характеризують відмінності між окремими класами, можна інтерпретувати як міжкласові ознаки. Внутрішньокласові ознаки, загальні для всіх розглянутих класів, не несуть корисної інформації з погляду розпізнавання й можуть не братися до уваги. Вибір ознак уважається однієї з важливих завдань, пов'язаних з побудовою систем, що розпізнають. Якщо результати вимірів дозволяють одержати повний набір розпізнавальних ознак для всіх класів, властиво розпізнавання й класифікація образів не викличуть особливих утруднень. Автоматичне розпізнавання тоді зведеться до процесу простого зіставлення або процедурам типу перегляду таблиць. В більшості практичних завдань розпізнавання, однак, визначення повного набору розпізнавальних ознак виявляється справою винятково важким, якщо взагалі не неможливим. З вихідних даних звичайно вдається витягти деякі з розпізнавальних ознак і використовувати їх для спрощення процесу автоматичного розпізнавання образів. В частковості, розмірність векторів вимірів можна знизити за допомогою перетворень, що забезпечують мінімізацію втрати інформації.

Третя проблема, пов'язана з побудовою систем розпізнавання образів, полягає у відшуканні оптимальних вирішальних процедур, необхідних при ідентифікації й класифікації. Після того як дані, зібрані про підлягаючі розпізнаванню образах, представлені точками або векторами вимірів у просторі образів, надамо машині з'ясувати, якому класу образів ці дані відповідають. Нехай машина призначена для розрізнення M класів, позначених w_1, w_2,..., w_m. В такому випадку, простір образів можна вважати, що полягають із M областей, кожна з яких містить точки, відповідні до образів з одного класу. При цьому завдання розпізнавання може розглядатися як побудова границь областей рішень, що розділяють M класів, виходячи із зареєстрованих векторів вимірів. Нехай ці границі визначені, наприклад функціями, що вирішують, $d_1(x)$, $d_2(x)$,..., $d_m(x)$. Ці функції, називані також дискримінантними функціями, являють собою скалярні й однозначні функції образа x. Якщо $d_i(x) > d_j(x)$, то образ x належить класу w_1. Інакше кажучи, якщо і-а вирішальна функція $d_i(x)$ має найбільше значення, те змістовною ілюстрацією подібної схеми автоматичної класифікації, заснованої на реалізації процесу ухвалення рішення.

Вирішальні функції можна одержувати цілим рядом способів. В тих випадках, коли про розпізнавані образи є повні апріорні відомості, що вирішують функції можуть бути визначені точно на основі цієї інформації. Якщо щодо образів є лише якісні відомості,

можуть бути висунуті розумні допущення про вид вирішальних функцій. В останньому випадку, границі областей рішень можуть суттєво відхилятися від дійсних, і тому необхідно створювати систему, здатну приходити до задовільного результату за допомогою ряду послідовних коректувань.

Об'єкти (образи), підмети розпізнаванню й класифікації за допомогою автоматичної системи розпізнавання образів, повинні мати набір вимірних характеристик. Коли для цілої групи образів результати відповідних вимірів виявляються аналогічними, уважається, що ці об'єкти належать одному класу. Ціль роботи системи розпізнавання образів полягає в тому, щоб на основі зібраної інформації визначити клас об'єктів з характеристиками, аналогічними обмірюваним у розпізнаваних об'єктів. Правильність розпізнавання залежить від обсягу інформації, що розрізняє, утримується у вимірюваних характеристиках, і ефективності використання цієї інформації.

Основні методи реалізації систем розпізнавання образів

Розпізнаванням образів називаються завдання побудови й застосування формальних операцій над числовими або символьними відображеннями об'єктів реального або ідеального миру, результати, рішення яких відбивають відносини еквівалентності між цими об'єктами. Відносини еквівалентності виражають приналежність оцінюваних об'єктів до яких-небудь класів, розглянутих як самостійні семантичні одиниці.

При побудові алгоритмів розпізнавання класи еквівалентності можуть задаватися дослідником, який користується власними змістовними виставами або використовує зовнішню додаткову інформацію про подібність і відмінність об'єктів у контексті розв'язуваного завдання. Тоді говорять про “розпізнавання із вчителем”. А якщо ні, то, тобто коли автоматизована система вирішує завдання класифікації без залучення зовнішньої навчальної інформації, говорять про автоматичну класифікацію або “розпізнавання без вчителя”. Більшість алгоритмів розпізнавання образів вимагає залучення досить значних обчислювальних потужностей, які можуть бути забезпечені тільки високопродуктивною комп'ютерною технікою.

Різні автори (Ю.Л. Барабаш [24], В.І. Васильєв [25], А.Л. Горелік, В.А. Скрипкін [26], Р. Дуда, П. Харт [13], Л.Т. Кузин [2], Ф.І. Перегудів, Ф.П. Тарасенко [3], Темників Ф.Е., Афонін В.А., Дмитрієв В.І. [4], Дж. Ту, Р. Гонсалес [5], П. Вінстон [6], К. Фу [7], Я.С. Ципкін [8] і ін.) дають різну типологію методів розпізнавання образів. Одні автори розрізняють параметричні, непараметричні й евристичні методи, інші – виділяють групи методів, виходячи з історично склавшихся шкіл і напрямків у даній області.

У той же час, відомі типології не враховують одну дуже істотну характеристику, яка відбиває специфіку способу вистави знань про предметну область за допомогою якого-небудь формального алгоритму розпізнавання образів. Д.А.Поспєлов виділяє два основні способи вистави знань [9]:

– Інтенсіональне подання – у вигляді схеми зв'язків між атрибутами (ознаками).

– Екстенсіональне подання – за допомогою конкретних фактів (об'єкти, приклади).

Необхідно відзначити, що існування саме цих двох груп методів розпізнавання:, що оперують із ознаками, що й оперують із об'єктами, глибоко закономірно. Із цього погляду жоден із цих методів, узятий окремо від іншого, не дозволяє сформувати адекватне відбиття предметної області. Між цими методами існує відношення додатковості в змісті Н.Бору [11], тому перспективні системи розпізнавання повинні забезпечувати реалізацію обох цих методів, а не тільки якого-або одного з них.

Таким чином, в основу класифікації методів розпізнавання, запропонованої Д.А.Поспєловим [9], покладені фундаментальні закономірності, що лежать в основі людського способу пізнання взагалі, що ставить її в зовсім особливе (привілейоване) положення в порівнянні з іншими класифікаціями, які на цім тлі виглядають більш легковагими й штучними.

Інтенсіональні методи

Відмінною рисою інтенсіональних методів є те, що в якості елементів операцій при побудові й застосуванні алгоритмів розпізнавання образів вони використовують різні характеристики ознак і їх зв'язків. Такими елементами можуть бути окремі значення або інтервали значень ознак, середні величини й дисперсії, матриці зв'язків ознак і т.п., над якими проводяться дії, що виражаються в аналітичній або конструктивній формі. При цьому об'єкти в даних методах не розглядаються як цілісні інформаційні одиниці, а виступають у ролі індикаторів для оцінки взаємодії й поведінки своїх атрибутів.

Група інтенсіональних методів розпізнавання образів велика, і її розподіл на підкласи носить у певній мері умовний характер:

– методи, засновані на оцінках щільностей розподілу значень ознак [10]

– методи, засновані на припущеннях про клас вирішальних функцій

– логічні методи

– лінгвістичні (структурні) методи.

Методи, засновані на оцінках щільностей розподілу значень ознак. Ці методи розпізнавання образів запозичені із класичної теорії статистичних рішень, у якій об'єкти дослідження розглядаються як реалізації багатомірної випадкової величини, розподіленої в просторі ознак за яким-небудь законом. Вони базуються на байєсовській схемі прийняття рішень, що апелює до апріорних ймовірностей приналежності об'єктів до того або іншому розпізнаваному класу й умовним щільностям розподілу значень вектора ознак. Дані методи зводяться до визначення відносини правдоподібності в різних областях багатомірного простору ознак.

Група методів, заснованих на оцінці щільностей розподілу значень ознак, має пряме відношення до методів дискримінантного аналізу. Байєсовський підхід до прийняття рішень і ставиться до найбільш розроблених у сучасній статистиці так званих параметричних методів, для яких уважається відомим аналітичне вираження закону розподілу (у цьому випадку нормальний закон) і потрібно оцінити лише невелика кількість параметрів (вектори середніх значень і коваріаційні матриці).

До цієї групи ставиться й метод обчислення відносини правдоподібності для незалежних ознак. Цей метод, за винятком припущення про незалежність ознак (яке в дійсності практично ніколи не виконується), не припускає знання функціонального виду закону розподілу. Його можна віднести до непараметричних методів [9].

Інші непараметричні методи, застосовувані тоді, коли вид кривої щільності розподілу невідомий і не можна зробити взагалі ніяких припущень про її характер, займають особливе положення. До них ставляться відомі метод багатомірних гістограм, метод k-найближчих сусідів, метод евклідової відстані, метод потенційних функцій і ін., узагальненням яких є метод, що одержав назву “оцінки Парзена”. Ці методи формально оперують об'єктами як цілісними структурами, але залежно від типу завдання розпізнавання можуть виступати й в інтенсіональной і в екстенсіональной іпостасях.

Непараметричні методи аналізують відносні кількості об'єктів, що попадають у задані багатомірні обсяги, і використовують різні функції відстані між об'єктами навчальної вибірки й розпізнаваними об'єктами. Для кількісних ознак, коли їх число багато менше обсягу вибірки, операції з об'єктами відіграють проміжну роль в оцінці локальних щільностей розподілу умовних ймовірностей і об'єкти не несуть значеннєвого навантаження самостійних інформаційних одиниць. У той же час, коли кількість ознак порівнянна або більше числа досліджуваних об'єктів, а ознаки носять якісний або дихотомічний характер, те ні про які локальні оцінки щільностей розподілу ймовірностей не може йти мови. У цьому випадку об'єкти в зазначених непараметричних методах розглядаються як самостійні інформаційні одиниці (цілісні емпіричні факти) і дані методи набувають сенсу оцінок подібності й відмінності досліджуваних об'єктів.

Таким чином, ті самі технологічні операції непараметричних методів залежно від умов завдання мають сенс або локальних оцінок щільностей розподілу ймовірностей значень ознак, або оцінок подібності й відмінності об'єктів.

У контексті інтенсіонального вистави знань тут розглядається перша сторона непараметричних методів, як оцінок щільностей розподілу ймовірностей. Багато авторів відзначають, що на практиці непараметричні методи типу оцінок Парзена працюють добре. Основними труднощами застосування зазначених методів уважаються необхідність запам'ятовування всієї навчальної вибірки для обчислення оцінок локальних щільностей розподілу ймовірностей і високий чутливість до непоказності навчальної вибірки.

Методи, засновані на припущеннях про клас вирішальних функцій. У даній групі методів уважається відомим загальний вид вирішальної функції й заданий функціонал її якості. На підставі цього функціонала по навчальній послідовності шукається найкраще наближення вирішальної функції. Найпоширенішими є вистави вирішальних функцій у вигляді лінійних і узагальнених нелінійних поліномів. Функціонал якості вирішального правила звичайно зв'язують із помилкою класифікації.

Основною гідністю методів, заснованих на припущеннях про клас вирішальних функцій, є ясність математичної постановки завдання розпізнавання, як завдання пошуку екстремуму. Рішення цього завдання нерідко досягається за допомогою яких-небудь градієнтних алгоритмів. Різноманіття методів цієї групи пояснюється широким спектром використовуваних функціоналів якості вирішального правила й алгоритмів пошуку екстремуму. Узагальненням розглянутих алгоритмів, до яких ставляться, зокрема, алгоритм Ньютона, алгоритми перцептроного типу й ін., є метод стохастичної апроксимації. На відміну від параметричних методів розпізнавання успішність застосування даної групи методів не так сильно залежить від неузгодженості теоретичних вистав про закони розподілу об'єктів у просторі ознак з емпіричною реальністю. Усі операції підлегло однієї головної мети – знаходженню екстремуму функціонала якості вирішального правила. У той же час результати параметричних і розглянутих методів можуть бути схожими. Як показано вище, параметричні методи для випадку нормальних розподілів об'єктів у різних класах з рівними коваріаційними матрицями приводять до лінійних вирішальних функцій. Відзначимо також, що алгоритми відбору інформативних ознак у лінійних діагностичних моделях, можна інтерпретувати як приватні варіанти градієнтних алгоритмів пошуку екстремуму.

Можливості градієнтних алгоритмів пошуку екстремуму, особливо в групі лінійних вирішальних правил, досить добре вивчені. Збіжність цих алгоритмів доведена тільки для випадку, коли розпізнавані класи об'єктів відображаються в просторі ознак компактними геометричними структурами. Однак прагнення добитися достатньої якості вирішального правила нерідко може бути задоволене за допомогою алгоритмів, що не мають строгого математичного доказу збіжності рішення до глобального екстремуму [9].

До таких алгоритмів ставиться більша група процедур евристичного програмування, що представляють напрямок еволюційного моделювання. Еволюційне моделювання є біонічним методом, запозиченим у природи. Воно засноване на використанні відомих механізмів еволюції з метою заміни процесу змістовного моделювання складного об'єкта феноменологичним моделюванням його еволюції.

Відомим представником еволюційного моделювання в розпізнаванні образів є метод групового обліку аргументів (МГОА). В основу МГОА покладений принцип самоорганізації, і алгоритми МГОА відтворюють схему масової селекції. В алгоритмах МГОА особливим образом синтезуються й відбираються члени узагальненого полінома, який часто називають поліномом Колмогорова-Габора. Цей синтез і відбір проводиться з наростаючим ускладненням, і заздалегідь не можна вгадати, який остаточний вид буде мати узагальнений поліном. Спочатку звичайно розглядають прості попарні комбінації вихідних ознак, з яких складаються рівняння вирішальних функцій, як правило, не вище другого порядку. Кожне рівняння аналізується як самостійна вирішальна функція, і по навчальній

вибірці тем або іншим способом перебувають значення параметрів складених рівнянь. Потім з отриманого набору вирішальних функцій відбирається частина в деякому змісті кращих. Перевірка якості окремих вирішальних функцій здійснюється на контрольній (перевірочної) вибірці, що іноді називають принципом зовнішнього доповнення. Відібрані приватні вирішальні функції розглядаються далі як проміжні змінні, що служать вихідними аргументами для аналогічного синтезу нових вирішальних функцій і т.д. Процес такого ієрархічного синтезу триває доти, поки не буде досягнутий екстремум критерію якості вирішальної функції, що на практиці проявляється в погіршенні цієї якості при спробах подальшого збільшення порядку членів полінома щодо вихідних ознак.

Принцип самоорганізації, покладений в основу МГОА, називають евристичною самоорганізацією, тому що весь процес ґрунтується на введенні зовнішніх доповнень, обираних евристично. Результат рішення може суттєво залежати від цих евристик. Від того, як розділені об'єкти на навчальну й перевірочну вибірки, як визначається критерій якості розпізнавання, яка кількість змінної пропускається в наступний ряд селекції і т.д., залежить результуюча діагностична модель.

Зазначені особливості алгоритмів МГОА властиві й іншим підходам до еволюційного моделювання. Але відзначимо тут ще одну сторону розглянутих методів. Це – їх змістовна сутність. За допомогою методів, заснованих на припущеннях про клас вирішальних функцій (еволюційних і градієнтних), можна будувати діагностичні моделі високої складності й одержувати практично прийнятні результати. У той же час досягненню практичних цілей у цьому випадку не супроводжує добування нових знань про природу розпізнаваних об'єктів. Можливість добування цих знань, зокрема знань про механізми взаємодії атрибутів (ознак), тут принципово обмежена заданою структурою такої взаємодії, зафіксованої в обраній формі вирішальних функцій. Тому максимально, що можна сказати після побудови тієї або іншої діагностичної моделі – це перелічити комбінації ознак і самі ознаки, що ввійшли в результуючу модель. Але зміст комбінацій, що відбивають природу й структуру розподілів досліджуваних об'єктів, у рамках даного підходу часто залишається нерозкритим.

Логічні методи. Логічні методи розпізнавання образів базуються на апарату алгебри логіки й дозволяють оперувати інформацією, укладеної не тільки в окремих ознаках, але й у комбінаціях значень ознак. У цих методах значення якої-небудь ознаки розглядаються як елементарні події.

У самому загальному виді логічні методи можна охарактеризувати як різновид пошуку по навчальній вибірці логічних закономірностей і формування деякої системи логічних вирішальних правил (наприклад, у вигляді кон’юнкцій елементарних подій), кожне з яких має власна вага. Група логічних методів різноманітна й включає методи різної складності й глибини аналізу. Для дихотомічних (булевих) ознак популярними є так звані деревоподібні класифікатори, метод тупикових тестів, алгоритм “Кора” і інші. Більш складні методи ґрунтуються на формалізації індуктивних методів Д.С.Мілля. Формалізація здійснюється шляхом побудови квазіаксіоматичної теорії й базується на багатосортній багатозначній логіці із кванторами по кортежах змінної довжини [9].

Алгоритм «Кора», як і інші логічні методи розпізнавання образів, є досить трудомістким, оскільки при відборі кон’юнкцій необхідний повний перебір. Тому при застосуванні логічних методів пред'являються високі вимоги до ефективної організації обчислювального процесу, і ці методи добре працюють при порівняно невеликих размірностях простору ознак і тільки на потужних комп'ютерах.

Лінгвістичні (синтаксичні або структурні) методи. Лінгвістичні методи розпізнавання образів засновані на використанні спеціальних граматик, що породжують мови, за допомогою яких може описуватися сукупність властивостей розпізнаваних об'єктів [13]. Граматикою називають правила побудови об'єктів із цих непохідних елементів.

Якщо опис образів проводиться за допомогою непохідних елементів (підобразів) і їх відносин, то для побудови автоматичних систем розпізнавання застосовується

лінгвістичний або синтаксичний підхід з використанням принципу спільності властивостей. Образ можна описати за допомогою ієрархічної структури підобразів, аналогічній синтаксичній структурі мови. Ця обставина дозволяє застосовувати при рішення завдань розпізнавання образів теорію формальних мов. Передбачається, що граматика образів містить кінцеві безлічі елементів, називаних змінними, непохідними елементами й правилами підстановки. Характер правил підстановки визначає тип граматики. Серед найбільш вивчених граматик можна відзначити регулярні, бесконтекстні й граматики безпосередньо складових. Ключовими моментами даного підходу є вибір непохідних елементів образа, об'єднання цих елементів і єднальних їхніх відносин у граматики образів і, нарешті, реалізація у відповідній мові процесів аналізу й розпізнавання. Такий підхід особливо корисний при роботі з образами, які або не можуть бути описані числовими вимірами, або настільки складні, що їх локальні ознаки ідентифікувати не вдається й доводиться звертатися до глобальних властивостей об'єктів.

Наприклад, Е.А. Бутаков, В.І. Островський, І.Л. Фадєєв[12] пропонують наступну структуру системи для обробки зображень, що використовує лінгвістичний підхід, де кожний з функціональних блоків є програмним (мікропрограмним) комплексом (модулем), що реалізують відповідні функції.

Спроби застосувати методи математичної лінгвістики до завдання аналізу зображень приводять до необхідності вирішити ряд проблем, пов'язаних з відображенням двовимірної структури зображення на одномірні ланцюжки формальної мови[13].

Екстенсіональні методи

У методах даної групи, на відміну від інтенсіонального напрямку, кожному досліджуваному об'єкту в більшій або меншій мері надається самостійне діагностичне значення. По своїй суті ці методи близькі до клінічного підходу, який розглядає людей не як проранжировану по тому або іншому показнику ланцюжок об'єктів, а як цілісні системи, кожна з яких індивідуальна й має особливу діагностичну цінність [14]. Таке дбайливе відношення до об'єктів дослідження не дозволяє виключати або втрачати інформацію про кожний окремий об'єкт, що відбувається при застосуванні методів інтенсіонального напрямки, що використовують об'єкти тільки для виявлення й фіксації закономірностей поведінки їх атрибутів.

Основними операціями в розпізнаванні образів за допомогою обговорюваних методів є операції визначення подібності й відмінності об'єктів. Об'єкти в зазначеній групі методів відіграють роль діагностичних прецедентів. При цьому залежно від умов конкретного завдання роль окремого прецеденту може мінятися в самих широких межах: від головної й визначальної й до досить непрямої участі в процесі розпізнавання. У свою чергу умови завдання можуть вимагати для успішного рішення участі різної кількості діагностичних прецедентів: від одного в кожному розпізнаваному класі до повного обсягу вибірки, а також різних способів обчислення заходів подібності й відмінності об'єктів. Цими вимогами пояснюється подальший поділ екстенсіональних методів на підкласи:

- метод порівняння із прототипом;
- метод k-найближчих сусідів;
- алгоритми обчислення оцінок ("голосування");
- колективи вирішальних правил.

Метод порівняння із прототипом. Це найбільш простий екстенсіональний метод розпізнавання. Він застосовується, наприклад, тоді, коли розпізнавані класи відображаються в просторі ознак компактними геометричними угрупованнями. У такому випадку звичайно в якості точки – прототипу вибирається центр геометричного угруповання класу (або найближчий до центру об'єкт).

Для класифікації невідомого об'єкта перебуває найближчий до нього прототип, і об'єкт ставиться до того ж класу, що й цей прототип. Очевидно, ніяких узагальнених образів класів у даному методі не формується.

У якості заходу близькості можуть застосовуватися різні типи відстаней. Часто для дихотомічних ознак використовується відстань Хеммінгу, яке в цьому випадку дорівнює квадрату евклідова відстані. При цьому вирішальне правило класифікації об'єктів еквівалентно лінійної вирішальної функції.

Зазначений факт слід особливо зазначити. Він наочно демонструє зв'язок прототипної і ознакової репрезентації інформації про структуру даних. Користуючись наведеною виставою, можна, наприклад, будь-яку традиційну вимірювальну шкалу, що є лінійною функцією від значень дихотомічних ознак, розглядати як гіпотетичний діагностичний прототип. У свою чергу, якщо аналіз просторової структури розпізнаваних класів дозволяє зробити вивід про їхню геометричну компактність, то кожний із цих класів досить замінити одним прототипом який, фактично еквівалентний лінійної діагностичної моделі.

На практиці, звичайно, ситуація часто буває відмінної від описаного ідеалізованого прикладу. Перед дослідником, що наміряються застосувати метод розпізнавання, заснований на порівнянні із прототипами діагностичних класів, встають непрості проблеми. Це, у першу чергу, вибір заходу близькості (метрики), від якого може суттєво змінитися просторова конфігурація розподілу об'єктів. І, по-друге, самостійною проблемою є аналіз багатомірних структур експериментальних даних. Обидві ці проблеми особливо гостро встають перед дослідником в умовах високої розмірності простору ознак, характерної для реальних завдань.

Метод k-найближчих сусідів. Метод k-найближчих сусідів для рішення завдань дискримінантного аналізу був уперше запропонований ще в 1952 році. Він полягає в наступному.

При класифікації невідомого об'єкта перебуває задане число (k) геометрично найближчих до нього в просторі ознак інших об'єктів (найближчих сусідів) із уже відомою приналежністю до розпізнаваних класів. Рішення про віднесення невідомого об'єкта до того або іншому діагностичному класу ухвалюється шляхом аналізу інформації про цю відому приналежність його найближчих сусідів, наприклад, за допомогою простого підрахунку голосів.

Спочатку метод k-найближчих сусідів розглядався як непараметричний метод оцінювання відносини правдоподібності. Для цього методу отримані теоретичні оцінки його ефективності в порівнянні з оптимальним байєсовським класифікатором. Доведене, що асимптотичні ймовірності помилки для методу k-найближчих сусідів перевищують помилки правила Байеса не більш ніж у два рази.

Як відзначалося вище, у реальних завданнях часто доводиться оперувати об'єктами, які описуються більшою кількістю якісних (дихотомічних) ознак. При цьому розмірність простору ознак порівнянна або перевищує обсяг досліджуваної вибірки. У таких умовах зручно інтерпретувати кожний об'єкт навчальної вибірки, як окремий лінійний класифікатор. Тоді той або інший діагностичний клас представляється не одним прототипом, а набором лінійних класифікаторів. Сукупна взаємодія лінійних класифікаторів дає в підсумку кусочно-лінійну поверхню, що розділяє в просторі ознак розпізнавані класи. Вид поділяючої поверхні, що полягає зі шматків гіперплощин, може бути різноманітним і залежить від взаємного розташування класифікуємих сукупностей.

Також можна використовувати іншу інтерпретацію механізмів класифікації за правилом k-найближчих сусідів. У її основі лежить подання про існування деяких латентних змінних, абстрактних або зв'язаних яким-небудь перетворенням з вихідним простором ознак. Якщо в просторі латентних змінних попарні відстані між об'єктами такі ж, як і в просторі вихідних ознак, і кількість цих змінних значне менше числа об'єктів, то інтерпретація методу k-найближчих сусідів може розглядатися під кутом зору порівняння непараметричних оцінок щільностей розподілу умовних ймовірностей. Наведене тут подання про латентні змінні близько по своїй суті до вистави про дійсну розмірність і іншим виставам, використовуваним у різних методах зниження розмірності.

При використанні методу k-найближчих сусідів для розпізнавання образів дослідникові доводиться вирішувати складну проблему вибору метрики для визначення близькості діагностуємих об'єктів. Ця проблема в умовах високої розмірності простору ознак надзвичайно загострюється внаслідок достатньої трудомісткості даного методу, яка стає значимою навіть для високопродуктивних комп'ютерів. Тому тут так само, як і в методі порівняння із прототипом, необхідно вирішувати творче завдання аналізу багатомірної структури експериментальних даних для мінімізації числа об'єктів, що представляють діагностичні класи.

Алгоритми обчислення оцінок (голосування). Принцип дії алгоритмів обчислення оцінок (АОО) полягає в обчисленні пріоритеті (оцінок подібності), що характеризують "близькість" розпізнаваного й еталонних об'єктів по системі ансамблів ознак, що представляє собою систему підмножин заданого безлічі ознак.

На відміну від усіх раніше розглянутих методів алгоритми обчислення оцінок принципово по-новому оперують описами об'єктів. Для цих алгоритмів об'єкти існують одночасно в самих різних підпросторах простору ознак. Клас АОО доводить ідею використання ознак до логічного кінця: оскільки не завжди відомо, які комбінації ознак найбільш інформативні, то в АОО ступінь подібності об'єктів обчислюється при зіставленні всіх можливих або певних комбінацій ознак, що входять в описи об'єктів [9].

Колективи вирішальних правил. У вирішальному правилі застосовується дворівнева схема розпізнавання. На першому рівні працюють приватні алгоритми розпізнавання, результати яких поєднуються на другому рівні в блоці синтезу. Найпоширеніші способи такого об'єднання засновані на виділенні областей компетентності того або іншого приватного алгоритму. Найпростіший спосіб знаходження областей компетентності полягає в апріорній розбивці простору ознак виходячи із професійних міркувань конкретної науки (наприклад, розшарування вибірки за деякою ознакою). Тоді для кожної з виділених областей будується власний алгоритм, що розпізнає. Інший спосіб базується на застосуванні формального аналізу для визначення локальних областей простору ознак як околиць розпізнаваних об'єктів, для яких доведена успішність роботи якого-небудь приватного алгоритму розпізнавання.

Самий загальний підхід до побудови блоку синтезу розглядає результуючі показники приватних алгоритмів як вихідні ознаки для побудови нового узагальненого вирішального правила. У цьому випадку можуть використовуватися всі перераховані вище методи інтенсіонального й екстенсіонального напрямків у розпізнаванні образів. Ефективними для рішення завдання створення колективу вирішальних правил є логічні алгоритми типу "Кора" і алгоритми обчислення оцінок (АОО), покладені в основу так званого алгебраїчного підходу, що забезпечує дослідження й конструктивний опис алгоритмів розпізнавання, у рамки якого укладаються всі існуючі типи алгоритмів [9].

Нейромережеві методи

Нейромережеві методи – це методи, що базуються на застосуванні різних типів нейронних мереж (НМ). Основні напрямки застосування різних НМ для розпізнавання образів і зображень [1]:

– застосування для добування ключових характеристик або ознак заданих образів;
– класифікація самих образів або вже витягнутих з них характеристик (у першому випадку добування ключових характеристик відбувається неявно усередині мережі);
– рішення оптимізаційних завдань.

Багатошарові нейронні мережі. Архітектура багатошарової нейронної мережі (БНМ) складається з послідовно з'єднаних шарів, де нейрон кожного шару своїми входами зв'язаний з усіма нейронами попереднього шару, а виходами – наступного.

Найпростіше застосування одношарової НМ (називаної автоасоціативною пам'яттю) полягає в навчанні мережі відновлювати подавані зображення. Подаючи на вхід тестове зображення й обчислюючи якість реконструйованого зображення, можна оцінити наскільки мережа розпізнала вхідне зображення. Позитивні властивості цього методу полягають у

тому, що мережа може відновлювати перекручені й зашумленні зображення, але для більш серйозних цілей він не підходить.

БНМ так само використовується для безпосередньої класифікації зображень – на вхід подається або саме зображення в якому-небудь виді, або набір раніше витягнутих ключових характеристик зображення, на виході нейрон з максимальною активністю вказує приналежність до розпізнаного класу. Якщо ця активність нижче деякого порога, то вважається, що поданий образ не ставиться до жодного з відомих класів. Процес навчання встановлює відповідність подаваних на вхід образів із приналежністю до певного класу. Це називається навчанням із вчителем [14]. Такий підхід гарний для завдань контролю доступу невеликої групи осіб. Такий підхід забезпечує безпосереднє порівняння мережею самих образів, але зі збільшенням числа класів час навчання й роботи мережі зростає експоненційно. Тому для таких завдань, як пошук схожої людини у великій базі даних, вимагає добування компактного набору ключових характеристик, на основі яких можна робити пошук.

Підхід до класифікації з використанням частотних характеристик усього зображення, описаний в [15]. Застосовувалася одношарова НМ, заснована на багатозначних нейронах.

В [16] показане застосування НМ для класифікації зображень, коли на вхід мережі надходять результати декомпозиції зображення по методу головних компонентів.

У класичній БНМ міжшарові нейронні з'єднання повнозв’язні, і зображення представлене у вигляді одномірного вектора, хоча воно двумерно. Архітектура згорткової НМ [20] спрямована на подолання цих недоліків. У ній використовувалися локальні рецепторні поля (забезпечують локальну двовимірну зв’язність нейронів), загальні ваги (забезпечують детектування деяких ознак у будь-якому місці зображення) і ієрархічна організація із просторовими підвиборками (spatial subsampling). Згорткова НМ (ЗНМ) забезпечує часткову стійкість до змін масштабу, зсувам, поворотам, викривленням.

БНМ застосовуються й для виявлення об'єктів певного типу. Крім того, що будь-яка навчена БНМ у деякій мері може визначати приналежність образів до “своїх” класів, її можна спеціально навчити надійному детектуванню певних класів. У цьому випадку вихідними класами будуть класи приналежні й не приналежні до заданого типу образів. В [22] застосовувався нейромережевий детектор для виявлення зображення особи у вхідному зображенні. Зображення сканувалося вікном 20x20 пікселів, яке подавалося на вхід мережі, що вирішує чи належить дана ділянка до класу осіб. Навчання проводилося як з використанням позитивних прикладів (різних зображень осіб), так і негативних (зображень, що не є особами). Для підвищення надійності детектування використовувався колектив НМ, навчених з різними початковими вагами, внаслідок чого НМ помилялися по різному, а остаточний рішення ухвалювався голосуванням усього колективу.

НМ застосовується так само для добування ключових характеристик зображення, які потім використовуються для наступної класифікації. В [17,23], показаний спосіб нейромережевої реалізації методу аналізу головних компонентів. Суть методу аналізу головних компонентів полягає в одержанні максимально декорельованих коефіцієнтів, що характеризують вхідні образи. Ці коефіцієнти називаються головними компонентами й використовуються для статистичного стиску зображень, у якому невелике число коефіцієнтів використовується для вистави всього образа. НМ із одним схованим шаром утримуючим N нейронів (яке багато менше ніж розмірність зображення), навчена по методу зворотного поширення помилки відновлювати на виході зображення, подане на вхід, формує на виході схованих нейронів коефіцієнти перших N головних компонентів, які й використовуються для порівняння. Звичайно використовується від 10 до 200 головних компонентів. Зі збільшенням номера компоненти її репрезентативність сильно знижується, і використовувати компоненти з більшими номерами не має змісту. При використанні нелінійних активаційних функцій нейронних елементів можлива нелінійна декомпозиція на головні компоненти. Нелінійність дозволяє більш точно відбити варіації вхідних даних.

Застосовуючи аналіз головних компонентів до декомпозиції зображень осіб, одержимо головні компоненти, називані власними особами [23], яким так само притаманно корисна властивість – існують компоненти, які в основному відбивають такі істотні характеристики особи як стать, раса, емоції. При відновленні компонента мають вигляд, схожий на особу, причому перші відбивають найбільш загальну форму особи, останні – різні дрібні відмінності між особами (мал. 5). Такий метод добре застосуємо для пошуку схожих зображень осіб у більших базах даних. Показана так само можливість подальшого зменшення розмірності головних компонентів за допомогою НМ [23]. Оцінюючи якість реконструкції вхідного зображення можна дуже точно визначати його приналежність до класу осіб.

Нейронні мережі високого порядку. Нейронні мережі високого порядку (НМВП) відрізняються від БНМ тим, що в них тільки один шар, але на входи нейронів надходять так само терми високого порядку, що є добутком двох або більш компонент вхідного вектора [17]. Такі мережі так само можуть формувати складні поділяючі поверхні.

Нейронні мережі Хопфилда. НМ Хопфилда (НМХ) є одношаровою й повнозв’язной (зв'язки нейронів на самі себе відсутні), її виходи зв'язані із входами. На відміну від БНМ, НМХ є релаксаційной – тобто будучи встановленою в початковий стан, функціонує доти, поки не досягне стабільного стану, який і буде її вихідним значенням. Для пошуку глобального мінімуму стосовно до оптимізаційним завданням використовують стохастичні модифікації НМХ [17].

Застосування НМХ у якості асоціативної пам'яті дозволяє точно відновлювати образи, яким мережа навчена, при подачі на вхід перекрученого образа. При цьому мережа “згадає” найбільш близький (у змісті локального мінімуму енергії) образ, і в такий спосіб розпізнає його. Таке функціонування так само можна представити як послідовне застосування автоассоціативної пам'яті, описаної вище. На відміну від автоассоціативної пам'яті НМХ ідеально точно відновить образ. Для запобігання інтерференційних мінімумів і підвищення ємності мережі використовують різні методи [17,18].

Нейроні мережі, які самоорганзуються Кохонена (НМСК) забезпечують топологічне упорядкування вхідного. Вони дозволяють топологічно безупинно відображати вхідне n-мірний простір у вихідне m-мірне, mn. Вхідний образ проектується на деяку позицію в мережі, кодуєму як положення активованого вузла. На відміну від більшості інших методів класифікації й кластеризації, топологічне впорядковувані класів зберігає на виході подобу у вхідних образах [19,20], що є особливо корисним при класифікації даних, що мають велику кількість класів.

Когнитрон. Когнитрон [21] своєю архітектурою схожий на будову зорової кори, має ієрархічну багатошарову організацію, у якій нейрони між шарами зв'язані тільки локально. Навчається конкурентним навчанням (без вчителя). Кожний шар мозку реалізує різні рівні узагальнення; вхідний шар чутливий до простих образів, таким, як лінії, і їх орієнтації в певних областях візуальної області, у той час як реакція інших шарів є більш складною, абстрактною й незалежною від позиції образа. Аналогічні функції реалізовані в когнитроні шляхом моделювання організації зорової кори.

Неокогнитрон [21] є подальшим розвитком ідеї когнитрона й більш точно відбиває будова зорової системи, дозволяє розпізнавати образи незалежно від їхніх перетворень, обертань, викривлень і змін масштабу.

Когнитрон є потужним засобом розпізнавання зображень, однак вимагає високих обчислювальних витрат, які на сьогоднішній день недосяжні [21].

Розглянуті нейромережеві методи забезпечують швидке й надійне розпізнавання зображень, але при використанні цих методів виникають проблеми розпізнавання тривимірних об'єктів. Проте, даний підхід має масу переваг.

У цей час існує досить велика кількість систем автоматичного розпізнавання образів для різних прикладних завдань.

Розпізнавання образів формальними методами як фундаментальний науковий напрямок є невичерпним.

Математичні методи обробки зображень мають найрізноманітніші застосування: наука, техніка, медицина, соціальна сфера. Надалі роль розпізнавання образів у житті людини буде зростати ще більше.

Нейромережеві методи забезпечують швидке й надійне розпізнавання зображень. Даний підхід має масу переваг і є одним з найбільш перспективних.

Традиційно, для пошуку зображень використовують їх текстові характеристики: ім'я файлу, заголовок, ключові слова тощо. Однак такий підхід має ряд недоліків. Перш за все необхідне втручання людини для опису вмісту зображень у відповідності до обраного набору підписів та ключових слів. У більшості випадків зображення містить декілька об'єктів, кожен з яких має свій набір атрибутів. Крім цього, потрібно описати просторові відношення між цими об'єктами, щоб зрозуміти його зміст. Оскільки розміри баз даних зображень зростають, використання ключових слів стає не тільки складним але і недостатнім для представлення зображення. Інша проблема даного підходу полягає у неадекватності єдиного текстового опису зображення. Як результат є необхідність для автоматизованого отримання примітивних властивостей зображень і пошук зображень на основі цих властивостей. Для великої бази даних із понад десятками тисяч образів ефективна індексація є важливим інструментом в AR/VR/MR-системах. Успішна класифікація зображень зменшує час опрацювання зображень фільтруванням зайвих класів образів під час пошуку подібних до них.

Принцип роботи AR/VR/MR-системи

Сучасні AR/VR/MR-системи працюють у два етапи: Індексування та Пошук. На етапі індексування кожний образ у базі даних представляється вектором властивостей. Існуючі універсальні системи AR/VR/MR відносять до однієї із трьох категорій залежно від підходу отримання властивостей образу: гістограма, кольорове розташування і пошук за регіонами. Такими властивостями, зокрема, є: колір, форма, структура і розташування. Отримані властивості зберігаються в окремій базі даних візуальних властивостей. На етапі пошуку обчислюються властивості із образу-запиту користувача. Використовуючи критерії подібності, отриманий вектор властивостей порівнюється з векторами у базі даних візуальних властивостей. Користувач у відповідь отримує образи, які максимально відповідають запиту. Системи пошуку за регіонами використовують локальні властивості регіонів (ідеальних об'єктів) у протилежність глобальним властивостям повного зображення. Якщо об'єкти в межах зображення сегментовані і кожна властивість об'єкту отримана автоматично, то такі особливості роблять можливу систему пошуку зображень за регіонами. Представлення візуального образу адекватним числом кластерів (об'єкти у зображенні) може краще відобразити його вміст, однак цей підхід є часозалежним.

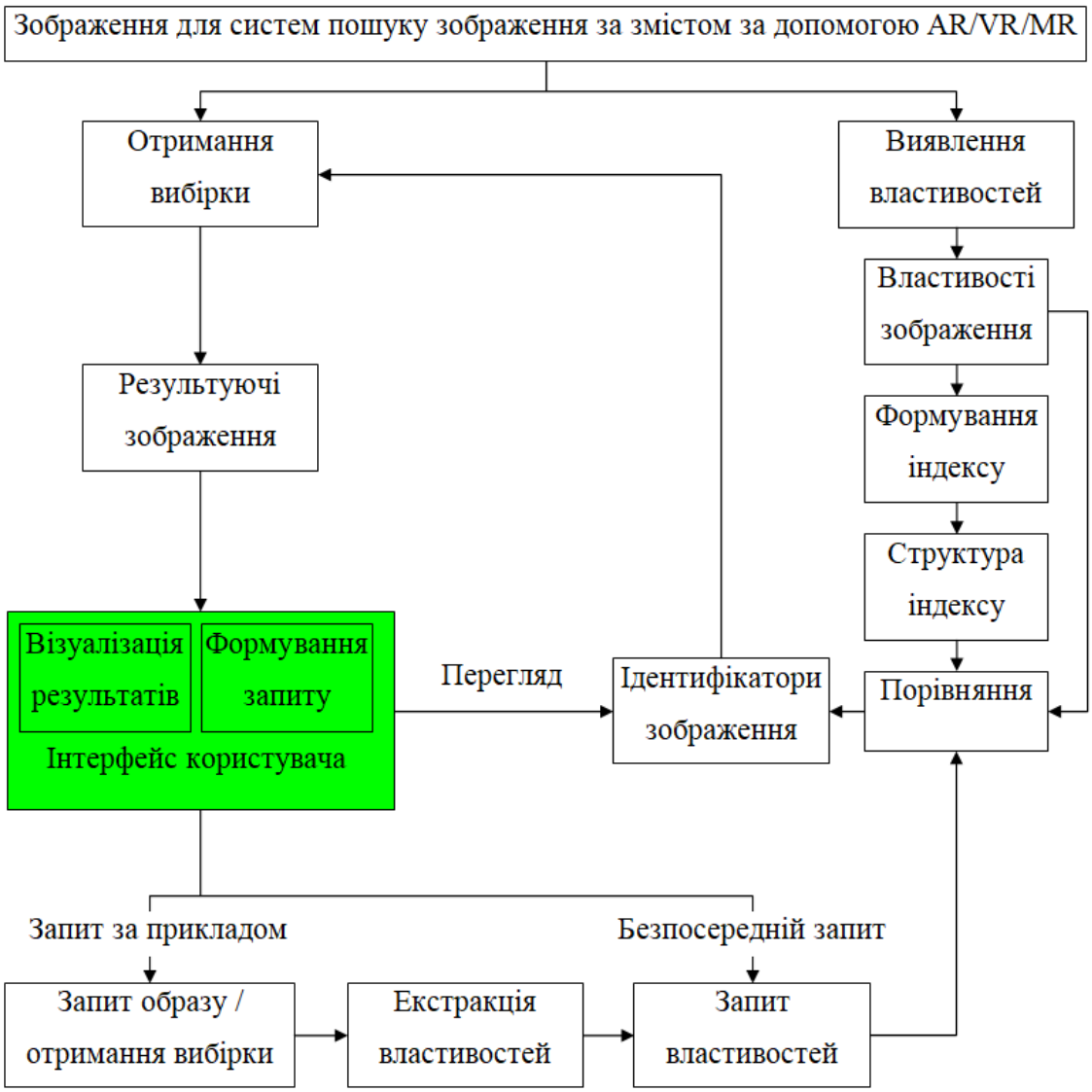


Рисунок 1 – Структурна схема системи

Інтерфейс користувача (UI, User Interface), як правило, складається з двох частин: формування запиту і візуалізація результатів виконання запиту. Більшість AR/VR/MR-систем є результатами досліджень, і підкреслюють один з аспектів пошуку на основі вмісту. Іноді це можливість представлення результатів у вигляді ескізів у користувальницькому інтерфейсі, іноді це використання нової структури даних для індексування. Деякі системи існують у дослідницьких, комерційних версіях та версіях для виробництва. Комерційні версії, як правило, володіють більш стандартними пошуковими можливостями.

Деякі системи надають користувачеві інтерфейс, який дозволяє більш гнучко формулювати запити. Чим простіше властивість може бути отримана із зображення, тим легше її впровадити в систему, і тим легше використовувати цю властивість. Наприклад, властивості кольору для пошуку образів здебільшого ефективні, оскільки їх не важко отримати і впровадити в систему. Однак, властивості форми, які є стійкіші до шуму, беруть активнішу участь у AR/VR/MR-системах. Як результат, використовуються дуже прості функції, які часто є малоефективними. Більшість систем використовують ознаки кольору і текстури, меншість – ознаки форми та розташування. Результатом пошуку за кольором зазвичай є зображення зі схожими кольорами. Результатом пошуку за текстурою не завжди є зображення із подібною текстурою, якщо база даних містить багато зображень із домінуючими текстурами. Результати пошуку за формою часто є несподіваними. Тому вони не є найбільш ефективними властивостями.

Методи опису характеристик

Тут представлені найбільш загальні методи опису характеристик зображень, що використовуються для подальшого порівняння їх між собою. Всі вони є потенційно широко застосовними, тобто не специфічними для будь-якого особливого підкласу систем.

Форма

Опис форми передбачає опис геометричної форми окремих фрагментів зображення. Для її визначення до фрагмент спочатку застосовують сегментацію або Виділення контурів зображення. Існують і інші способи, наприклад фільтрація форм. Часто визначення форми вимагає втручання людини, тому що методи типу сегментації складно повністю автоматизувати для широкого класу задач.

Програмні системи та алгоритми

Попри те, що існує безліч програмних комплексів з пошуку зображень в базах даних, проблема пошуку на основі піксельного змісту в більшості ситуацій поки не має ефективного реалізованого рішення.

Способи побудови запитів

Різні реалізації систем пошуку зображень за змістом працюють з наступними типами користувальницьких запитів:

Запит за шаблоном

Передбачається, що система робить пошук на основі вхідного зображення, поданого користувачем. Алгоритми, що лежать в основі системи, можуть мати різні способи опису та роботи з вхідним зображенням, але всі результати пошуку повинні мати спільні характеристики із вхідним зображенням, що подавалося користувачем.

Користувач може подати на вхід як існуюче зображення, так і грубий начерк необхідного результату (розмітку на кольорові області або прості геометричні форми).

При даному способі побудови запитів не виникає труднощів, пов'язаних з описом зображення за допомогою слів.

Розпізнавання семантики запиту

В ідеалі система пошуку повинна вміти обробляти запити користувача, сформульовані у вільній формі, наприклад «знайти фотографії собак» або навіть «знайти портрети людини». Запити такого типу дуже складні для обробки комп'ютером, адже фотографії лабрадора і карликового пуделя сильно різняться, а людина не завжди дивиться в камеру в однаковій позі. У цей час багато систем використовують для класифікації характеристики нижчого рівня, такі як колір, текстура і форма об’єкту, хоча існують і системи, в основному засновані на диференціації критеріїв високого рівня (див. Теорія розпізнавання образів). Більшість систем не є широко орієнтованими. Наприклад, системи пошуку зображень, згенерованих на комп'ютері, з успіхом обходяться характеристиками, основаними на поєднанні форм та градієнтів.

Колір

Пошук зображень за допомогою порівняння колірних складових проводиться за допомогою побудови Гістограми кольору їх розподілу. У цей час ведуться дослідження з побудови опису, в якому зображення ділиться на регіони за схожими колірним характеристикам, і далі враховується їх взаємне розташування. Опис зображень за допомогою кольорів, з яких воно складається, є найбільш поширеним, оскільки воно не залежить від розміру або орієнтації зображення. Побудова гістограм з наступним їх порівнянням використовується найбільш часто, але не є єдиним способом опису колірних характеристик.

Текстура

Методи такого опису працюють з порівнянням текстурних зразків, присутніх на зображенні, і їх взаємного розташування. Для визначення текстури використовують текселі, які об'єднують в множини. Вони містять не тільки інформацію, що описує текстуру, а й її місце розташування на описуваному зображенні. Текстуру як сутність складно формалізовано описати, і зазвичай її представляють у вигляді двомірного масиву зміни

яскравості. Також в опис іноді включають міру контрастності, спрямованості градієнту та регулярності. Існує проблема порівняння коваріації пікселів з метою віднесення текстури до певного класу (наприклад, «гладка» або «груба»).

Інші способи

Ця категорія включає в себе такі форми запитів, як визначення категорії в запропонованій ієрархії, запит у вигляді частини зображення, очікуваного як результат, розширення запиту додатковими зображеннями, задання графічного шаблону, що складається зі складних форм, а також комбінацію методів.

Також можливе поступове уточнення запиту, коли користувач в процесі роботи системи пошуку позначає проміжні результати як «підходящі» або «незадовільні», і система продовжує працювати з уточненим запитом.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів пошуку зображення за змістом за допомогою AR/VR/MR. В межах України в недостатній мірі представлені вітчизняні розробки в цій області. У роботі наведені теоретичне узагальнення й рішення наукового завдання дослідження методів пошуку зображення за змістом за допомогою AR/VR/MR. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем пошуку зображення за змістом за допомогою AR/VR/MR; Досліджена система пошуку зображення за змістом за допомогою AR/VR/MR; На основі отриманих результатів досліджень створена програмна реалізація системи пошуку зображення за змістом за допомогою AR/VR/MR. Розроблені під час виконання роботи алгоритми дозволяють успішно вирішувати завдання пошуку зображення за змістом за допомогою AR/VR/MR. 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. Смірнова Т.В. Дослідження та програмна реалізація системи пошуку зображення за змістом за допомогою AR/VR/MR // Збірник праць молодих науковців ЦНТУ. – Вип. 11. – Кропивницький: ЦНТУ, 2021.
2. Кузин Л.Т. Основы кибернетики: Основы кибернетических моделей. Т.2. – М.: Энергия, 1979. – 584с.
3. Перегудов Ф.И., Тарасенко Ф.П. Введение в системный анализ: Учебное пособие. – М.: Высшая школа, 1997. – 389с.
4. Темников Ф.Е., Афонин В.А., Дмитриев В.И. Теоретические основы информационной техники. – М.: Энергия, 1979. – 511с.
5. Ту Дж., Гонсалес Р. Принципы распознавания образов. /Пер. с англ. – М.: Мир, 1978. – 410с.
6. Уинстон П. Искусственный интеллект. /Пер. с англ. – М.: Мир, 1980. – 520с.
7. Фу К. Структурные методы в распознавании образов: Пер.с англ. – М.: Мир, 1977. – 320с.
8. Цыпкин Я.З. Основы информационной теории идентификации. – М.: Наука, 1984. – 520с.
9. Поспелов Г.С. Искусственный интеллект – основа новой информационной технологии. – М.: Наука, 1988. – 280с.
10. Ю. Лифшиц, Статистические методы распознавания образов ///modern/07modernnote.pdf
11. Бор Н. Атомная физика и человеческое познание. /Пер.с англ. – М.: Мир, 1961. – 151с.
12. Бутаков Е.А., Островский В.И., Фадеев И.Л. Обработка изображений на ЭВМ.1987.-236с.
13. Дуда Р., Харт П. Распознавание образов и анализ сцен. /Пер.с англ. – М.: Мир, 1978. – 510с.
14. Дюк В.А. Компьютерная психодиагностика. – СПб: Братство, 1994. – 365с.
15. Aizenberg I. N., Aizenberg N. N. and Krivosheev G.A. Multi-valued and Universal Binary Neurons: Learning Algorithms, Applications to Image Processing and Recognition. Lecture Notes in Artificial Intelligence – Machine Learning and Data Mining in Pattern Recognition, 1999, pp. 21-35.
16. Ranganath S. and Arun K. Face recognition using transform features and neural networks. Pattern Recognition 1997, Vol. 30, pp. 1615-1622.
17. Головко В.А. Нейроинтеллект: Теория и применения. Книга 1. Организация и обучение нейронных сетей с прямыми и обратными связями – Брест:БПИ, 1999, – 260с.
18. Vetter T. and Poggio T. Linear Object Classes and Image Synthesis From a Single Example Image. IEEE Transactions on Pattern Analysis and Machine Intelligence 1997, Vol. 19, pp. 733-742.
19. Головко В.А. Нейроинтеллект: Теория и применения. Книга 2. Самоорганизация, отказоустойчивость и применение нейронных сетей – Брест:БПИ, 1999, – 228с.

20. Lawrence S., Giles C. L., Tsoi A. C. and Back A. D. Face Recognition: A Convolutional Neural Network Approach. IEEE Transactions on Neural Networks, Special Issue on Neural Networks and Pattern Recognition, pp. 1-24.
21. Уоссермен Ф. Нейрокомпьютерная техника: Теория и практика, 1992 – 184с.
22. Rowley H. A., Baluja S. and Kanade T. Neural Network-Based Face Detection. IEEE Transactions on Pattern Analysis and Machine Intelligence 1998, Vol. 20, pp. 23-37.
23. Valentin D., Abdi H., O'Toole A. J. and Cottrell G. W. Connectionist models of face processing: a survey. IN: Pattern Recognition 1994, Vol. 27, pp. 1209-1230.
24. Барабаш Ю.Л. Коллективные статистические решения при распознавании. – М.: Радио и связь, 1983. – 224с.
25. Васильев В.И. Распознающие системы: Справочник. – К.: Наукова думка, 1983. – 230с.

УДК 004

Є. Смоляр, магістр гр. КІ-19М-1,4
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ УПРАВЛІННЯ ІНФРАСТРУКТУРОЮ НА ОСНОВІ РІШЕНЬ SD-WAN

У статті розроблено програмне забезпечення, яке призначено для системи управління інфраструктурою на основі рішень SD-WAN. Метою розробки є дослідження та програмна реалізація системи управління інфраструктурою на основі рішень SD-WAN. Об’єктом дослідження є процес управління інфраструктурою на основі рішень SD-WAN. Предметом дослідження є методи управління інфраструктурою на основі рішень SD-WAN. Методи дослідження базуються на методах теорії телетрафіку, методах математичної статистики, методах розробки програмного забезпечення. 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 інфраструктурою, SD-WAN

Постановка проблеми. На сучасному рівні існує кілька тенденцій, що визначають нові вимоги до організації територіально розподілених мереж (WAN). Одна з них – перехід до гібридних IT-середовищ, коли необхідні для роботи додатків ресурси можуть перебувати на віддалених площадках, включаючи власні ЦОДи замовника, приватні хмари в комерційних ЦОДах і публічні хмари. При цьому необхідно забезпечити оперативне підключення нових мережних сервісів і нових вузлів (філій), що вкрай складно зробити на основі традиційних технологій WAN. Тому все частіше замовники звертаються до програмно обумовлених рішень SD-WAN, у яких мережна взаємодія підкоряється вимогам з боку додатків.

У пропонованого SD-WAN-рішення є ряд унікальних особливостей. Зокрема, ця наявність конвергентного пристрою SD, що сполучить функції шлюзу SD-WAN і WAN-оптимізатора. Шлюзи SD-WAN мають убудовану функціональність міжмережевого екрана й захисту від погроз. Ще одна цікава особливість рішення – можливість об'єднання в програмно обумовленій мережі як WAN-, так і LAN-складових, до останнього ставляться комутатори локальної мережі й точки доступу Wi-Fi. Істотне посилення своєї пропозиції в частині побудови локальних мереж вийшло завдяки використанню унікальних масивів, що містять кілька точок доступу із секторними антенами й убудованим контролером. Такий масив може обслуговувати тисячі користувачів і дуже ефективний там, де необхідні рішення високої щільності. Продукт, крім відмінної масштабованості, відрізняються ще гнучким вибором моделей впровадження: так, система керування може бути розміщена в приватній або публічній хмарі.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-15] було виявлено певні прогалини у забезпеченні системи управління інфраструктурою на основі рішень SD-WAN.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи управління інфраструктурою на основі рішень SD-WAN.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем управління інфраструктурою на основі рішень SD-WAN.
– Дослідження системи управління інфраструктурою на основі рішень SD-WAN.
– Програмна реалізація системи управління інфраструктурою на основі рішень SD-WAN.

Об'єктом дослідження є процес управління інфраструктурою на основі рішень SD-WAN.

Предметом дослідження є методи управління інфраструктурою на основі рішень SD-WAN.

Методи дослідження базуються на методах теорії телетрафіку, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Мережі SD-WAN приходять на зміну застаріваючим традиційним територіально розподіленим мережам, як колись смартфони потіснили звичайні мобільники. Відповідно до досліджень Gartner, більше 36% великих компаній планують почати користуватися SD-WAN до кінця 2019 року. І щороку кількість мереж SD-WAN буде рости в середньому на 65%.

Рішення SD-WAN – це перший великий крок у реалізації концепції програмно обумовлених мереж SDN стосовно до територіально розподілених мереж. Ідея програмувальних мереж (Software-Defined Network, SDN) полягає в тому, що функції контролю й керування виконуються не безліччю мережних пристроїв, а контролером SD-WAN.

SD-WAN дозволяє відмовитися від складного керування кожним мережним пристроєм за допомогою командного рядка (Command Line Interface, CLI) на користь централізованого: контролер SD-WAN розсилає налаштування всім пристроям за допомогою спеціального протоколу (SNMP, NETCONF і т.п.) і відслідковує стан маршрутизаторів і каналів зв'язку.

Чим це зручно?

Сучасні маршрутизатори мають багату функціональність (яка, до речі, багато в чому визначає їхню чималу вартість). От тільки використовувати більшість функцій, як правило, не вдається: чим масштабніше мережа, чим більше різних вузлів, тим складніше конфігурація мережного встаткування й забезпечення її погодженості. Звідси природно випливають два емпіричних факти: чим більше вузлів, тим простіше налаштування; чим складніше налаштування, тим рідше вони міняються.

У той же час гнучка адаптація мережі, необхідна для підтримки різноманітних сервісів, вимагає як складних налаштувань, так і швидкої їхньої зміни.

Представте, що великої організації треба провести важливу нараду керівників всіх філій по відео-конференц-зв'язку. На кілька годин потрібно надати максимальний пріоритет і гарантувати пропускну здатність у каналах, достатню для трафіку реального часу.

Або представте: у тієї ж організації наступає сезон звітів, коли відповідальні підрозділи з філій завантажують на центральні сервери величезні файли даних. У цьому випадку потрібно виділити необхідну смугу й забезпечити мінімум втрат для трафіку відповідних додатків.

Але чи багато мережних адміністраторів зважаться внести тимчасові зміни в конфігурацію, якщо мова йде про десятки або навіть сотні пристроїв? Контролер SD-WAN дозволяє легко створювати налаштування маршрутизаторів будь-якої складності поза залежністю від масштабів мережі, а міняти їх можна дуже просто й швидко відповідно до поточних потреб.

Щоб виконати завдання, описані вище, адміністраторові мережі SD-WAN досить заздалегідь створити відповідні профілі якості обслуговування з використанням зручного графічного інтерфейсу. При необхідності він може застосувати їх до всіх потрібних пристроїв натисканням однієї кнопки. Контролер SD-WAN переведе дані із шаблонів на мову зрозумілих мережним пристроям команд, відправить ці налаштування на маршрутизатори, забезпечить їхня несуперечність і сумісність із іншими налаштуваннями – як даного маршрутизатора, так і інших пристроїв у мережі.

Страховка від помилок

Від мережних інженерів, що вперше почули про SD-WAN, часто доводиться чути саме це питання: що відбудеться, якщо при налаштуванні маршрутизатора через контролер SD-WAN буде допущена помилка?

При налаштуванні мережних пристроїв через інтерфейс командного рядка ймовірність помилки була досить велика. Так, конфігураційний файл граничного маршрутизатора може містити більше 1000 команд, тому при зміні його «вручну» є щонайменше 1000 шансів помилитися.

Звичайно, не всі помилки приведуть до втрати зв'язку, але помилки в налаштуваннях QoS, маршрутизації й політик інформаційної безпеки можуть дорого обійтися.

Використання в контролері SD-WAN зручного графічного інтерфейсу й шаблонів дозволяє звести ймовірність погрішностей до мінімуму.

Наприклад, для описаних вище сценаріїв з виділенням необхідної смуги певному типу трафіку вводити десятки рядків команд уже не знадобиться – досить вибрати зі списку потрібний додаток і вказати бажану пропускну здатність. Застосування команд і контроль за їх согласованістю на всіх мережних пристроях візьме на себе інтелектуальна функція контролера.

З якими типами каналів може працювати SD-WAN?

У концепцію SD-WAN споконвічно була закладена підтримка будь-яких каналів: L3VPN, Інтернет, LTE і ін.

По-перше, це зручно з погляду моніторингу: адміністратор мережі бачить на панелі управління контролера актуальний стан всіх каналів поза залежністю від їхнього типу. Але ця не найбільша перевага.

Вартість каналів Інтернету постійно знижується, а доступна смуга пропущення збільшується. Зараз за ту ж ціну можна орендувати канал із пропускною здатністю в 10 разів більше, ніж 10 років тому, і найчастіше по якості він не буде уступати виділеному L3VPN,

для якого оператор надає гарантований рівень обслуговування.

Тому з появою SD-WAN стали можливі відмова від оренди дорогих каналів L3VPN і використання каналів Інтернету від різних провайдерів зі збереженням необхідної якості обслуговування. Це й відображено на структурній схемі системи.

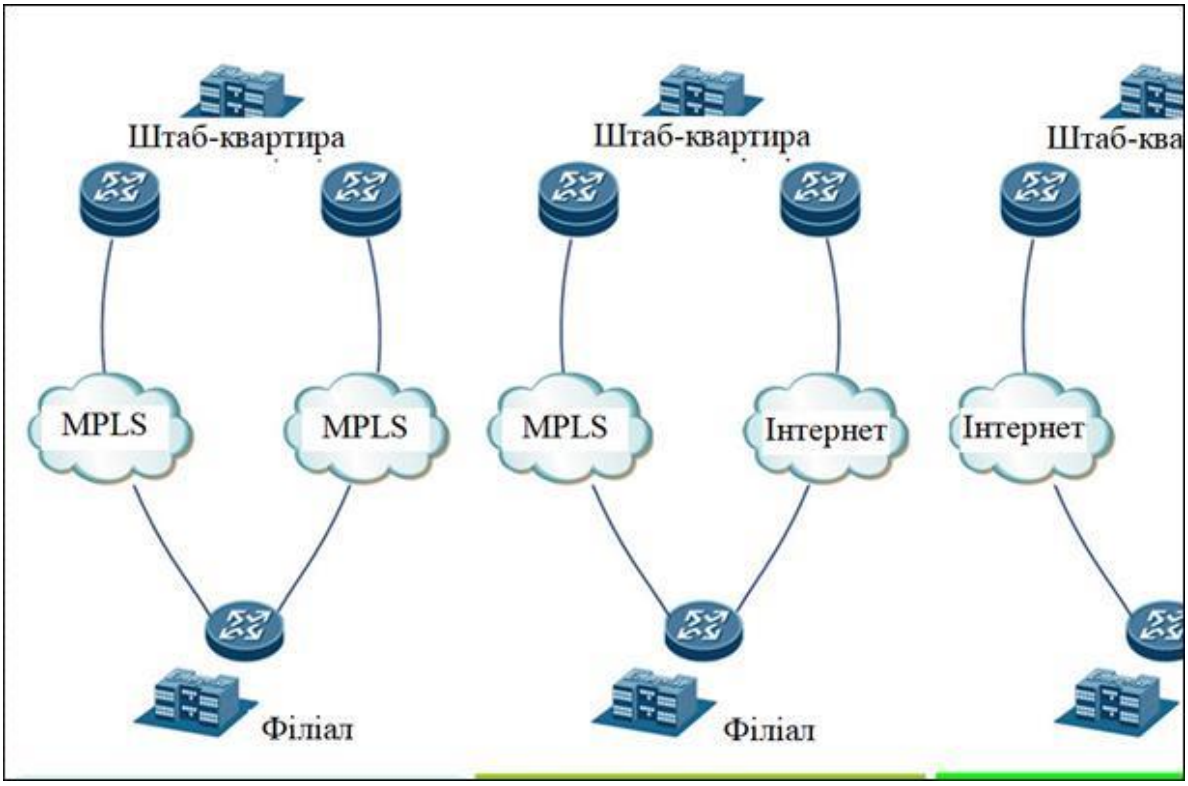


Рисунок 1 – Структурна схема системи

Мережа SD-WAN постійно відслідковує стан всіх каналів по різних параметрах і перемикає трафік критичних додатків з каналу на канал, якщо якість зв'язку виявляється нижче заданого порога.

Тому що на структурній схемі присутня MPLS, приведемо його опис.

MPLS

MPLS (англ. multiprotocol label switching – багатопротокольна комутація по мітках) – механізм у високопродуктивній телекомунікаційній мережі, що здійснює передачу даних від одного вузла мережі до іншого за допомогою міток.

MPLS є масштабованим і незалежним від яких-небудь протоколів механізмом передачі даних. У мережі, заснованої на MPLS, пакетам даних привласнюються мітки. Рішення про подальшу передачу пакета даних іншому вузлу мережі здійснюється тільки на підставі значення привласненої мітки без необхідності вивчення самого пакета даних. За рахунок цього можливе створення наскрізного віртуального каналу, незалежного від середовища передачі й протокол, що використовує будь-який, передачі даних.

В 1996 році група інженерів з фірми «Ipsilon Networks» розробила «Протокол керування потоком» (англ. flow management protocol; RFC 1953) [1].

Заснована на цьому протоколі технологія «комутації IP-пакетів» (англ. IP switching), що працює тільки поверх спрощеної мережі ATM, не одержала комерційного успіху. Фірма «Cisco Systems» розробила схожу технологію «комутації на основі тегів» (англ. tagswitching), не обмежену передачею поверх мережі ATM [2].

Дана технологія, згодом перейменована в «комутацію на основі міток» (англ. label switching), була закритою розробкою фірми «Cisco». Пізніше вона була передана в спеціальну комісію інтернет-розробок (IETF) для відкритієї стандартизації.

Перевага

MPLS дозволяє досить легко створювати віртуальні канали між вузлами мережі.

Технологія дозволяє інкапсулювати різні протоколи передачі даних.

Основною перевагою MPLS є

– незалежність від особливостей технологій канального рівня, таких як ATM, Frame Relay, SONET/SDH або Ethernet;

– відсутність необхідності підтримки декількох мереж другого рівня, необхідних для передачі різного роду трафіку. По виду комутації MPLS ставиться до мереж з комутацією пакетів.

Технологія MPLS була розроблена для організації єдиного протоколу передачі даних як для додатків з комутацією каналів, так і додатків з комутацією пакетів(маються на увазі додатки з датаграмною передачею пакетів). MPLS може бути використаний для передачі різного виду трафіку, включаючи IP-пакети, осередки ATM, фрейми SONET/SDH [3] і кадри Ethernet.

Для рішення ідентичних завдань раніше були розроблені такі технології, як Frame Relay та ATM. Багато інженерів уважали, що технологія ATM буде замінена іншими протоколами з меншими накладними витратами на передачу даних і при цьому буде забезпечувати передачу пакетів даних змінної довжини із установленням з'єднання між вузлами мережі. Технологія MPLS розроблялася з обліком сильних і слабких сторін ATM. У цей час устаткування з підтримкою MPLS заміняє на ринку встаткування з підтримкою вищезгаданих технологій. Імовірно, що в майбутньому MPLS повністю витисне дані технології [4].

Зокрема, MPLS обходиться без комутації осередків і набору сигнальних протоколів, характерних для ATM. При розробці MPLS прийшло розуміння того, що на рівні ядра сучасної мережі немає необхідності в осередках ATM маленького фіксованого розміру, оскільки сучасні оптичні мережі мають таку велику швидкість передачі даних [5], що навіть пакет даних максимальної довжини в 1500 байт випробовує незначну затримку в чергах буферів комутаційного встаткування (необхідність скорочення таких затримок, наприклад, для забезпечення заданої якості голосового трафіку, вплинула на вибір осередків малого розміру, характерних для ATM).

У той же час в MPLS спробували зберегти механізми оптимізації й керування трафіком (англ. teletraffic engineering) і керування окремо від переданого потоку даних, які зробили технології Frame relay і ATM привабливими для впровадження в більших мережах передачі даних.

Незважаючи на те, що перехід на MPLS дає переваги керування потоками даних (поліпшення надійності й підвищення продуктивності мережі), існує проблема втрати контролю потоків даних, що проходять через мережу MPLS, з боку звичайних IP-додатків [6].

Принцип роботи

Технологія MPLS заснована на обробці заголовка MPLS, що додається до кожного пакета даних. Заголовок MPLS може складатися з однієї або декількох «міток». Кілька записів (міток) у заголовку MPLS називаються стеком міток.

Таблиця 1 – Формат запису в стеці міток

Формат запису в стеці міток			
32 біта			
20 біт	3 біти	1 біт	8 біт
Label	TC	S	TTL

Кожний запис у стеці міток складається з наступних чотирьох полів:

– значення мітки (англ. label); займає 20 біт;

– поле «клас трафіку» (англ. traffic class); використовується для реалізації механізмів якості обслуговування (QoS) і явного повідомлення про перевантаження (англ. explicit congestionnotification, ECN) (до RFC 5462 це поле називалася Exp (англ. experimental use)); займає 3 біти;

– прапор «дно стека» (англ. bottom of stack); якщо прапор установлений в 1, те це означає, що поточна мітка остання в стеці; займає 1 біт;

– поле TTL (англ. time to live); використовується для запобігання петель MPLS комутації; займає 8 біт.

В MPLS-маршрутизаторі пакет з MPLS-міткою комутирується на наступний порт після пошуку мітки в таблиці комутації замість пошуку по таблиці маршрутизації. При розробці MPLS пошук міток і комутація по мітках виконувалися швидше, ніж пошук по таблиці маршрутизації або RIB (англ. **r**outing **i**nformation **b**ase – інформаційна база маршрутизації), тому що комутація може бути виконана безпосередньо на комутаційній фабриці замість центрального процесора. Маршрутизатори, розташовані на вході або виході MPLS-мережі, називаються LER (англ. label edge router – граничний маршрутизатор міток). LER на вході в MPLS-мережу додають мітку MPLS до пакета даних, а LER на виході з MPLS-мережі видаляє мітку MPLS з пакета даних. Маршрутизатори, що виконують маршрутизацію пакетів даних, ґрунтуючись тільки на значенні мітки, називаються LSR (англ. label switching router – комутуючий влучний маршрутизатор). У деяких випадках пакет даних, що надійшов на порт LER, уже може містити мітку, тоді новий LER додає другу мітку в пакет даних. Мітки між LER і LSR розподіляються за допомогою LDP (англ. label distribution protocol)] – протокол розподілу міток) [7]. Для того, щоб одержати повну картину MPLS-мережі, LSR постійно обмінюються мітками й інформацією про кожний сусідній вузол, використовуючи стандартну процедуру. Віртуальні канали (тунелі), називані LSP (англ. label switchpath – шляхи комутації міток), установлюються провайдерами для рішення різних завдань, наприклад, для організації VPN або для передачі трафіку через мережу MPLS по зазначеному тунелі. Багато в чому LSP нічим не відрізняється від PVC у мережах ATM або Frame relay, за винятком того, що LSP не залежать від особливостей технологій канального рівня. При описі віртуальних приватних мереж, заснованих на технології MPLS, LER, розташовані на вході або виході мережі, звичайно називаються PE-машрутизаторами (англ. provider edge – маршрутизатори на границі мережі провайдеру), а вузли, що працюють як транзитні маршрутизатори, називаються P-маршрутизаторами (англ. provider – маршрутизатори провайдеру) [8].

Простір значень міток

Поле значення мітки в MPLS заголовку займає 20 біт, у такий спосіб максимально можливе значення мітки дорівнює 1 048 575.

Наступні номери міток зарезервовані для різних цілей:

– мітка з номером 0 може використовуватися тільки як остання мітка в стеці. Наявність мітки 0 означає, що заголовок MPLS повинен бути віддалений, і наступна маршрутизація пакета повинна ґрунтуватися на значенні заголовка IPv4;

– мітка з номером 1 має особливу назву – мітка оповіщення маршрутизатора(англ. router alert label). Використання мітки 1 аналогічно використанню опції «Router alert option» при передачі в IP-пакетах. Мітка 1 не може використовуватися як остання мітка в стеці;

– мітка з номером 2 може використовуватися тільки як остання мітка в стеці. Наявність мітки 2 означає, що заголовок MPLS повинен бути віддалений, і наступна маршрутизація пакета повинна ґрунтуватися на значенні заголовка IPv6;

– мітка з номером 3 має особливу назву – неявна нульова мітка (англ. implicit NULL label). Мітку 3 може привласнювати й розсилати LSR, але мітка, у дійсності, ніколи не може використовуватися в стеці міток. Якщо LSR зустріне дану мітку в стеці міток, то замість заміни однієї мітки на іншу LSR видалить весь стек міток. Хоча в дійсності мітка 3 не може з'явитися в стеці міток, вона повинна бути зазначена в LDP;

– мітки з номерами від 4 до 15 зарезервовані.

Установка й видалення тунелів

Для мережі MPLS існує два стандартних протоколи керування тунелями:

– LDP (англ. label distribution protocol – протокол розподілу міток);

– RSVP-TE [en] (англ. resource reservation protocol for traffic engineering) – розширення протоколу RSVP для оптимізації й керування трафіком [9] [10].

Також існують розширення протоколу BGP, здатні управляти віртуальними каналами в мережі MPLS [11] [12] [13].

Заголовок MPLS не вказує тип даних, переданих в MPLS-Тунелі. Якщо виникла необхідність передачі двох різних типів трафіку між двома маршрутизаторами так, щоб вони по різному оброблялися маршрутизаторами ядра мережі MPLS, потрібно встановити два різних MPLS-Тунелі для кожного типу трафіку.

Порівняння MPLS і IP

MPLS як протокол некоректно порівнювати із протоколом IP, оскільки MPLS працює разом з IP і протоколами маршрутизації (IGP).

Основні переваги технології IP/MPLS:

– більше висока швидкість просування IP-пакетів по мережі за рахунок скорочення часу обробки маршрутної інформації;

– можливість організації інформаційних потоків у каналах зв'язку. За допомогою міток кожному інформаційному потоку (наприклад, що несе телефонний трафік) може призначатися необхідний клас обслуговування (Co (англ.)). Потоки з більше високим Co одержують пріоритет перед всіма іншими потоками. Таким чином, за допомогою MPLS забезпечується якість обслуговування (QoS), властивим мережам SDH і ATM;

– повне відокремлення друг від друга віртуальних корпоративних мереж за рахунок створення для кожної з них своєрідних тунелів;

– прозорий пропуск через ядро IP/MPLS трафіку протоколів Ethernet, Frame relay або ATM, що дозволяє підключати користувачів, що використовують всі ці різноманітні протоколи.

Побудова мереж

Технологія MPLS використовується для побудови IP-мереж.

На практиці MPLS використовується для передачі трафіку IP і Ethernet.

Основними областями застосування MPLS є:

– оптимізація й керування трафіком (англ. traffic engineering);

– організація віртуальних приватних мереж (VPN).

Альтернативи

На рівні транспортної мережі з MPLS конкурують такі технології, як PBB і MPLS-TP. За допомогою цих технологій так само можливо надавати послуги L2 VPN і L3 VPN. Також у якості конкурентної MPLS технології пропонується використання протоколу L2TPv3, однак він не популярний для рішення завдань, характерних для MPLS.

ZTP: включив і працюй

Незважаючи на бурхливий розвиток засобів віддаленого адміністрування, донедавна початковим налаштуванням маршрутизаторів у більшості випадків займався кваліфікований мережний інженер. Він повинен був перебувати поруч із пристроєм на відстані не більше 3 м (стандартна довжина кабелю для підключення до службового COM-порту), тобто мати локальний доступ до встаткування.

Уявіть, що маршрутизатори доставлені в Кропивницький для установки по всій області, а фахівці перебувають у Києві. Що в цьому випадку робити? Відправляти встаткування до інженерів або навпаки? Можливі, звичайно, і інші варіанти, але зручніше за все використовувати Zero Touch Provisioning.

При використанні ZTP мережні пристрої будь-яких розмірів і функціональності вводяться в лад так само просто, як домашні інтернет-центри plug-and-play. Виробники по-різному реалізують функцію ZTP, але всіх прагнуть зробити так, щоб для запуску маршрутизатора треба було всього лише підключити кабель і подати живлення. Контролер SD-WAN автоматично настроїть маршрутизатор відповідно до параметрів, які визначив адміністратор для даного вузла (групи вузлів), але спочатку маршрутизатор повинен одержати інформацію для зв'язку з контролером.

Кожний вендор вирішує це завдання по-своєму. Наприклад, маршрутизаторам SD-WAN початкові налаштування передаються через сервер DHCP або за допомогою флешки, що відправляється на об'єкт монтажу разом з маршрутизатором. А Huawei пропонує наступний спосіб: за допомогою електронної пошти або SMS монтажник відправляє контролеру ідентифікатор пристрою (серійний номер) і у відповідь одержує листа з гіперпосиланням. Потім досить підключитися до маршрутизатора через інтерфейс керування й клацнути по цьому посиланню. Мережний пристрій автоматично одержить від контролера всі необхідні налаштування.

Є й інші реалізації, але всі вони покликані максимально спростити уведення в лад нового обладнання.

Перехід на SD-WAN

Стратегія переходу на SD-WAN визначається поточним станом мережі (архітектурою, використовуваним устаткуванням) і бажаною реалізацією SD-WAN. Інтуїтивно здається, що простіше впроваджувати рішення SD-WAN того виробника, чия техніка вже використовується в мережі. Однак старі моделі найчастіше не будуть підтримувати керування через новий, нехай і того ж виробника, контролер SD-WAN. Крім того, перехід на SD-WAN може виявитися гарним приводом придбати встаткування іншої марки, якщо до існуючого нагромадилося багато претензій.

Сьогодні будь-який контролер SD-WAN може управляти пристроями тільки того ж виробника. До такого розвитку подій потрібно бути готовим, але це не привід відмовлятися від тих зручностей, які приносить впровадження SD-WAN. Як показує історія впровадження мереж SDN у центрах обробки даних, між появою робітників пропрієтарних рішень і виробітком єдиного стандарту по керуванню пристроями можуть пройти роки.

Найбільш раціональний сценарій – перехід на SD-WAN у міру додавання в мережу нових вузлів (маршрутизаторів) або по ходу планової заміни встаткування на існуючих вузлах. На проміжній стадії частина пристроїв буде залишатися під «ручним» керуванням, а нові – під управлінням контролера SD-WAN. При цьому обмін трафіком і маршрутною інформацією між маршрутизаторами буде відбуватися як звичайно. Чим більше пристроїв виявиться під управлінням контролера SD-WAN, тим швидше й зручніше стане керування мережею.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів управління інфраструктурою на основі рішень SD-WAN. В межах України в недостатній мірі представлені вітчизняні розробки в цій області. У роботі наведені теоретичне узагальнення й рішення наукового завдання дослідження методів управління інфраструктурою на основі рішень SD-WAN. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем управління інфраструктурою на основі рішень SD-WAN; Досліджена система управління інфраструктурою на основі рішень SD-WAN; На основі отриманих результатів досліджень створена програмна реалізація системи управління інфраструктурою на основі рішень SD-WAN. Розроблені під час виконання роботи алгоритми дозволяють успішно вирішувати завдання управління інфраструктурою на основі рішень SD-WAN. 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. Смоляр Є.В. Дослідження та програмна реалізація системи управління інфраструктурою на основі рішень SD-WAN // Збірник праць молодих науковців ЦНТУ. – Вип. 11. – Кропивницький: ЦНТУ, 2021.
2. RFC 1953 Ipsilon Flow Management Protocol Specification for IPv4
3. Yakov Rekhter et al., Tag switching architecture overview // Proc. IEEE 82 (December, 1997), 1973—1983.
4. RFC 4842 SONET/SDH Circuit Emulation over Packet (CEP)
5. Applied Data Communications (A Business-Oriented Approach) James E. Goldman & Phillip T. Rawles, 2004

(ISBN 0-471-34640-3)
6. RFC 3037 LDP Applicability
7. RFC 4364 BGP/MPLS IP Virtual Private Networks (VPNs)
8. RFC 3036 LDP Specification
9. RFC 3209 RSVP-TE: Extensions to RSVP for LSP Tunnels
10. RFC 2547 BGP/MPLS IP Virtual Private Networks (VPNs)
11. RFC 3107 Carrying Label Information in BGP-4
12. RFC 4781 Graceful Restart Mechanism for BGP with MPLS
13. Гольдштейн А. Б., Гольдштейн Б. С. Технология и протоколы MPLS. – СПб.: БХВ – Санкт-Петербург, 2005. – 304 с. – ISBN 5-8206-0126-2.
14. 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.
15. 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.

УДК 004

О. Юхимчак, магістр гр. КІ-19М-1,4
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ КЕРУВАННЯ ТЕХНОЛОГІЧНИМИ ПРОЦЕСАМИ ЗА РАХУНОК ВИКОРИСТАННЯ ТЕХНОЛОГІЙ INDUSTRIAL INTERNET REFERENCE ARCHITECTURE

У статті розроблено програмне забезпечення, яке призначено для системи керування технологічними процесами за рахунок використання технологій Industrial Internet Reference Architecture. Метою розробки є дослідження та програмна реалізація системи керування технологічними процесами за рахунок використання технологій Industrial Internet Reference Architecture. Об'єктом дослідження є процес керування технологічними процесами за рахунок використання технологій Industrial Internet Reference Architecture. Предметом дослідження є методи керування технологічними процесами за рахунок використання технологій Industrial Internet Reference Architecture. Методи дослідження базуються на методах побудови автоматизованих систем управління, методах математичної статистики, методах розробки програмного забезпечення. 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, Industrial Internet Reference Architecture

Постановка проблеми. Індустріальний інтернет (індустріальний інтернет речей, промисловий інтернет, Industrial Internet of Things, IIoT) – концепція побудови інфокомунікаційних інфраструктур, що припускає підключення до мережі Інтернет будь-яких непобутових пристроїв, устаткування, датчиків, сенсорів, автоматизованої системи управління технологічним процесом (АСУ ТП), а також інтеграцію даних елементів між собою, що приводить до формування нових бізнес-моделей при створенні товарів і послуг, а також їхній доставці споживачам. Ключовим драйвером реалізації концепції «Індустріального інтернету» є підвищення ефективності існуючих виробничих і технологічних процесів, зниження потреби в капітальних витратах. Ресурси компаній, що вивільняються таким чином, формують попит на рішення в сфері Індустріального інтернету. У систему інтернету речей сьогодні утягуються всі необхідні для його функціонування ланки:

виробники датчиків і інших пристроїв, програмного забезпечення, системні інтегратори й організації-замовники (причому як B2B, так і B2G), оператори зв'язку. Впровадження індустріального інтернету значно впливає на економіку окремі компанії і країни в цілому, сприяє підвищенню продуктивності праці й росту валового національного продукту, позитивним образом позначається на умовах праці й професійному росту співробітників. Сервісна модель економіки, що створюється в процесі цього переходу, ґрунтується на цифровізації виробництва й інших традиційних галузей, обміні даними між різними суб'єктами виробничого процесу й аналітику великих обсягів даних. Найбільш цікавими для рішень і платформ IIoT виглядають житлово-комунальне господарство, транспорт, медицина, сільське господарство, а також енергетика.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи керування технологічними процесами за рахунок використання технологій Industrial Internet Reference Architecture.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи керування технологічними процесами за рахунок використання технологій Industrial Internet Reference Architecture.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем керування технологічними процесами за рахунок використання технологій Industrial Internet Reference Architecture.

– Дослідження системи керування технологічними процесами за рахунок використання технологій Industrial Internet Reference Architecture.

– Програмна реалізація системи керування технологічними процесами за рахунок використання технологій Industrial Internet Reference Architecture.

Об'єктом дослідження є процес керування технологічними процесами за рахунок використання технологій Industrial Internet Reference Architecture.

Предметом дослідження є методи керування технологічними процесами за рахунок використання технологій Industrial Internet Reference Architecture.

Методи дослідження базуються на методах побудови автоматизованих систем управління, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Індустріальний інтернет речей кардинально змінює всю економічну модель взаємодії «постачальник – споживач». Це дозволяє:

– автоматизувати процес моніторингу й управління життєвим циклом устаткування;

– організувати ефективні ланцюжки, які самооптимизуються, від підприємств – постачальників до компаній – кінцевих споживачів;

– перейти до моделей «економіки спільного використання» і багато чого іншого.

У найбільш просунутих випадках індустріальний Інтернет речей дозволяє не тільки підвищити якість технічної підтримки устаткування з використанням розвинених засобів телеметрії, але й забезпечити перехід до нового бізнес-моделі його експлуатації, коли устаткування оплачується замовником по факті використання його функцій.

Впровадження мережевої взаємодії між машинами, устаткуванням, будинками й інформаційними системами, можливість здійснювати моніторинг і аналіз навколишнього середовища, процесу виробництва й власного стану в режимі реального часу, передавача функції управління й прийняття рішень інтелектуальним системам приводять до зміни «парадигми» технологічного розвитку, називаної також «четвертою промисловою революцією».

Закордонні експерти визнають інтернет речей технологією, що вносить необоротну трансформацію в організацію сучасних виробничих і бізнес-процесів і породжує нові бізнес-моделі.

Проведений консультантами J'son & Partners Consulting аналіз досвіду впровадження інтернету речей у світі показує, що перехід на концепцію IIoT відбувається за рахунок формування крос-індустріальних відкритих (по горизонталі й вертикалі) виробничо-сервісних екосистем, що поєднують безліч різних інформаційних систем управління різних підприємств і задіючий безліч різних пристроїв.

Такий підхід дозволяє реалізувати у віртуальному просторі як завгодно складні наскрізні бізнес-процеси, які здатні в автоматичному режимі здійснювати оптимізаційне управління (наскрізний інжиніринг) різного роду ресурсами через весь ланцюжок поставок і створення вартості продукції – від розробки ідеї, дизайну, проектування до виробництва, експлуатації й утилізації.

Для реалізації такого підходу потрібно, щоб вся необхідна інформація про фактичний стан ресурсів (сировина й матеріали, електроенергія, верстати й промислове устаткування, транспортні засоби, виробництво, маркетинг, продажі) як усередині одного, так і на різних підприємствах, була доступна автоматизованим системам управління різних рівнів (приводи й сенсори, контроль, управління виробництвом, реалізацією й плануванням).

Таким чином, можна сказати, що індустріальний інтернет речей являє собою організаційно-технологічну трансформацію виробництва, що базується на принципах «цифрової економіки», що дозволяє на рівні управління поєднувати реальні виробничі, транспортні, людські, інженерні й інші ресурси в практично необмежено масштабовані програмно-керовані віртуальні пули ресурсів (shared economy) і надавати користувачеві не самі пристрої, а результати їхнього використання (функції пристроїв) за рахунок реалізації наскрізних виробничих і бізнес-процесів (наскрізного інжинірингу).

Відмінністю екосистеми IoT від традиційних ринків є трансформація підприємств із ізольованих самодостатніх систем, усередині яких реалізовані всі необхідні для виробництва товару або послуги виробничі й бізнес-процеси, у відкриті системи інтегрованих високоавтоматизованих процесів. Такі відкриті системи реалізовані по моделі хмарних сервісів, у яких різні учасники ринку об'єднані в єдину платформу надання послуг кінцевому споживачеві, для створення якої основними засобами виробництва виступає не персонал, а хмарні сервіси, що автоматично управляють об'єднаними в пули программно-визначаємими пристроями.

Інакше кажучи, для традиційних підприємств і їхніх систем (ринків) базовим ресурсом, необхідним для безпосереднього управління всіма іншими видами ресурсів, є персонал, і, як наслідок, основним видом інформаційного обміну в таких системах є обмін голосовою інформацією й даними між людьми. А для екосистем IoT, які не використовують ручну працю безпосередньо при виконанні виробничих процесів, і система управління яких автоматично звертається прямо до необхідних виконавчих пристроїв і сенсорів, базовим ресурсом є інформація й автоматичні засоби її обробки.

Впровадження інтернету речей вимагає зміни підходів до створення й використання автоматизованих інформаційних систем управління (АСУ) і загальних підходів до управління підприємствами й організаціями. Застарілі виробничі лінії, які по різних причинах не можуть бути автоматизовані за допомогою IoT, можуть бути замінені на нове автоматизоване й роботизоване устаткування в майбутньому. Іншою перешкодою, що обмежує розвиток IoT, є відсутність або недостатня високий розвиток традиційних корпоративних інформаційних систем управління (ERP), тоді рішення IoT будуть локальними й вирішувати нішеві функції й завдання.

IoT може послідовно еволюціонувати від підключення окремих продуктів і об'єктів з метою їхньої діагностики й контролю до об'єднання різних продуктів і більш складних технологічних об'єктів управління в мережі IoT, а мережі IoT – у більш складні мережеві платформи й комплексні виробничі рішення.

У частині технологій управління й обробки інформації ці зміни полягають у наступному:

– реалізація програмної логіки АСУ як взаємодіючих між собою хмарних сервісів («хмара управління», «платформа IoT»);

– перехід від жорстко ієрархічно вибудуваних інформаційно ізольованих АСУ на безпосереднє, без участі людини й проміжних АСУ, підключення об'єктів управління в «хмару управління».

При цьому «хмара управління» виконує весь необхідний функціонал (програмні алгоритми обробки даних і управління) як низових систем управління, так і систем управління рівня підприємства й вище. Інакше кажучи, «хмару управління» одночасно виконує функції універсального засобу інтеграції й функції виконання як завгодно складних і різноманітних алгоритмів управління.

За рахунок використання механізму відкритих прикладних інтерфейсів програмування (Application Programming Interface, API) реалізується можливість підключення до «хмари управління» будь-яких пристроїв і будь-яких АСУ без необхідності внесення змін у підключаються устройства, що, і системи, і можливість реалізації логіки обробки поставляються в «хмару управління» даних з використанням готових шаблонів і, при їхній відсутності, з використанням убудованих засобів розробки програмних застосунків.

Ефект «Великих даних», що накопичуються в таких платформах IoT, і застосування технологій машинного навчання дозволяє автоматизувати процеси вдосконалювання виконуваною програмно «хмарою управління» алгоритмів, тобто оптимізувати алгоритми управління в міру нагромадження історичних даних, що надходять від широкої номенклатури пристроїв і АСУ, що в принципі неможливо в інформаційно ізольованих АСУ.

Накопичений у світі досвід впровадження IoT показує, що перехід на концепцію IoT дозволяє оперативно реалізовувати як завгодно складні наскрізні повністю автоматизовані бізнес-процеси. Такі процеси охоплюють безліч різних АСУ різних підприємств і організацій і задіють безліч різних пристроїв, що при використанні традиційного підходу до автоматизації в великості випадків неможливо реалізувати в розумний термін і за економічно обґрунтований бюджет.

При переході на принципи IoT наскрізні повністю автоматизовані процеси можуть охопити всі види взаємодій виробників товарів і послуг і їхніх споживачів. Це, наприклад, управління дорожнім рухом і транспортною інфраструктурою, управління комунальною інфраструктурою, процеси промислового виробництва й експлуатації виробів, забезпечення безпеки й багато чого іншого.

Така трансформація підприємств із закритих самодостатніх «чорних ящиків» в елементи відкритих екосистем, у свою чергу, вимагає кардинального перегляду бізнес-моделей підприємств і організацій всіх галузей економіки, особливо в частині зміни характеру взаємодії в ланцюжку «постачальник-споживач», що, властиво й відбувається в останні роки у світовій економіці.

Технологічний фактор, відмічуваний менеджментом компаній протягом уже чотирьох років як робить найбільший вплив на зміну підприємств, – це зміна технологій управління, а не технологій виробництва. Саме стік технологій управління й автоматизації управління, на відміну від попередніх технологічних (промислових) революцій, визначає перехід до нового технологічного укладу – четвертої промислової революції.

З погляду макроекономіки ріст ефективності процесів у ланцюжку « постачальник-споживач» означає перехід від інфляційного розвитку, що складає в перекладанні зростаючих витрат (ріст виторгу постачальника – це ріст витрат споживача) на «наступного в ланцюжку», а від кінцевого споживача – назад до виробників (роботодавцям) через вимоги про ріст зарплат, – до дефляційного. Дефляційний розвиток базується на росту ефективності всіх учасників екосистеми IoT, включаючи кінцевих споживачів, що є безпрецедентним для історії розвитку світової економіки.

Коли ресурси екстенсивного росту економіки за рахунок нарощування виробництва нових товарів і послуг на попередньому циклі технологічного розвитку вповільнюються (це відбувається зараз у великості розвинених економік), ключовим фокусом розвитку стає ріст

ефективності збутових-виробничо-збутових процесів. Цим, насамперед, і характеризується епоха активного розвитку інтернет-сервісів і впровадження IT-технологій.

Окремим сегментом росту національних економік є не споживачі інтернет-послуг, а самі виробники й провайдери інтернет-сервісів, продуктів і рішень, які захоплюють традиційні галузеві ніші й переформатують їх на основі хмарних технологій. Типовими прикладами є інтернет-медіа, електронна комерція й онлайн-замовлення таксі.

Переваги промислового інтернету речей для економіки

На думку J'son & Partners Consulting, за кількісним ростом інтернету речей і організаційно-технологічною трансформацією виробництва коштують важливі якісні зміни в економіці:

– дані, які раніше були недоступні, з ростом проникнення убудованих пристроїв являють собою коштовну інформацію про характер використання продукту й устаткування для всіх учасників виробничого циклу, є основний формування нових бізнес-моделей і забезпечують застосунковий дохід від пропозиції нових послуг, таких як, наприклад: контракт життєвого циклу на промислове устаткування, контрактне виробництво як сервіс, транспорт як сервіс, безпека як сервіс і інші;

– віртуалізація виробничих функцій супроводжується формуванням «економіки спільного використання» (shared economy), що характеризується істотно більш високою ефективністю й продуктивністю за рахунок підвищення використання наявних ресурсів, зміни функціонала пристроїв без внесення змін у фізичні об'єкти, шляхом зміни технологій управління ними;

– моделювання технологічних процесів, наскрізне проектування й, як результат, оптимізація ланцюжка створення вартості на всіх етапах життєвого циклу продукту в режимі реального часу, дозволяють робити штучний або дрібносерійний продукт за мінімальною ціною для Замовника й із прибутком для виробника, що в традиційному виробництві можливо тільки при масовому виробництві;

– еталонна архітектура, стандартизовані мережі й модель оренди замість оплати повної вартості володіння, роблять спільну виробничу інфраструктуру доступної для середнього й малого бізнесу, що полегшує їхнього зусилля по управлінню виробництвом, дозволяє прискорити реагування на вимоги, що змінюються, ринку й скорочення життєвого циклу продукції, і спричиняє розробку й появу нових застосунків і сервісів;

– аналіз даних про користувача, його виробничих об'єктах (машинах, будинках, устаткуванні) і характері споживання відкривають можливості для постачальника послуги з поліпшення клієнтського досвіду, створенню великої зручності користування, кращого рішення й скороченню витрат клієнта, що веде до підвищення задоволеності й лояльності від роботи з даним постачальником;

– функціонування різних галузей економіки буде безупинно ускладнюватися під впливом розвитку технологій і усе більш здійснюватися за рахунок автоматичного прийняття рішень самими машинами на основі аналізу великого обсягу даних з підключених пристроїв, що приведе до поступового зниження ролі виробничого персоналу, у тому числі кваліфікованого. Буде потрібно якісне професійне утворення, включаючи інженерне, спеціальні навчальні програми для працівників і тренінги.

Оцінка ефективності використання

В остаточному підсумку, впровадження будь-яких засобів автоматизації, у тому числі й відповідно до концепції інтернету речей, буде виправдано, якщо це дає економічний ефект у порівнянні із прийнятими формами виробництва й бізнес-процесів. У зв'язку із цим, консультанти J'son & Partners Consulting провели аналіз кейсів по застосуванню інтернету речей у різних галузях у світі й проаналізували чисельні значення показників ефективності.

Застосування IIoT у різних галузях

Аналіз кращих світових практик впровадження IIoT у дослідженні J'son & Partners Consulting показує, що основними сферами застосування рішень у сфері промислового

інтернету є виробництва, що характеризуються наявністю одного або декількох наступних важливих умов:

– випуск широкої номенклатури продукції, використання значного переліку комплектуючих;

– потреба в підвищенні якості випускається продукції, що, і зниженні ступеня шлюбу;

– потреба в забезпеченні ефективного сервісного обслуговування раніше поставленої продукції;

– потреба в зниженні експлуатаційних витрат виробництва;

– значна енергоємність виробництва;

– складні виробничі умови;

– потреба в оперативній діагностиці несправностей технологічного устаткування для зниження незапланованих зупинок виробництва;

– потреба в забезпеченні високої продуктивності персоналу;

– потреба в забезпеченні безпеки персоналу;

– необхідність системної інтеграції широкого спектра.

Типові результати впровадження ПоТ у промисловості

Дослідження J'son & Partners Consulting показало, що, по-перше, застосування датчиків контролю роботи устаткування з виходом у мережу дозволяє виробникові устаткування віддалено контролювати його роботу, вчасно проводити регламентні роботи, пророкувати аварії й проводити люб'язний-планово-попереджувальний ремонт або заздалегідь підготувати необхідні деталі на заміну й т.п. Таким чином, ми говоримо про те, що Інтернет речей є ефективним інструментом управління життєвим циклом продукції.

По-друге, знання про фактичне й плановане завантаження виробничого устаткування, з'єднаного з мережею, дозволяє організувати автоматичну мережу замовлень між різними виробництвами в довгому ланцюжку від постачальників матеріалів до споживачів кінцевої продукції. Це досягається шляхом підключення всіх виробничих площадок до єдиної програмної платформи, причому її учасниками можуть бути юридично різні компанії.

Така модель кардинально оптимізує транзакційні витрати в коопераційних ланцюжках, які здобувають якість самооптимізуючихся. Інакше кажучи, застосування концепції Інтернету речей дозволяє максимально оптимізувати коопераційні зв'язки для всього ланцюжка підприємств-учасників з метою досягнення найбільше економічно ефективного результату для кінцевого споживача.

По-третє, це стосується переходу від моделі продажу пристроїв і устаткування, вимірюваних кількістю поставленого устаткування, до моделі продажу функціонала (результатів використання) пристроїв і устаткування «на вимогу». Наприклад, коли компанія продає не просто компресори, а стиснене повітря із чітко певними й гарантованими параметрами.

Таким чином, у найбільш просунутих випадках мова може йти не просто про нову якість технічної підтримки устаткування (з використанням розвинених засобів телеметрії), але й об інший бізнес-моделі його експлуатації, коли устаткування взагалі не передається у власність замовника, а оплачується їм по факті використання його функцій. По такому принципі працюють, наприклад:

– найбільший постачальник промислових компресорів Kaeser – оплата компресорного устаткування відбувається по обсязі зробленого їм стисненого повітря;

– виробник сільськогосподарської техніки John Deere – оплата фактичного часу використання сільськогосподарської техніки (тракторів);

– багато інших провідних виробників промислового устаткування й споживчої техніки, описані у звіті.

Важливо відзначити, що продаж «на вимогу» – це ключова характеристика хмарного сервісу. Інтернет речей виступає в якості необхідного технічного компонента для розширення хмарної моделі за рамки інформаційно-комунікаційної індустрії. У тих галузях економіки, де ІКТ-устаткування не є кінцевим продуктом, а обчислювальні й комунікаційні системи застосовуються як допоміжні (для комп'ютеризації управління іншими видами устаткування й пристроїв, так звані убудовані системи), модель хмарних обчислень здобуває формат контракту життєвого циклу, тобто нової моделі взаємин у ланцюжку «постачальник – споживач».

Типовий результат проекту IoT – кратне підвищення ефективності всіх учасників екосистеми IoT не тільки в сфері ІКТ і фінансів, де продукт може бути створений і спожитий у повністю цифровому виді, але й у галузях матеріального виробництва. Причому в міру росту масштабу цих екосистем їхня ефективність росте, а не знижується, на відміну від побудованих по традиційному принципі коопераційних ланцюжків, де ріст витрат пропорційний квадрату росту чисельності персоналу взаємодіючих підприємств, – відзначають в J`son & Partners Consulting.

Наслідком такого типового результату проектів IoT є ріст конкурентоспроможності учасників екосистем IoT у глобальній системі поділу праці й ріст їхньої акціонерної вартості, що коли перетерплює IoT-трансформацію «традиційна» компанія, досягаючи порівнянної з «технологічними» компаніями ефективності, починає оцінюватися інвесторами за коефіцієнтами хмарних/технологічних компаній, таких як Google, Amazon і інших аналогічних.

IIoT у системах енергопостачання

В електроенергетиці під визначення «інтернету речей» звичайно попадають «розумні» або «інтелектуальні» мережі (smart grids) і лічильники (smart meters). Нові технології особливо актуальні для Україні, що володіє історично сформованою масштабною централізованою системою енергопостачання, а це понад 2,5 млн км ліній електропередач, близько 500 тис. підстанцій, 700 електростанцій потужністю більш 5 Мвт. Однак на сьогоднішній день проникнення «інтернету речей» у російську енергетику перебуває на початковому рівні.

На рівні управління системою, балансами й режимами в електроенергетиці крок у напрямку цифрової обв'язки активів може дати можливість більш оптимально планувати завантаження потужностей, що генерують, і, головний, їхній обсяг. Тому що російська енергосистема побудована на резервуванні, створення інтелектуальної моделі розподілу дозволило б вивести частину неефективної генерації з експлуатації й частково вирішити питання надвиробництва потужностей, що генерують (ріст із 215 ГВт в 2008 р. до 235 ГВт в 2016 р. при відсутності росту, що корелює, споживання). Одночасно це дозволило б більш широко впровадити сучасні стимули зниження споживання електроенергії: наприклад, управління попитом (demand response).

В електромережевому господарстві більш широке впровадження інтелектуальних технологій, особливо з урахуванням довжини лінійних об'єктів, могло б привести до підвищення надійності й зниженню операційних витрат. Це нарешті-те дозволило б перейти до управління мережею «по стані», а не проводити ремонти відповідно до твердих регламентних строків.

З передачею інформації також не повинне виникнути проблем, тому що мережевий комплекс, по суті, є найбільшим оператором зв'язку в Україні: наприклад, на всіх підстанціях (ПС) 110 кВт є канали зв'язку (у переважній великості оптоволоконні), всі нові ПС 35 кВт мають вихід в інтернет. Інтелектуальна електрична мережа також дозволить інтегрувати різні об'єкти виробництва електроенергії, у тому числі на основі поновлюваних джерел енергії (ПДЕ – сонце, вітер і ін.), розподілену генерацію.

Поки обсяги ПДЕ в Україні незначні, а обсяг розподіленої генерації становить близько 5,5% установленої потужності (ледве менш 13 ГВт), однак досвід інших країн показує, що ці показники будуть рости.

У Північній Америці й Західній Європі «інтелектуальні мережі» також дозволяють організувати рух електроенергії у двох напрямках, уможливлюючи продаж надлишків електрики, зробленого домогосподарствами (в основному сонячними панелями на дахах будинків).

У генерації елементи «інтернету речей» також використовуються – це системи управління активами класу АСУ ТП (автоматизовані системи управління технологічними процесами). Вони встановлені в різних комбінаціях на всіх електростанціях нашої країни й дозволяють дистанційно управляти й одержувати інформацію про роботу ключових систем. При цьому частка вітчизняного устаткування, що втішно, досить велика.

Деякі приватні енергетичні компанії також активно оснащують свої об'єкти системами віддаленого контролю й діагностики з метою підвищити надійність і знизити витрати на експлуатацію.

Безумовно, більш інтелектуальна енергетика принесла б очевидні вигоди як споживачам і виробникам електроенергії, так і вітчизняній економіці в цілому. Відповідні цілі позначені в ряді програмних документів (затверджена енергетична стратегія Україні на період до 2030 р., проект нової стратегії до 2035 р. Однак, на нашу думку, необхідна більш чітка, предметна стратегія держави в розвитку інтелектуальної енергетики.

ЄС, наприклад, ставить метою забезпечення 80% споживачів «розумними лічильниками» до 2020 р. (200 млн електричного й 45 млн газових лічильників). У США кожний штат самостійно визначає політикові по їхньому впровадженню, однак число «розумних лічильників» у цілому по країні вже наближається до 50% від загального числа (у шести штатах частка «розумних лічильників» склала більш 80%).

IIoT у транспортній галузі

У транспорт інтернет речей проникнув набагато глибше. У галузі, де довжина різних видів шляхів перевищує 1,6 млн км, а кількість вантажного транспорту (автомобільних, залізничного й інших) – 7 млн одиниць, у принципі неможливо обійтися без систем віддаленого моніторингу.

Найбільший розвиток IoT одержав в автомобільному транспорті завдяки поширенню тих же смартфонів, які водії беруть із собою в дорогу й частка яких наблизилася до 50 % стільникових пристроїв в Україні. Завдяки їм побудовані системи моніторингу завантаженості доріг на картах Google і ін. Навколо смартфонів в автомобілі – цілі екосистеми програмних рішень (наприклад, Uber, і ін.).

Дані рішення повністю змінили ринок таксі у великих містах. Такі сервіси вже не обмежуються тільки сферою таксі й проникають у сферу логістики: подібно UberCargo і Trucker path в Україні з'явилися стартапи GoCargo і iCanDrive, в основі яких лежить саме використання IoT.

Більш серйозні системи інтелектуального моніторингу транспорту впроваджуються завдяки установці в автомобілі систем віддаленого моніторингу пересування на базі датчиків GPS і систем контролю за витратою палива. Такі пристрої дозволяють істотно скоротити витрати й контролювати цільове використання транспорту, аналізувати й оптимізувати маршрути руху, що вкрай важливо для логістики. Без таких пристроїв не обходиться, напевно, жодне більш-менш більш транспортне підприємство. При цьому вони використовуються не тільки для зовнішніх перевезень, але й усередині підприємств. На ринку також багато програмних продуктів, що дозволяють аналізувати одержувані дані й оптимізувати витрати й процеси.

Безпека IIoT

Агентство Європейського союзу по мережах і інформаційній безпеці (ENISA) наприкінці листопада 2018 року опублікувало рекомендації із забезпечення безпеки IoT-пристроїв у контексті об'єктів критичної інфраструктури.

Звіт консолідує знання галузі по промислової кібербезпеки, показує модель погроз промислового інтернету речей, а також описує доступні міри, які можуть захистити від цих

погроз. Експерти що беруть участь у групі IoTTSEC (ENISA IoT Security Experts Group), додали ряд рекомендацій для тих, хто займається розробкою уніфікованих політик безпеки.

Відповідно до результатів дослідження, інциденти із пристроями інтернету речей входять у трійку погроз із найбільшим фінансовим збитком для компаній. Це ставиться до компаній будь-якого розміру: як малого й середнього бізнесу, так і великих корпорацій.

Однією з головних проблем у сфері кібербезпеки індустріальних IoT-пристроїв дотепер залишається відсутність єдиних стандартів. Рекомендації ENISA, як очікується, стануть важливим кроком убік уніфікації практик і політик безпеки, причому вони стосуються як творців і користувачів промислових IoT-пристроїв, так і різноманітних агентств Євросоюзу, що розробляють політики безпеки.

Серед основних рекомендацій, розроблених для регуляторів:

– Сфокусуватися на специфічні для конкретного сектора рекомендаціях замість загальних.

– Стандартизувати рекомендації усередині ЄС, установити єдину термінологію й класифікацію.

– Співробітничати із представниками індустрії й утягувати приватний сектор у розробку законів, використовуючи діючі асоціації й об'єднання, наприклад, AIOTTI.

Головні рекомендації для виробників пристроїв і розроблювачів ПЗ:

– Переконатися, що всі співробітники мають актуальні знання й навичками в області кібербезпеки.

– Забезпечити сумісність даних з надійною автоматизованою системою установки патчів.

– Провести аудит коду під час процесу впровадження – це допоможе зменшити кількість помилок у кінцевій версії продукту, а також виявити будь-які спроби впровадження шкідливого коду або обходу автентифікації.

Повний текст документа «Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures» можна знайти на сайті ENISA.

Розробка структурної схеми

Здешевлення виробництва сенсорів і розвиток аналітичних застосунків створили передумови для зародження Промислового інтернету. Однак його поява була б принципово неможливим без організації інформаційного обміну між структурними доменами й іншими компонентами систем Промислового інтернету, включаючи користувачів і промислові установки. Саме забезпеченню цього інформаційного обміну й повинні сприяти сучасні промислові мережі.

Архітектура промислового інтернету

Відповідно до архітектури Industrial Internet Reference Architecture, розробленої Industrial Internet Consortium, система Промислового інтернету піддається декомпозиції на структурні домени. Вони утворять важливі типові будівельні блоки (частково вже існуючі на підприємствах), які можуть застосовуватися в різних галузях. Кожна система Промислового інтернету буде містити принаймні наступні структурні домени:

– Управління – набір функцій рівня АСУ ТП (взаємодія із промисловим устаткуванням, читання даних, створення керуючих команд відповідно до логіки контурів управління й т.п.).

– Експлуатаційний – набір функцій для управління конфігурацією, моніторингу й оптимізації однієї або декількох підсистем доменів управління.

– Інформаційний – набір функцій для збору даних з різних доменів (насамперед з доменів управління), а також для перетворення, збереження й аналізу цих даних з метою одержання інформації більш високого рівня про систему Промислового інтернету (технології Data Lake і т.п.).

– Застосунки – реалізація логіки застосунків, що виконують певні бізнес-функції. Укрупнений рівень управління всією системою Промислового інтернету в довгостроковій

перспективі й глобальному масштабі. Цей домен може містити в собі логіку застосунка, правила, моделі й т.д. Його можна представити і як домен аналітики.

Бізнес – забезпечення наскрізних операцій системи Промислового інтернету шляхом їхньої інтеграції із традиційними або новими типами підсистем управління бізнес-процесами, планування й т.п. Прикладами таких систем можуть бути ERP, CRM, PLM, MES, HRM, управління матеріальними цінностями, управління проектами й багато хто інші.

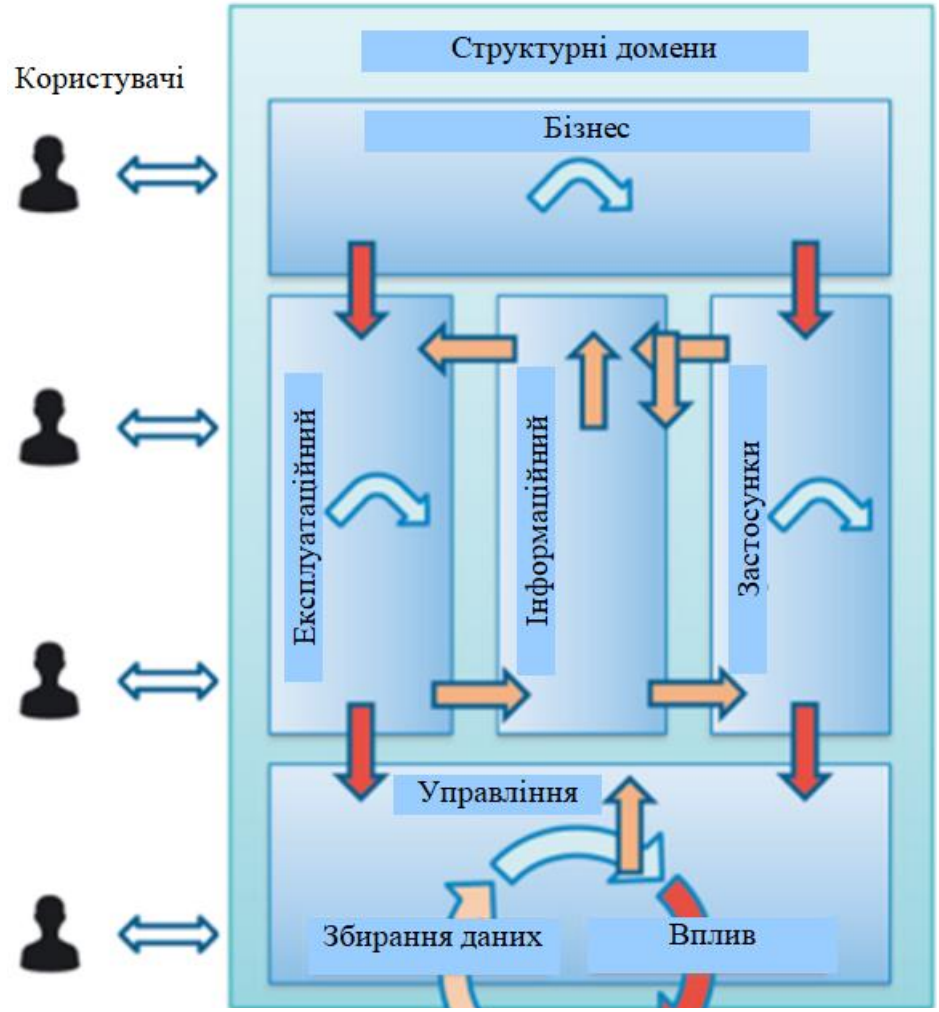


Рисунок 1 – Структурна схема системи

Структурні домени можуть піддаватися подальшої декомпозиції залежно від конкретних вимог до системи Промислового інтернету. У результаті якісь окремі функції можуть бути додані, виключені, об'єднані один з одним або виділені із уже наявних.

Використання різних мережевих технологій дозволяє забезпечити зв’язність , тобто можливість обміну даними між учасниками як у межах самого структурного домену, так і між структурними доменами в одній або різних системах Промислового інтернету. Обмін даними в рамках одного домену може складатися з опитування датчиків, повідомлень про події й зміни стану, аварійних сигналів, команд, відновлень конфігурації й т.п. Обмін між доменами може містити команди за результатами аналітичної обробки інформації з декількох доменів, автоматично створюваних планів обслуговування устаткування й т.п.

Фактично метою Промислового інтернету є забезпечення безшовного обміну інформацією між різними доменами й галузями. Однак за довгі роки попереднього розвитку для кожного домену були розроблені окремі набори мережевих технологій і протоколів, призначені для рішення вузького кола завдань. Крім того, щоб зберегти зроблені інвестиції й прискорити інновації, при впровадженні систем Промислового інтернету практично завжди

передбачається інтеграція існуючих систем з новими технологіями, через що запропонувати універсальне рішення неможливо.

У таких умовах питання сумісності будуть актуальні для всіх рівнів стека Промислового інтернету, навіть у рамках одного домену. Наприклад, на канальному рівні можуть виникнути проблеми об'єднання декількох сегментів Ethernet, якщо при їхній побудові використовувалися фірмові розширення протоколів, підтримуваних в устаткуванні різних виробників. На рівні фреймворку буде потрібно не тільки перетворити промислові протоколи, але й змінити формат даних.

Відповідність рівнів взаємодії систем Промислового інтернету й моделі OSI

Якщо всі домени й галузі, що використовують різні мережеві технології, спробувати інтегрувати один з одним прямо, то це приведе до утворення повнозв’язної схеми з кількістю зв'язків $N\times(N–1)/2$ і, як наслідок, до істотного ускладнення архітектури.

Для забезпечення повної зв’язності в рамках одного структурного домену потрібно вибрати основний стандарт, що повинен задовольняти всім істотним вимогам для даного домену. Підключення різноманітних технологій зв'язку (різні варіанти Ethernet, бездротові технології Wi-Fi, LoRaWAN, LTE та ін.) буде виконувати шлюз. Шлюзи можуть забезпечувати додаткові сервісні функції по перетворенню протоколів прикладного рівня, змінюючи структуру даних, і виконувати первинну локальну обробку даних з використанням технології мрячних обчислень, розглянуту далі. Шлюзи будуть також застосовуватися для зв'язку між тими доменами, де використовуються різні основні стандарти.

Подібний підхід дозволяє істотно поліпшити сумісність і масштабованість у порівнянні з повнозв’язною моделлю.

Взаємодія підрозділів

Для успішного впровадження систем Промислового інтернету дуже важливі налагоджені комунікації між різними підрозділами підприємства, відповідальними за підтримку різних доменів.

У виробничих і IT-підрозділів подання про зв’язності й безшовну інтеграцію можуть істотно розрізнятися. В IT-підрозділів зона інтересу звичайно обмежується мережевим рівнем моделі OSI і нижче. Виробничі підрозділи, відповідальні за підтримку й розвиток АСУ ТП у цілому, велику увагу приділяють інформаційному обміну на верхніх рівнях, де неминуче будуть виникати проблеми сумісності з успадкованими системами й іншими доменами Промислового інтернету.

Обидва типи підрозділів могли б співробітничати в спільних проектах – наприклад, таких як впровадження принтерів або обслуговування промислових комп'ютерів. Але, на жаль, ці й без того досить рідкі можливості найчастіше ігноруються. Звичайно приводом для звертання до колег служить яка-небудь проблема, що вимагає негайного рішення, – наприклад, інцидент інформаційної безпеки, збій системи або незапланований простій. Недолік взаємодії й взаєморозуміння між двома командами найчастіше приводить до неможливості розробки інноваційних рішень.

В умовах високої конкуренції й низьких цін на енергоносії власники підприємств змушені шукати нові рішення, які в великості випадків перебувають на стику промислових і IT-технологій. Щоб їх впровадити, необхідно кардинальну зміну підходу до організації взаємодії підрозділів.

Виробничі підприємства вже починають займатися адаптацією своїх процесів, технологій і бізнес-моделей. Самі передові компанії й під час кризи завзято працюють над тим, щоб одержати конкурентну перевагу й максимізувати прибуток, підвищуючи ефективність роботи. Саме вони й будуть очолювати цифрову трансформацію.

Очевидно, що фахівцям промислових і IT-підрозділів, що працюють у галузі, зовсім незабаром прийде реалізовувати нові, куди більш складні проекти. Робота над ними зажадає більш тісної взаємодії й підтримки з боку керівництва.

Далекоглядні керівники виробничих підрозділів визнають, що з великого обсягу даних, які вони вже зараз збирають і використовують, можна витягти додаткову цінність для

підприємства. Але для цього їхнього колеги з IT-підрозділів повинні зробити дані значимими й доступними для використання у всій організації, а крім того, допомогти інтегрувати їх у бізнес-системи, насамперед в інструменти планування ресурсів підприємства (ERP) і управління виробничими процесами (MES).

У той же час IT-підрозділу хочуть максимально повно реалізувати потенціал цифрового підприємства – від поліпшення ланцюжка поставок до впровадження інновацій і мінімізації простоїв. Однак для цього їм потрібні спеціальні знання й підтримка професіоналів, які розуміють і контролюють виробничі процеси й устаткування.

От чому старий формат взаємодії підрозділів, що часто обмежувався інфраструктурними проектами, повинен поступитися місцем могутнішим і продуктивним альянсам. Пройшло час, коли виробничі й IT-команди всього лише реагували на інциденти. Вони повинні взяти на себе ключову роль у здійсненні перетворень на своїх підприємствах і допомагати бізнесу використовувати нові можливості, роблячи його більш конкурентоспроможним, ефективним і безпечним.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів керування технологічними процесами за рахунок використання технологій Industrial Internet Reference Architecture. В межах України в недостатній мірі представлені вітчизняні розробки в цій області. У роботі наведені теоретичне узагальнення й рішення наукового завдання дослідження методів керування технологічними процесами за рахунок використання технологій Industrial Internet Reference Architecture. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем керування технологічними процесами за рахунок використання технологій Industrial Internet Reference Architecture; Досліджена система керування технологічними процесами за рахунок використання технологій Industrial Internet Reference Architecture; На основі отриманих результатів досліджень створена програмна реалізація системи керування технологічними процесами за рахунок використання технологій Industrial Internet Reference Architecture. Розроблені під час виконання роботи алгоритми дозволяють успішно вирішувати завдання керування технологічними процесами за рахунок використання технологій Industrial Internet Reference Architecture. 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. 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. Юхимчак О.О. Дослідження та програмна реалізація системи керування технологічними процесами за рахунок використання технологій Industrial Internet Reference Architecture // Збірник праць молодих науковців ЦНТУ. – Вип. 11. – Кропивницький: ЦНТУ, 2021.
8. Автоматизовані системи. Терміни та визначення: ДСТУ 2226-93 – [Чинний від 1993–09–09]. – Київ:

Держстандарт України, 1994. – 91 с. – (Національний стандарт України).
9. Аде Ф.Г. Искусственный интеллект / Ф.Г. Аде., В.Н. Бондарев. – Севастополь: Изд-во СевНТУ, 2002. – 615 с.
10. Алексєєва Т. В. Технічна діагностика гідравлічних приводів / В.Д. Бабанська, Т.М. Башта та ін. – М.: Машинобудування, 1989. – 263 с.
11. Артеменко А.М. Концептуальні основи подальшого розвитку РТВ Повітряних Сил Збройних Сил України на період до 2025 року. Погляди на створення єдиної системи РЛР та контролю повітряного простору / А.М. Артеменко // Новітні технології – для захисту повітряного простору: сьома наук. конф. Харківського університету Повітряних Сил імені Івана Кожедуба, 13 – 14 квіт. 2011 р.: тези доп. – Х.: ХУПС ім. І. Кожедуба, 2010. – С. 12-13..

УДК 338.439

Т. Бабенко, магістр гр. ЕО-19М
С. Мартиненко, доцент
Центральноукраїнський національний технічний університет

ЕКОЛОГІЧНА ОЦІНКА СТАНУ ПОВЕРХНЕВИХ ВОД М. КРОПИВНИЦЬКИЙ

Проаналізована питання впливу ОКВП «Дніпро – Кіровоград» на поверхневі води Кіровоградської області та запропоновано вирішення даної проблеми задля покрещення стану та якості поверхневих вод області.

Основною причиною забрудненн поверхневих вод України являється скид неочищених комунально- побутових і промислових стічних вод у водні об’єкти та через систему міської каналізації; надходження забруднюючих речовин у процесі повехневого стоку води з сільгоспугідь та забудованих територій до водних об’єктів.

Актуальність. Якісний стан оцінки поверхневих вод потрібно враховувати при водопостачанні, коунальному, рибному та сільському господарстві, виробництві промислової продукції, санітарно – курортному розвитку та багато іншого. На сьогоднішній день дуже сильно відчувається потреба в довідково – інформаційних матеріалах якісного стану поверхневих вод для водогосподарських та природоохоронних організацій, іншого матеріалу з питань охорони та відтворення та використання водних ресурсів.

Мета дослідження. Мета полягає в аналізі впливу ОКВП «Дніпро – Кіровоград» на якість поверхевих вод Кіровоградської області, прогнозування його стану, розробці відповідних рекомендацій та пропозицій з метою покращення стану поверхневих вод області.

Завдання:

- обрати місце та умови проведення відбору проб для лабараторного аналізу на вміст забруднюючих речов;
- дослідження впливуОКВП «Дніпро – Кіровоград» на формування та зміну якості поверхневих вод області;
- виявлення причин зміни якості поверхневих вод Кіровоградської області для запобігання небезпечним наслідкам;
- розробка рекомендацій та заходів для покращання якості поверхневих вод області;
- розробити заходи з охорони праці.

Об’єкт дослідження: поверхневі води Кіровоградської області.

Предмет дослідження: оцінка впливу ОКВП «Дніпро-Кіровоград» на поверхневі води Кіровоградської області.

Результати досліджень.

Вплив діяльності ОКВП «Дніпро-Кіровоград» на поверхневі води Кіровоградської області

Водопостачання та водовідведення. Забір поверхневих вод здійснюється з Кременчудського водосховища (басейн р. Дніпро) (м. Світловодськ Кіровоградська область). Відповідно до Дозволу на спеціальне водокористування № 319/КР/49д-19 від 24.06.2019 року ліміт забору води з поверхневих водойм становить 127721,99 м3 /добу або 42436,63 тис.м3 /рік, ліміт скиду по випуску №9 становить 946,834 м3 /год або 2355,804 тис.м3 /рік. Виробничі (промивні) води скидаються у Обломівську затоку р. Дніпро за межами населеного пункту с. Павлівка Світловодського району Кіровоградської області. Після проведення реконструкції забір поверхневої води з водоймища здійснюється за існуючою схемою.[1-5]

Промивні води відводяться до резервуарів повторного використання води та перекачуються на початок очисних споруд для повторної очистки або згідно до техрегламенту ОКВП «Дніпро-Кіровоград», а також нормативів «ГДС речовин у водний об'єкт із стічними водами підприємства, організації, установи» 2016 р. промивні води скидаються у Обломівську затоку Кременчуцького водосховища. Відстань до випуску становить 1,5 км. Ліміт 30 скиду відповідно до Дозволу на спеціальне водокористування становить 946,834 м 3 /год або 2355,804 тис.м3 /рік.

Джерелом водопостачання проектованих об'єктів являється існуюча на майданчику ВОС мережа господарсько-питного водопостачання. Існуючий господарсько питний водопровід прокладений з насосної станції другого підйому на відгалуженнях від колекторів Дніпро-Кіровоград. Один з трубопроводів діаметром 150 мм підключає існуючий блок основних споруд, адміністративний корпус і гараж, другий трубопровід діаметром 100 мм забезпечує водою БРГ, склад і хлораторну. Обидва трубопроводи тупикові, на них встановлені пожежні гідранти.

Проектом прийнято кільцювання існуючих мереж для забезпечення зовнішнього і внутрішнього пожежогасіння, питних і технологічних потреб проектованих будівель. При цьому ділянка трубопроводу від насосної станції другого підйому діаметром 100 мм перекладається на діаметр 150 мм. На проектованому трубопроводі встановлені пожежні гідранти в колодязях. Витрати води на технологічні потреби для блоку основних технологічних споруд, прийняті у відповідності з технологічною частиною проекту і становлять 21,9м3 /добу, 8м3 /год, 2,22 л/с. [5, 6]

Витрати води на технологічні потреби будівлі з обробки осаду, прийняті у відповідності з технологічною частиною проекту і становлять 39,5 м3 /добу, 48,0 м3 /год, 13,3 л/с. В будівлі з обробки осаду передбачається внутрішнє пожежогасіння - прийнято 2 струмені з витратою 5л/с, тобто загальна витрата складатиме 10л/с. Джерелом гарячого водопостачання блоку основних технологічних споруд та будівлі з обробки осаду прийняті електроводонагрівачі «THERMEX».

Проектована система побутової каналізації в будівлях фільтрувальної станції та будівлі з обробки осаду підключається до проектованого трубопроводу зовнішньої каналізації діаметром 200 мм. Перед початком будівництва блоку основних технологічних споруд проектом передбачено перенесення існуючої мережі побутової каналізації діаметром 200 мм, яка потрапила в зону будівництва. Надалі до цієї мережі будуть виконані підключення від проектованих будівель. Дощова каналізація На території очисних споруд відсутні мережі дощової каналізації. Відведення поверхневих стічних вод з покрівлі будівлі передбачаються відкритим способом за існуючою схемою на вимощення і далі в понижене місце рельєфу.

Джерела потенційного впливу планованої діяльності на поверхневі водні об'єкти, підземні та ґрунтові води:

Вплив на поверхневий водний об'єкт від водопровідних очисних споруд здійснюється шляхом відбору води з джерела водопостачання. При експлуатації реконструйованих водопровідних очисних поруд та водоводів не було встановлено потенційних джерел

негативного впливу на поверхневі водні об'єкти. Відбір води відбувається в межах встановлених лімітів.

Промивні води скидаються в межах встановлених лімітів. Межі зон санітарної охорони та санітарно-захисна смуга навеоло першого поясу водопровідних соруд витримані. Під час експлуатації водоводу, за рахунок аварійного витоку з мереж водопостачання, можливий вплив на грутові води. [6,7]

При проведенні будівельно-монтажних робіт не здійснювалось негативного впливу на поверхневі, ґрунтові та підземні води.

Забруднення річок Кіровоградської області внаслідок діяльності ОКВП «Дніпро – Кіровоград»

За результатами планової перевірки ОКВП «Дніпро – Кіровоград» з дотримання вимог природоохоронного законодавства, було встановлено, що Кропивницьким ВКГ відбувається скид недостатньо очищених зворотних вод у річку Інгул та Знам'янським ВКГ – у річку Інгулець, що є порушенням вимог статті 40 Закону України «Про охорону навколишнього природного середовища» та статей 44, 49, 70 Водного кодексу України.

Відповідальних осіб ОКВП «Дніпро – Кіровоград» за виявлені правопорушення природоохоронного законодавства державними інспекторами з охорони навколишнього природного середовища Кіровоградської області притягнуто до адміністративної відповідальності. Також були розраховані та пред'явлені претензії про відшкодування збитків, заподіяних державі внаслідок забруднення річок Інгул та Інгулець скидами недостатньо очищених зворотних вод. Загальна сума збитків склала 103569,98 грн. ОКВП «Дніпро – Кіровоград» направлено претензію для добровільного відшкодування збитків.[7-10]

Результати аналізів проб

Було проведено відбір проб поверхневих вод Кропивницького ВКГ у річці Інгул та Знам'янського ВКГ у річці Інгулець. Відібравши потрібну кількість проб води, їх було передано до лабораторії Держекоінспекції.

Безпосередньо в лабораторії було проведено повний аналіз відібраних проб назабруднюючі речовини, такі як: завислі речовини, хлориди, сульфати, водневий показник, фосфати, сухий залишок, амоній-іон, азот амонійний, нітрит-іони, нітрат-іони, залізо, СПАР (синтетичні поверхневі активні речовини).

Результати аналізу проб наведено в таблиця (4.1; 4.2; 4.3)

Таблиця 4.1 – р. Інгул, Кропивницького ВКГ, м. Кропивницький

Точка і місце відбору	Назва забруднюючих речовин	Позначення одиниці вимірю-вання	Результат вимірювання	ГДК
1	2	3	4	5
Ріка Інгул	Завислі речовини	мг/дм³	15,0	25,0
	Хлориди	мг/дм³	56,7	300,0
	Сульфати	мг/дм³	91,8	100,0
	Водневий показник	од. pH	7,8	6,5-8,5
	Фосфати	мг/дм³	2,18	2,15
	Сухий залишок	мг/дм³	520,0	1000,0
	Амоній-іон	мг/дм³	0,17	0,5
	Азот амонійний	мг/дм³	1,13	1,0
	Нітрит-іони	мг/дм³	0,09	0,08
	Нітрат-іони	мг/дм³	2,3	40,0
	Залізо	мг/дм³	0,6	0,1

	СПАР	мг/дм³	0,03	0,028
Ріка Інгул, на виїзді з міста	Завислі речовини	мг/дм³	12,6	25,0
	Хлориди	мг/дм³	81,5	300,0
	Сульфати	мг/дм³	189,7	100,0
	Водневий показник	од. pH	8	6,5-8,5
	Фосфати	мг/дм³	2,2	2,15
	Сухий залишок	мг/дм³	650,0	1000,0
	Амоній-іон	мг/дм³	1,5	0,5
	Азот амонійний	мг/дм³	1,2	1,0
	Нітрит-іони	мг/дм³	0,07	0,08
	Нітрат-іони	мг/дм³	2,1	40,0
	Залізо	мг/дм³	0,5	0,1
	СПАР	мг/дм³	0,18	0,028

Таблиця 4.2 – р. Інгулець, Знам'янського ВКГ, м Знам'янка

Точка і місце відбору	Назва забруднюючих речовин	Позначення одиниці вимірю-вання	Результат вимірювання	ГДК
1	2	3	4	5
Ріка Інгулець	Завислі речовини	мг/дм³	12,5	25,0
	Хлорид-іони	мг/дм³	117,0	300,0
	Водневий показник	од. pH	7,5	6,5-8,5
	Фосфати	мг/дм³	2,3	2,15
	Амоній-іон	мг/дм³	0,71	0,5
	Азот амонійний	мг/дм³	1,55	1,0
	Нітрит-іони	мг/дм³	0,15	0,08
	Нітрат-іони	мг/дм³	14,1	40,0
	Залізо	мг/дм³	0,11	0,1
	Сухий залишок	мг/дм³	1248,0	1000,0
	Сульфати	мг/дм³	308,6	100,0
	СПАР	мг/дм³	0,029	0,028

Таблиця 4.3 – р. Інгулець, нижче міста Знам'янка

Точка і місце відбору	Назва забруднюючих речовин	Позначення одиниці вимірю- вання	Результат вимірювання	ГДК
1	2	3	4	5
Ріка Інгулець, 2 км нижче міста Знам'янка	Завислі речовини	мг/дм³	18,0	25,0
	Хлорид-іони	мг/дм³	92,2	300,0
	Водневий показник	од. pH	7,6	6,5-8,5
	Фосфати	мг/дм³	2,9	2,15
	Амоній-іон	мг/дм³	1,076	0,5
	Азот амонійний	мг/дм³	1,84	1,0
	Нітрит-іони	мг/дм³	0,09	0,08
	Нітрат-іони	мг/дм³	6,7	40,0
	Залізо	мг/дм³	0,11	0,1
	Сухий залишок	мг/дм³	1108,0	1000,0
	Сульфати	мг/дм³	283,1	100,0
	СПАР	мг/дм³	5,8	3,0

Виходячи з отриманих результатів аналізу відібранних проб можемо зробити висновок, що ОКВП «Дніпро – Кіровоград» перевищує лімити ГДК по багатьом показникам забруднюючих речовин. Кропивницьким ВКГ здійснювався скид недостатньо очищених зворотних вод у річку Інгул, а Знам'янським ВКГ – у річку Інгулець. Це сприяє погіршенню стану поверхневих водойм, міняє pH, отруює риб, гине планктон.

Отже декілька прикладів, як саме впливає перевищення ГДК забруднюючих речовин. З наведених результатів бачимо, що як в річці Інгул так і в річці Інгулець більше перевищуються фосфати, залізо та СПАР (синтетичні поверхневі активні речовини).

За умов надмірного надходження фосфатів у водойми, він викликає їх евтрофікацію. Як наслідок відбувається накопичення біотоксинів, погіршення якості води, загибель гідробіонтів тощо. Використання мийних засобів на основі поліфосфатів теж сильно впливає підвищуючи біологічне навантаження на водні екосистеми. [11]

Тож надмірна концентрація фосфатів стає однією з найпоширеніших причин евтрофікації поверхневих вод. Результатом є надлишкова продукція автотрофів, особливо водоростей і ціанобактерій. Така висока продуктивність призводить до зростання бактеріальної популяції і високих темпів дихання. Це спричиняє гіпоксію або аноксію в погано переміщуваних придонних водах, а також в поверхневих водах. Низький рівень розчиненого кисню викликає загибель водяних тварин та вивільнення багатьох речовин, у тому числі різних форм фосфору. Це, в свою чергу, підсилює евтрофікацію.

Внаслідок вимивання вод з кристалічних порід українського геологічного щита та проходженням річкових водних об'єктів по заболоченій і лісистій місцевості, відбувається перевищення заліза загального та особливо марганцю.

Максимальний ризик отруєння солями важких металів зростає при використанні води без подальшого очищення з поверхневих водойм та криниць. У тих випадках, коли забруднені підземні води, також не рекомендується споживання води зі свердловин.

Наявність СПАР у воді призводить до інтенсивного розвитку мікрофлори. [11]

Висновок. Проведені дослідження щодо екологічного стану поверхневих вод Кіровоградської області дають змогу зробити ряд висновків і пропозицій.

Забруднення водних ресурсів – це будь-які зміни фізичних, хімічних і біологічних властивостей води у водних об'єктах у зв'язку із скиданням у них рідких, твердих і газоподібних речовин, які заподіюють шкоду, роблячи воду даних водоймищ небезпечною для використання, завдаючи збитку народному господарству, здоров'ю та безпеці населення.

Недостатньо очищені стічні води промислових і комунальних підприємств являються основними джерелами забруднення і засмічення водних об'єктів. Потрапляючи у водні об'єкти, забруднюючі речовини, призводять до якісних змін води, котрі частіше за все, виявляються в зміні фізичних властивостей води, у зміні хімічного складу води в наявності плаваючих речовин на поверхні води і відкладанні їх на дні водоймищ.

У водних об'єктах відбувається природний процес самоочищення води. Проте він протікає повільно. Поки промислово-побутові скиди були незначні, річки самостійно справлялися з ними. У зв'язку з різким збільшенням відходів у водні об'єкти, вони не справляються з таким значним забрудненням самостійно. Виникла необхідність знешкоджувати, очищати стічні води й утилізувати їх.

Отже виходячи з результатів дослідження заданої теми, можна зробити ряд пропозицій для покращення поверхневих вод Кіровогрдаської області, спрямованих на зменшення та усунення визначеного негативного впливу. [11, 12]

Захисні:

- припинити скид у водні об'єкти неочищених стічних вод;
- вести первинний облік водокористування та водовідведення;
- облік використання водних ресурсів із застосуванням лічильників з метою попередження перевищення ліміту, встановленого Дозволом на спеціальне водокористування;

- здійснювати лабораторний контроль якості вод що скидаються в природні водні об'єкти;
- забезпечити виключення можливості забруднення питної води через люки та перелівні труби резервуарів, пристроїв для заповнення насосів водою тощо;

Компенсаційні:

- забезпечити обов’язкове відшкодування збитків, заподіяних діяльністю, що супроводжувалась порушенням чинного законодавства;
- нарахування та сплата екологічного податку за скиди забруднюючих речовин в природні водні об'єкти.

Також передбачені заходи щодо зменшення негативного впливу на природне середовище:

1. Дотримання вимог Водного кодексу України;
2. Недопущення перевищення гранично допустимих концентрацій (ГДК) забруднюючих речовин в поверхневі води.

Якщо будуть надалі виявлені порушення законодавства про охорону навколишнього природного середовища підприємством ОКВП «Дніпро – Кіровоград» тоді негайно будуть вжиті заходи щодо усунення відповідних порушень, а також здійснено компенсацію в установленому порядку за шкоду, заподіяну довкіллю або здоров'ю і майну громадян, в повному обсязі. [11, 12]

Список літератури

1. Закон України «Про охорону навколишнього природного середовища».
2. ДБН А.2.2-1-2003 «Склад и зміст матеріалів оцінки впливів на навколишнє середовище (ОВНС) при проектуванні і будівництві підприємств, будинків і споруд».
3. ДСП 173-96 «Державні санітарні правила планування та забудови населених пунктів».
4. Закон України "Про охорону навколишнього природного середовища".
5. Водний Кодекс України.
6. "Порядок проведення громадських слухань у процесі оцінки впливу на довкілля", затверджений постановою Кабміну від 13.12.2017 р. № 989.
7. Постанова Кабміну України від 13.12.2017 р. № 1026 "Про затвердження Порядку передачі документації для надання висновку з оцінки впливу на довкілля та фінансування оцінки впливу на довкілля та Порядку ведення Єдиного реєстру з оцінки впливу на довкілля".
8. СанПин 4630-88 (v4630400-88) "Охрана поверхностных вод от загрязнения", Москва, 1988.
9. Хільчевський В. К. Гідрохімічний режим та якість води Інгульця в умовах техногенезу: Монографія [Електронний ресурс] / В. К. Хільчевський, Р. Л. Кравчинський, О. В. Чунарьов — К.: Ніка-центр, 2012. — 180 с.
10. Правила охорони поверхневих вод від забруднення зворотними водами, затверджених постановою Кабінету Міністрів України від 25.03.1999 № 465
11. Гранично допустимі значення показників якості води для рибогосподарських водойм. Загальний перелік ГДК і ОБРВ шкідливих речовин для води рибогосподарських водойм. К.: Міністерство рибного господарства СССР, 1990, 45 с.
12. Яцик, А. В., Гопчак, І. В. Методичні вказівки «Екологічна оцінка якості поверхневих вод за відповідними категоріями». Р.: НУВГП. 2012. С. 26.

УДК 004.087.2

Є. Бабич, магістр, гр. КІ-19М
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ОПИС СИСТЕМИ ВИЗНАЧЕННЯ ПРОДУКТИВНОСТІ ДАТА-ЦЕНТРУ

Для правильного вибору нового дата-центру або планування модернізації існуючого центру обробки даних необхідно уточнити запропоновані вимоги щодо зберігання даних в IT-системі. Головне - це потужність і продуктивність. На питання «Скільки терабайт корисної ємності потрібно?» зазвичай можна дати чітку відповідь і з цим не буде проблем. Але зазначити необхідну продуктивність системи зберігання даних може загнати багатьох людей у глухий кут.

Як перевірити продуктивність роботи дата-центру (СЗД)? Існує два підходи до оцінювання: технічний та користувальницький. У першому випадку продуктивність описується кількома технічними параметрами, пов'язаними з роботою СЗД. Цей підхід в основному застосовується IT-спеціалістами. У другому випадку продуктивність оцінюється на основі суб'єктивної думки користувача про те, як швидко працює IT-система. Очевидно, що такий підхід не підходить для реальної оцінки ефективності СЗД, але про нього не слід забувати, оскільки користувачі інформаційної системи можуть бачити ефективність компонентів IT-системи крізь призму монітора.

операційна система, програмне забезпечення, система зберігання даних, ризик-менеджмент

Постановка проблеми. Спочатку здається, для того щоб забезпечити високі показники IT, необхідно купувати найшвидші та найдорожчі СЗД. Що є не зовсім правдою. Не всі компанії задоволені цими придбаннями, оскільки існує чітка кореляція між показниками діяльності та витратами СЗД, а витрати на впровадження повинні мати мінімальний вплив на бюджет, і фінансовий відділ на першому місці. Щоб знайти баланс між ціною та якістю необхідно провести аналіз розрахунків. Саме тому розробка системи визначення продуктивності дата-центу є актуальною та необхідною задачею.

Таким чином, розробка програмного забезпечення системи визначення продуктивності дата-центру, є актуальною задачею, яка потребує вирішення.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1, 2] було виявлено певні прогалини системи визначення продуктивності дата-центру.

Мета й завдання дослідження. Метою роботи є розробка системи визначення продуктивності дата-центру.

Відповідно до поставленої мети, у роботі були вирішені такі *завдання*:

- досліджено існуючі системи, технології, архітектуру та програмні рішення за профілем теми магістерської дипломної роботи;
- обґрунтований вибір засобу для побудови системи;
- описані та обґрунтовані проектні рішення (функціональна схема);
- розроблена блок-схема та алгоритм функціонування системи;

Об'єктом дослідження є вивчення особливостей існуючих дата-центрів, баз-даних, за стосунків, СЗД та продуктивності дата-центру.

Предметом дослідження є теоретичні та прикладні аспекти процесу реалізації продуктивності дата-центру.

Методи дослідження базуються на математичному аналізу, аналітичний, групування, порівняння, класифікації, коефіцієнтний.

Продуктивність системи зберігання даних (далі СЗД) в IOPS (input/output operations per second) використовується для оцінки навантаження транзакційних програм, таких як бази

даних Online Transaction Processing (OLTP), зберігання файлів та поштові системи. Іншим технічним параметром, тісно пов'язаним із навантаженням транзакцій, є час відгуку на операції вводу-виводу. Іншими словами, цей час витрачається на обробку СЗД однієї операції вводу-виводу та надсилання результату хосту.

Раніше час відгуку використовувався разом із кількістю IOPS для детального планування конфігурації СЗД. Однак цей параметр набув широкої популярності з моменту появи СЗД, повністю побудованого на флеш-накопичувачах. Головною особливістю цих систем є те, що вони можуть обробляти додатки вводу-виводу після відгуку менше 1 мілісекунди. Для деяких додатків, включаючи бази даних OLTP, мінімально можливий час відгуку так само важливий, як і IOPS.

Продуктивність IT-системи в цілому визначається роботою окремих компонентів (додатків, операційних систем, фізичних або віртуальних серверів, мереж обміну даними між серверами та СЗД і самої СЗД). Кожен із цих компонентів, як правило, складається з багатьох окремих підсистем, кожна з яких може впливати на загальну продуктивність IT-системи. Отже, навіть із 100 високопродуктивними процесорними ядрами, якщо на вашому сервері закінчується оперативна пам'ять, загальна продуктивність вашої IT-системи може значно погіршитися. Або, наприклад, неправильно підібрана конфігурація дискової підсистеми вдосконаленої СЗД буде «сповільнювати» всю IT-систему, незважаючи на те, що така СЗД може витримати набагато більше навантаження.

На перший погляд здається, що щоб забезпечити високі показники IT у кожному підрозділі, слід купувати найдорожчі та найшвидші СЗД. Але це не зовсім так. Не всі підрозділи підприємства задоволені цими придбаннями, оскільки існує чітка кореляція між показниками діяльності та витратами СЗД, а витрати на впровадження повинні мати мінімальний вплив на бюджет, і фінансовий відділ на першому місці. Однак чим менше грошей витрачено на нову СЗД , тим менша продуктивність і втрати стають звичайним користувачем IT-системи. Тому IT-фахівці, відповідальні за впровадження нового сховища, повинні враховувати фінансові обмеження та знаходити вихід, і щоб продуктивність була достатньою [5].

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 за стосунків: бази даних у конфігурації «сховище даних» (Data Warehouse, DWH); застосунки для обробки відеоконтенту; резервне копіювання.

Таким чином, розробка програмного забезпечення системи визначення продуктивності дата-центру, є актуальною задачею, яка потребує вирішення.

Для існуючої IT-системи, яку потрібно лише перебудувати (наприклад, завдяки зростанню чи розширенню бізнесу), це дуже просте завдання. Потрібно виміряти поточну ефективність та потужність СЗД, потім спланувати збільшення їх протягом наступних двох або трьох років та придбати відповідні компоненти СЗД.

Впровадження нових рішень зазвичай не викликає особливих труднощів. Постачальники програмного забезпечення, як правило, вже підготували рекомендації щодо розгортання системи. Наприклад, компанія VMware має поняття «користувачі шаблонів» для рішень по віртуалізації робочих місць VDI. У прийнятній класифікації всі користувачі діляться на три категорії. Легкі користувачі мають менше навантаження на систему, а середні та важкі користувачі потребують більше ресурсів. Для кожної категорії підготовлені кількісні характеристики: рекомендована ємність пам'яті, кількість ядер процесора, IOPS, кількість переданих мегабайт в секунду тощо. Отже, експерти, які знають, що їм потрібно розгорнути систему VDI для 1000 користувачів, можуть заздалегідь передбачити IT-ресурси, які їм знадобляться для цього [6].

Однак існують ситуації, коли інформація про вимоги до продуктивності дискової підсистеми відсутня, або є обґрунтовані сумніви щодо застосовності даних шаблону. У цьому випадку IT-систему можна перевірити на запланованому обладнанні перед покупкою.

Багато постачальників обладнання та програмного забезпечення надають послуги, які допомагають оцінити поведінку певних IT-систем, які обробляють конкретні дані в різних програмно-апаратних конфігураціях, і розуміти, що потрібно для успішного впровадження.

Як показує досвід впровадження та експлуатації IT-систем, перед відновленням програмних чи апаратних компонентів існуючої IT-системи слід зібрати статистичні дані щодо продуктивності всіх компонентів (програми, сервера, СЗД) і повторити ту ж процедуру після впровадження. Це допомагає, по-перше, оцінити, наскільки покращилась ефективність роботи кожного компонента IT-системи, а по-друге, надає бізнес-користувачам можливість продемонструвати ефективність відновлення. У більшості випадків оцінка досягнутих результатів залежить від суб'єктивної думки. Один експерт консольного обладнання працює повільніше, а інший експерт працює швидше. Отже, запис чітких кількісних характеристик до і після відновлення дозволяє побачити, що насправді сталося з системою.

Найбільш оптимальним варіантом використання різних типів дисків у СЗД є багаторівневе зберігання даних. По суті, це не засіб підвищення продуктивності дискової підсистеми системи зберігання, а скоріше спосіб зменшення витрат шляхом встановлення різних типів дисків в одному дисковому пулі з точки зору продуктивності та вартості.

Жорсткий диск - це найповільніший компонент дискової системи. Твердотільний або SSD-диск став популярнішим аналогом данного накопичувача. Другим кроком є вибір типу RAID масиву. RAID – абревіатура Redundant Array of Inexpensive (надмірний масив недорогих (незалежних) дисків). Як правило, RAID-масив поєднує два або більше жорстких дисків (як правило, пристрій NAS або сервер) для підвищення продуктивності або забезпечення певного рівня стійкості системи. «Відмовостійкість», як правило, означає наявність «захисної сітки» у разі несправності обладнання, наприклад жорсткого диска, що дозволяє ПК продовжувати працювати після аварії. Час простою та ймовірність втрати даних зменшуються через відмовостійкість. RAID-масив можна налаштувати двома способами: апаратним або програмним [2].

За останнє десятиліття продуктивність процесора у сервера зросла в десять разів, обсяг оперативної пам'яті також, а продуктивність жорстких дисків зростає строго лінійно і досить повільно. А з процесором та пам'яттю все просто і зрозуміло - чим більше, тим краще. Але з дисками все набагато складніше. І в більшості випадків продуктивність дисків і СЗД є вузьким місцем у віртуальній інфраструктурі через неправильний розмір.

На рисунку 1 представлена функціональна схема розробленої у магістерській роботі системи. Система складається з таких блоків:

Блок розподілу визначає, який тип масиву RAID використовувати за критерієм критична/важлива інформація. Якщо інформація про дата-центр не критична, використовується RAID 0. Коли інформація про дата-центр важлива, використовується швидший і менш надійний RAID 1 або RAID 6, дуже стабільний, але менш швидкий залежно від важливості та вимог до продуктивності.

Блок вибору кількості дисків призначений для визначення кількості дисків у RAID-масиві. Якщо дисків 2, використовуються технології RAID 0 та RAID 1, а якщо дисків більше 2, використовуються технології RAID 0 та RAID 6.

Блок створення віртуального диска використовується, коли є лише один диск. Потім на цих дисках формується кілька віртуальних дисків, виконуючи операції, подібні до того, що відбувається з фізичними дисками. Іншими словами, масив RAID складається з віртуальних дисків.

Блок RAID 0, RAID 1 і RAID 6 реалізують ту чи іншу технологію.

Рисунок 1 - Функціональна схема системи

Код Рід-Соломона – це недвійковий круговий код, який може виправити помилки в блоках даних. Елементами кодового вектора є не біти, а групи бітів (блоків) [4]. Коди Рід-Соломона, які працюють у байтах (октетах), дуже поширені.

Зараз він широко використовується в системах відновлення даних з компакт-дисків і широко використовується при створенні архівів з шумостійким кодуванням, які містять інформацію, яку можна відновити у разі пошкодження.

Код Ріда-Соломона є важливим частковим прикладом БЧХ-коду (Код Бозе-Чоудхурі-Хокінгема), який є коренем генеративного полінома в тому самому полі, в якому складається код (m=1).

На рисунку 2 показана основна блок-схема програми визначення продуктивності дата-центру. Робота основної програми складається з початкового етапу ініціалізації програмного забезпечення, перевірки наявності системних ресурсів, стартового блоку основного циклу, де підсистема чекає запиту абонента, та завершального етапу перевірки поточного стану. Під час роботи підпрограми основні функції системи виконуються в циклічній послідовності, щоб перевірити поточний стан і повернутися до головного прапора програми в робочому стані.

Був використаний підхід із використанням UML, уніфікованої мови моделювання, що використовується в об'єктивно-орієнтованій парадигмі програмування. Це невід’ємна частина інтегрованого процесу розробки програмного забезпечення. UML - мова широкого профілю, відкритий стандарт для створення абстрактних моделей систем, що називаються UML-моделями з використанням графічних позначень. UML був створений насамперед для визначення, візуалізації, проектування та документування програмних систем. UML не є

мовою програмування, але в засобах виконання UML-моделей як інтерпретованого коду можлива кодогенерація [7].

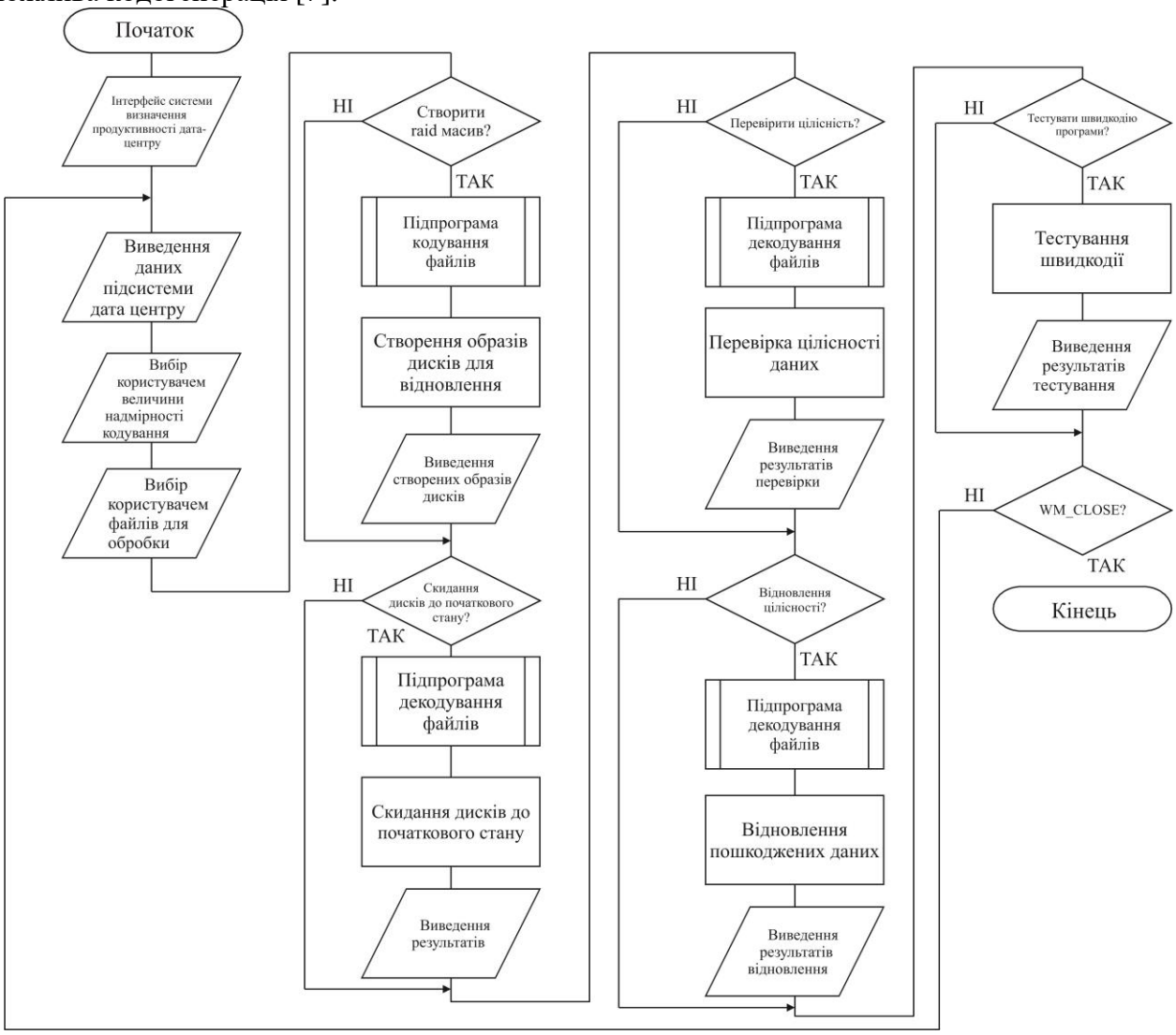


Рисунок 2 – Блок схема програми

При розробці ПЗ було використано підходи ризик-менеджменту – це система управління ризиками, яка включає стратегії та тактики управління, спрямовані на досягнення ключових цілей [3]. Ефективний ризик-менеджмент включає:

– систему управління;

– систему ідентифікації та вимірювання;

– систему підтримки (моніторингу та контролю).

Сучасна наука представляє ризики як можливі події, і їх виникнення може призвести до позитивних, нейтральних або негативних наслідків. Якщо ризик означає наявність як позитивних, так і негативних результатів, це означає спекулятивний ризик. Якщо результат негативний або відсутній, ці ризики називаються чистими.

Висновки: Програмне забезпечення, створене в результаті виконання магістерської дипломної роботи, призначено для реалізації системи визначення продуктивності дата-центру.

Дане 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 призначена для виконання під управлінням багатозадачної операційної системи Windows XP/Vista/7/8/10.

Список літератури

1. Gartner : Стратегическая дорожная карта хранения данных на 2018 год. Дайджест. Вип 15.С. 3.
2. Patterson D., Garth G., Katz R., A Case for Redundant Arrays of Inexpensive Disks (RAID). University of Califomia, Berkely, Report No. UC8/CSD/87/391, December 1987.
3. Арбузов С. Г., Колобов Ю. В., Міщенко В. І., Науменкова С. В. Ризик-менеджмент // Банківська енциклопедія. Київ : Центр наукових досліджень Національного банку України : Знання, 2011. 504 с.
4. Касперски К. Могущество кодов Рида-Соломона или информация, воскресшая из пепла. Системный администратор № 12. С 8-12 http://www.insidepro.com/kk/027/027r.shtml
5. Коваленко А.С., Смірнов О.А. Розробка структури бази даних інтегрованої інформаційної системи. 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.
6. Скотт Лоу. V Mware vSphere 4: повний довідник. «Діалектика», 2010. 800 с.
7. Яковина, В.С., Парфенюк Ю.І. Використання засобів UML для прогнозування надійності програмного забезпечення на етапі його проектування Львів: Національний університет “Львівська політехніка”, 2013. С 151 -156.

УДК 621.43.065

Б. Богаченко, магістр гр. АТ19М
Центральноукраїнський національний технічний університет

АНАЛІЗ ТИПІВ ГЛУШНИКІВ СИСТЕМИ ВИПУСКУ АВТОМОБІЛЬНИХ ДВИГУНІВ

Виконано аналіз конструкцій основних типів глушників, встановлено їх переваги та недоліки. Визначено елементи конструкцій глушників, що максимально впливають на рівень шуму випускної системи автомобільного двигуна.
шум, глушник, система випуску двигуна

Постановка проблеми. Одним із значущих джерел шуму автотранспортних засобів є система випуску відпрацьованих газів, тому вдосконалення методів проектування і дослідження конструкції систем випуску з метою зниження її шуму є важливим завданням і дозволить істотно знизити звукове випромінювання від автотранспортного засобу в цілому.Очевидним і першочерговим вирішенням проблеми, що склалася, є зниження шуму, який безпосередньо генерується вантажними автомобілями в процесі їх експлуатації. Оптимізація внутрішніх вузлів глушників шуму системи випуску відпрацьованих газів двигунів внутрішнього згоряння (ДВЗ) сучасних конструкцій автомобілів дозволяє на даний момент часу досягати істотного заглушення газодинамічної складової шумового випромінювання і виключати помітний вплив на загальні рівні їх зовнішнього і внутрішнього шуму.

Вирішення представлених проблем обумовлює необхідність проведення ефективних наукових досліджень по розробці методів, які дозволяють з найменшими витратами матеріальних, фінансових і тимчасових витрат використовувати ефективні технічні засоби зниження рівнів шуму джерел на стадіях проектування та експериментальної доведення конструкції автотранспортних засобів (АТЗ).

На підставі вищесказаного, проблема зниження шуму АТЗ є актуальною, що вимагає вдосконалення методів проектування, дослідження і доведення віброакустичних характеристик автомобілів.

Аналіз останніх досліджень та публікацій. Проблема зниження шуму висвітлювалася в багатьох роботах і публікаціях. Методи розрахунку ефективності даного типу глушників в різних виконаннях і комбінаціях детально розглянуті в працях Б. К. Шапіро, Р. Н. Старобінского, А. І. Комкіна [5], І. І. Клюкина, А. В. Васільєва [17], Л. С. Гільмана [12], Д. В. Баженова та інших авторів [1-14].

Мета і завдання досліджень. *Метою роботи* - є розробка вимог до вибору глушників шуму вихлопу двигунів внутрішнього згоряння автомобілів, а також розробка рекомендацій щодо проектування глушників шуму вихлопу двигунів внутрішнього згоряння для зниження акустичного забруднення і внутрішнього шуму.

Для досягнення поставленої мети вирішувалися наступні задачі досліджень:

1. виконати аналіз джерел шуму автомобіля;
2. проаналізувати причини підвищеної шумності системи випуску автомобілів;
3. виконати аналіз існуючих конструкцій автомобільних глушників.

Об'єкт дослідження – глушник випускної системи автомобіля.

Предмет дослідження – джерела генерування аеродинамічного шуму автомобільного двигуна та випускна система автомобілів як засіб зменшення акустичної енергії шумогенеруючих джерел ДВЗ.

Методи досліджень базуються на методах визначення рівнів шуму, що випромінюються випускною системою двигунів.

Використання глушників. Використання глушників вихлопу свого є найважливішим методом зниження шуму ДВЗ легкових автомобілів. Рівні незаглушенного шуму вихлопу ДВЗ можуть досягати 115...130 дБА (на відстані 0,25 м від відкритого зрізу хвостовій труби) і в десятки разів перевищувати шум інших джерел. Незважаючи на те, що глушник вихлопу в конструкції АТЗ застосовуються вже давно, до цих пір ведуться науково-практичні роботи з метою оптимізації їх конструкцій [7, 14].

Автовиробники для задоволення існуючих нормативних, експлуатаційних і екологічних вимог, підвищення споживчих властивостей і поліпшення вагових і вартісних показників АТЗ реалізують досить широку гаму нових високоефективних типів, поєднань і різновидів глушників [11]. Як правило, проектування глушника - це компроміс між досягненням необхідного шумопоглинання і вимогою мінімального протитиску газам, що проходять через глушник.

Як було зазначено вище, одним з основних джерел шумових випромінювань різних типів АТС є аеродинамічні (газодинамічні) шуми, що генеруються їх силовими установками, що включають ДВЗ, і випромінюються в атмосферу системами газообміну (газодинамічні шуми впуску і вихлопу). Для зменшення цих шумових випромінювань використовуються різного типу конструкції глушників в системі, що складаються, як правило, з розширювальних або резонаторних камер (замкнутих обсягів), відповідним чином сполучених трубами (патрубками, перфорованими перегородками і т.п.).

Крім розширювальних камер в складі базових (модульних) конструкцій глушників ДВЗ використовуються резонаторні камери, налаштовані на придушення шумових випромінювань у відносно вузьких смугах звукового спектра [11]. Додаткові резонаторні камери, в якості автономних шумоподавляючих пристроїв, використовують, як правило, для послаблення резонансного посилення звуку, що транспортується в трубопроводах системи випуску ДВЗ [12].

Крім того, в системах газообміну ДВЗ широко використовуються різні трубопровідні об'ємні елементи, основна функція яких безпосередньо не пов'язана з процесом шумоглушіння, але через які шумове випромінювання супутньо (вимушено) транспортується разом з потоком газів. Оптимізація акустичних характеристик такого типу камер також є вельми актуальною.

До наступного напрямку боротьби з шумом процесу випуску відносять використання глушників, застосування випускних колекторів з різною довжиною рукавів, використання високочастотних глушників в кожному циліндрі та ін.

Найбільш ефективним способом зниження шуму випуску досі залишається застосування різного роду глушників. Результати досліджень зниження шумоутворення в джерелі в даний час не дозволяють створити ДВЗ, що не потребує глушника. У той же час для двигуна із зменшеним шумоутворенням знижується і необхідна ефективність глушника, тому навіть часткові результати в цьому напрямі можуть бути корисні.

Глушник - це пристрій, що служить для перетворення енергії, який установлюють в кінці газовипускного тракту з метою зниження шуму [7].

Глушники повинні знижувати шум, що утворюється в основному двома процесами [14]:

- перший процес пов'язаний зі звуком, який виникає поза межами глушника і передається на нього через трубопроводи. Зниження цього шуму глушником засноване на таких акустичних принципах, як відбивання, поглинання або інтерференція звуку.
- інший процес - утворення аеродинамічного шуму на зрізі випускного пристрою при проходженні потоку стисненого повітря або відпрацьованих газів. Ослаблення аеродинамічного шуму тут досягається шляхом впливу на потік, що проходить через глушник, і зниження його енергії.

Для зменшення енергії потоків або струменів використовується наступне:

- зміна руху газового потоку або струменя шляхом раптового розширення або стиснення прохідного перетину, повороту, подовження шляху і т.п .;
- вчинення потоком (струменем) роботи;
- охолодження газового потоку;
- введення додаткового опору при русі потоку або струменя.

З цією метою в глушниках застосовуються розширювальні камери, перфоровані трубки і перегородки, глухі перегородки, трубки Вентурі, перфоровані обичайки і ін.

Результат узагальнення класифікацій глушників, представлених в різних літературних джерелах [7, 10, 14], показаний.

Камерні глушники діють як акустичні фільтри, знижуючи звук на деяких частотах за рахунок його відбивання в місцях звуження і розширення повітропроводу [14]. Даний вид глушників найбільш ефективний на низьких частотах, а їх акустична характеристика може мати широкі смуги заглушення і вузькі смуги повного проходження звуку.

Резонансні глушники є газовими порожнинами, що сполучаються з трубопроводом за допомогою отвору. Ці глушники зазвичай оформлюються у вигляді групи резонаторів, вони застосовуються для придушення дискретних складових шуму. Кожен резонатор є елементарною коливальною системою з загасанням, яка будучи збудженою падаючої на неї звуковою хвилею, відбирає від останньої акустичну енергію на частотах, близьких до власної частоти [7].

У абсорбційних глушниках зниження шуму досягається за рахунок переходу звукової енергії в теплову в звукопоглинальних елементі. Глушники ефективні в середньо- і високочастотному діапазонах з максимумом на частотах, при яких коефіцієнт звукопоглинання матеріалу близький до одиниці [7].

Інтерференційні глушники для зниження шуму використовують взаємне ослаблення звукових хвиль, що пройшли через канали різної довжини і знаходяться, внаслідок цього, в протифазі. Застосування глушників даного типу, так само як і резонансних, найбільш ефективне, коли потрібно заглушити одну або кілька тональних складових в стабільному спектрі шуму.

Комбіновані глушники об'єднують в собі декілька принципів зниження шуму і можуть мати ознаки всіх перерахованих вище типів глушників. Їх ефективність складається з ефективностей, які входять до складу стандартних типів глушників (заснованих на одному принципі зниження шуму). Всі вищеназвані типи глушників є пасивними, оскільки не використовують для зниження шуму зовнішніх джерел енергії.

В даний час накопичено чималий досвід у проектуванні та попередньому розрахунку результативності пасивних глушників шуму. Активні глушники шуму ґрунтуються на

принципу інтерференції: накладення звукових хвиль з однаковими амплітудами і протилежними фазами з їх взаємним гасінням. Вони мають високу ефективність в низькочастотному діапазоні, і на відміну від іншого не вимагають для цього великих габаритів і дорогих матеріалів. Багато дослідників визнають велику перспективність застосування даного типу глушників [3, 4, 5].

Так як у сучасних легкових автомобілях практично не помітний шум вихлопу, поширеною є думка про те, що при установці подібних систем глушіння на вантажний автомобіль буде спостерігатися такий же ефект. Слід пам'ятати, що більшість сучасних вантажних автомобілів оснащені дизельними двигунами, а вони характеризуються більш жорсткою роботою і більш високими тисками в циліндрах. При цьому середня потужність і літраж ДВЗ вантажних автомобілів набагато вища більшості легкових автомобілів. Це визначає більш значні амплітуди пульсацій об'ємної витрати газів у вихлопній системі, а отже, і більш високий загальний рівень шуму.

Також слід враховувати той факт, що довжина випускного тракту легкових і вантажних автомобілів дуже різниться.

Враховуючи вище приведений аналіз, можливо зробити висновок, що при створенні систем зниження шуму доцільно використовувати пасивні методи зниження шуму, що дозволяють отримати конструктивні рішення, спрямовані на зниження структурного шуму і від зрізу випускної труби, при забезпеченні вимог щодо токсичності та протитиску.

Висновки. 1. ДВЗ (його механізми і системи) - є основним джерелом як зовнішнього, так і внутрішнього шуму автотранспортного засобу і зокрема вантажних автомобілів, парк яких з року в рік збільшується, тому зниження шуму ДВЗ є вкрай актуальним завданням.

2. Незважаючи на вже накопичений досвід проектування автомобілів, навіть застосування відомих методів зниження шуму вимагає наукових досліджень для отримання оптимальної системи заходів щодо його зниження.

3. Виконані дослідження моделей реактивних, абсорбційних і комбінованих глушників дозволяють зробити наступні висновки:

- збільшення обсягу глушника збільшує його ефективність на низьких і середніх частотах (до 500 Гц);

- до числа найбільш важливих конструктивних елементів, які здійснюють організацію газового потоку в реактивному глушителі, відносяться перфоровані трубки і перегородки.

Список літератури

1. Старобинский Р.Н. Теория и синтез глушителей шума для систем впуска и выпуска газов ДВС: дисс. д-ра техн. наук: 05.04.02 / Р.Н. Старобинский -М.: МАДИ, 1983. – 333 с.
2. Галевко В.В. Совершенствование акустических качеств автомобильных V-образных дизелей: дис. … канд. техн. наук.: 05.04.02 / Владимир Владимирович Галевко. -М.: МАДИ (ТУ), 1982. -241 с.
3. Бабасова, Е. М. Активные методы гашения звуковых полей / Е. М. Бабасова, М. П. Завадская, Б. Л. Энгельский.– Л.: ЦНИИ «Румб», 1982.– 54 с.
4. Белякин, С. К. Разработка метода акустического расчета комбинированных глушителей шума транспортных средств: дис. канд. техн. наук / С. К. Белякин.– Курган, 2000.– 189с.
5. Комкин, А. И. Снижение шума активным методом / А. И. Комкин.– М.: МГТУ им. Н. Э. Баумана, 2000.- 24 с.
6. Луканин, В. Н. Шум автотракторных двигателей внутреннего сгорания / В.Н. Луканин.– М.: Машиностроение, 1971.– 271 с.
7. Старобинский, Р. Н. Теория и синтез глушителей шума для систем впуска и выпуска газов двигателей внутреннего сгорания: автореф. дис. … докт. техн. наук / Р. Н. Старобинский.– М., 1983.– 24 с.
8. Юдин, Е. Я. Борьба с шумом на производстве: справочник / Е. Я. Юдин, Л.А. Борисов, И. В. Горенштейн и др.; под ред. Е. Я. Юдина.– М.: Машиностроение, 1985.– 399 с.
9. Кане, А. Б. Борьба с шумом всасывания дизелей / А. Б. Кане.–М.:Машиностроение, 1969.– 144 с.
10. Мокринский, А. В. Методика комплексного снижения шума тепловых двигателей: автореф. дис. … канд. техн. наук / А. В. Мокринский.– Тольятти, 2003.–214 с.
11. Федоров В.В., Сахно В.П. Класифікація глушників шуму // Автошляховик України. - 2000, № 2. - С. 13 - 16.
12. Сахно В.П., Федоров В.В. До питання щодо сертифікації транспортних засобів по рівню зовнішнього шуму

// Збірник наукових праць “Проблеми автомобільного транспорту”, 2000. — С. 75 79.
13. Федоров В.В., Сахно В.П. Уточнення формули для визначення частоти вихлопу відпрацьованих газів ДВЗ /Автошляховик України. - 2001. - № 2. - С. 25 - 26.
14. Федоров В.В., Сахно В.П., Капко А.О., Федоров В.А. Спосіб глушіння шумів та пристрій для його здійснення. Деклараційний патент № 31715А, бюлетень “Промислова власність” № 7-II, 15.12.2000 р.

УДК 004

М. Мошніков, магістр гр. КІ-19М-1,4
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ КОРПОРАТИВНОЇ МЕРЕЖІ ВІД КІБЕРАТАК

У статті розроблено програмне забезпечення, яке призначено для системи забезпечення безпеки корпоративної мережі від кібератак. Метою розробки є дослідження та програмна реалізація системи забезпечення безпеки корпоративної мережі від кібератак. Об’єктом дослідження є процес забезпечення безпеки корпоративної мережі від кібератак. Предметом дослідження є методи забезпечення безпеки корпоративної мережі від кібератак. Методи дослідження базуються на методах захисту інформації, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи забезпечення безпеки корпоративної мережі від кібератак.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, безпека, корпоративна мережа, кібератака

Постановка проблеми. Корпоративна мережа, яка розглядається у рамках поточної роботи, представлена у вигляді сервіс-компонентної архітектури. Сервісно-компонентна архітектура (SCA) – специфікація, або, скоріше, набір специфікацій, розроблений для опису моделі створення додатків і систем на базі сервісно-орієнтованої архітектури (SOA). SCA надає модель побудови додатків, що складаються із сукупності сервісів і бізнес-функціонала. Переваги SCA над іншими SOA-технологіями не завжди очевидні відразу. Під час створення первісного варіанта SOA-системи звичайно передбачається наявність гомогенного середовища, усі компоненти якої використовують єдиний стандарт Web-сервісів і одна загальну мову програмування. Проблема полягає в тому, що часто таке оточення нереалістично. Звичайно є вже існуючі успадковані додатки, що вимагають інтеграції із системою й найчастіше що погано вписуються в гетерогенне оточення. Але виникають наступні запитання. Що, якщо обраний для інтеграції стандарт Web-сервісів виявиться невідповідним? Що, якщо буде потрібно використовувати більше новий стандарт для взаємодії із сервісами зовнішніх постачальників, або буде обраний інший метод для надання сервісів вашої компанії третій стороні? Прийшов час переписувати всі сервіси? Тільки не з архітектурою SCA. При цьому, побудова сучасних систем неможлива без використання систем захисту, у тому числі й побудова систем на базі сервіс-компонентної архітектури.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи забезпечення безпеки корпоративної мережі від кібератак.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи забезпечення безпеки корпоративної мережі від кібератак.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем забезпечення безпеки корпоративної мережі від кібератак.

– Дослідження системи забезпечення безпеки корпоративної мережі від кібератак.

– Програмна реалізація системи забезпечення безпеки корпоративної мережі від кібератак.

Об'єктом дослідження є процес забезпечення безпеки корпоративної мережі від кібератак.

Предметом дослідження є методи забезпечення безпеки корпоративної мережі від кібератак.

Методи дослідження базуються на методах захисту інформації, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Корпоративна мережа побудована на компонентній архітектурі сервісів (SCA) – це безліч специфікацій, що описують модель побудови додатків і систем з використанням сервіс-орієнтованої архітектури (SOA). SCA розширює й доповнює попередні методи реалізації сервісів і ґрунтується на відкритих стандартах, таких як веб-сервіси.

По-суті, SCA забезпечує програмну модель для реалізації SOA.

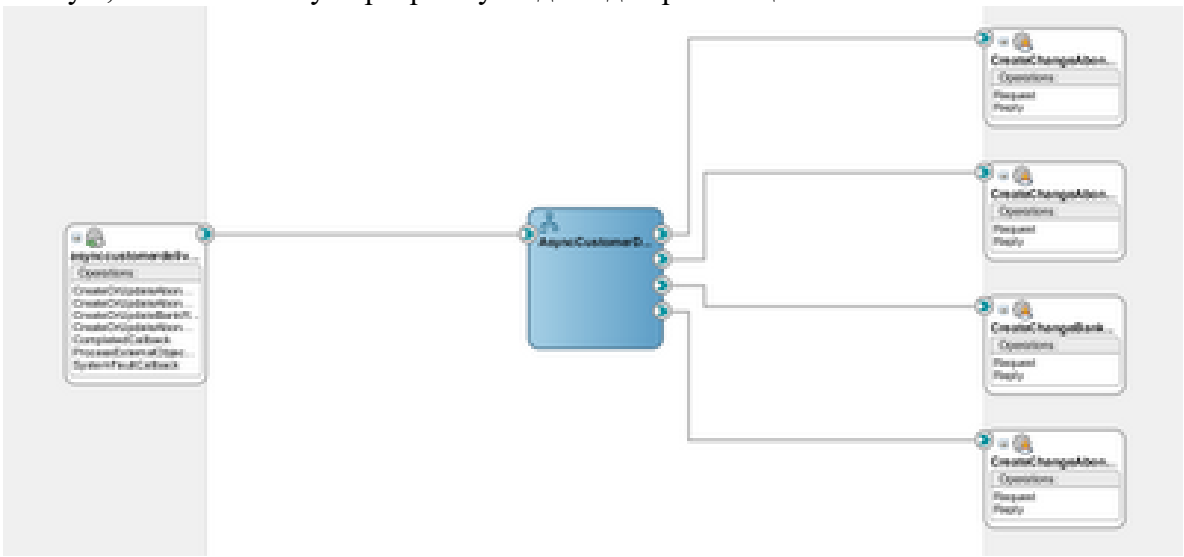


Рисунок 1 – Структура програмної моделі SCA

Специфікація складається із двох основних частин, що описують методи

– Реалізації компонентів, що надають одні й що використовують інші сервіси.

– Об'єднання безлічі компонентів для побудови бізнес-додатків шляхом зв'язування сервісів і сервісних посилань (service references).

Розроблювачем специфікації є консорціум Open SOA Collaboration (www.osoa.org). Поточна версія специфікації – 1.0 від 21 березня 2007 р. Деякі частини специфікації прийняті пізніше, наприклад SCA Assembly Extensions for Event Processing and Pub/Sub V1.00 – 30 квітня 2009 р. Існує чернетка версії 1.1, випущеної 31 травня 2011. Незважаючи на те, що це – чернетка, вона вже підтримується Oracle.

SCA підкреслює незалежність способу реалізації й об'єднання сервісів від можливостей інфраструктури й використовуваних методів доступу. Компоненти SCA обслуговують бізнес-рівень і використовують мінімум API проміжного шару.

Дана специфікація підтримує реалізації сервісів, написані з використанням різних мов програмування, включаючи об'єкто-орієнтовані й процедурні мови, такі як Java, PHP, C, C++, COBOL, мови-підмножини XML, такі як BPEL і XSLT, а так само мови декларативного програмування, такі як SQL і XQuery.

SCA так само підтримує різні стилі програмування, включаючи асинхронне, орієнтоване на обробку повідомлень і стиль "запит-відповідь".

Так само специфікація підтримує велику кількість методів доступу до сервісів: веб-сервіси, системи обміну повідомленнями, CORBA IIOP і т.д. Зв'язування сервісів один з одним здійснюється декларативно й не залежить від коду реалізації самих сервісів. Інфраструктурні можливості, такі як забезпечення безпеки, транзакції й використання гарантованої доставки, так само підключаються декларативно й окремо від коду реалізації сервісів. Використання інфраструктурних можливостей здійснюється за допомогою механізму політик.

Однією із цілей розробки SCA є спрощення створення сервісних компонентів: програміст може сконцентруватися на завданнях бізнес-логіки, і не звертати увагу на інфраструктурні питання. Специфікація так само пропонує прозору модель об'єднання сервісних компонентів у бізнес-рішення із забезпеченням декларативною інформацією, що визначає зв'язку сервісів, посилань і використовуваних протоколів.

Для подання бізнес-даних використовуються сервісні об'єкти даних – Service Data Objects (SDO), які формують параметри виклику й значення, що повертаються сервісами,, а так само забезпечують уніфікований доступ до бізнес-даним на додаток до уніфікованого доступу до бізнес-сервісам, реалізованому SCA самостійно. Тобто SCA надає уніфікований доступ до бізнес-сервісів, а SDO у добавок до цього – уніфікований доступ до бізнес-даних.

Введення такого уніфікованого методу доступу до даних дозволяє звільнити розроблювача від необхідності розуміння безлічі різних форматів даних і програмних інтерфейсів, які необхідні для їхньої обробки (наприклад, JDBC для реляційних даних, JAX-P для XML і т.д.) Так само SDO підтримує роз'єднаний, оптимістично-обновлюваний стиль програмування, де дані зчитуються з деякого джерела, обновляються клієнтським додатком і передаються назад в оригінальне місце розташування без необхідності блокування вихідних даних на час їхньої обробки.

Основні поняття SCA

Нижче наведений словник, що включає в себе основні поняття специфікації SCA.

Сервіс – представляє інтерфейс, реалізований компонентом або цілою SCA-збіркою – композитом. Даний інтерфейс може використовуватися клієнтом композита або компонентом. Сервіс, реалізований ззовні композита, називається зовнішнім сервісом.

Компонент – представляє частину бізнес-логіки. Це може бути логіка процесу, такого як BPEL- або BPMN-процес, логіка маршрутизації, така як Mediator або інші компоненти. Компонент – ядро SCA і може бути реалізований на будь-якій мові, підтримуваній даною специфікацією. Будучи один раз певним, компонент може декларативно конфігуруватися за допомогою механізму властивостей.

Посилання – це залежність від сервісу, надаваного іншим компонентом, інший SCA-складанням або зовнішньою сутністю, такий як вилучений веб-сервіс. Посилання на сервіс, реалізований поза композитом, називається зовнішнім посиланням. Посилання дозволяють компоненту взаємодіяти з іншими сервісами. Посилання дозволяються під час завантаження або під час виконання.

Модель складання – описує як сервіси визначаються й настроюються.

Зв'язок. Сервіси й посилання поєднуються разом за допомогою зв'язків. Зв'язок позначає залежність між компонентами або між компонентом і зовнішньою сутністю.

З'єднання (wiring). Компоненти поєднуються за допомогою зв'язків, які вказують кожному компоненту, які в нього є джерела інформації і які приймачі. З'єднання описуються декларативно. SCA не вимагає, щоб джерело й приймач мали однакові типи (наприклад, допускається з'єднання Java і WSDL). Для спрощення розробки SCA підтримує автоматичні з'єднання (Autowiring). Поки інформація про посилання однозначна, контейнер має можливість з'єднувати компоненти під час виконання.

Зв'язування (binding). Модель SCA здійснює комунікацію між сервісами й посиланнями за допомогою механізму зв'язування, що підтримує безліч технологій. Всі сумісні зі специфікацією SCA реалізації повинні підтримувати SCA Service Binding і WebService Binding. Зв'язування використовуються сервісами й посиланнями. Сервіси

використовують зв'язування для визначення того, як вони можуть викликатися. Посилання використовують зв'язування для визначення того, як вони можуть викликати сервіси.

Композит. Компоненти групуються в композити. Залежно від опису, композит може використовуватися як сервіс або як новий компонент. У такий спосіб SCA підтримує рекурсивне складання.

Quality of Service (QoS) і механізм політик

Для реалізації QoS і нефункціональних вимог модель SCA пропонує механізм політик (Policy Framework). Політики можуть використовуватися для забезпечення безпеки, доступності, транзакційності й реалізації інших вимог.

Політики можуть бути асоційовані з кожним компонентом. Сервіси й посилання можуть мати множинні політики для забезпечення різних способів доступу. Основні елементи механізму політик це Наміру (Intents), Профілі (Profiles) і Безлічі політик (Policy Sets).

Намір – це абстрактне твердження про обмеження QoS для реалізації компонента. Наприклад, повідомлення може бути конфіденційним, відповідно визначається намір з назвою confidentiality.

Профайл – це набір найменувань намірів. Наміри, на які посилається Профайл, відображаються на конкретні реалізації в безлічі політик.

Безліч політик відповідає реалізації Намірів. Визначає специфічне для технології обмеження на елементи в моделі складання. Наприклад, описує використання інфраструктури публічних ключів для реалізації шифрування.

В Oracle SOA Suite політики можна додавати до компонентів як під час розробки за допомогою JDeveloper, так і під час роботи за допомогою Enterprise Manager'a.

Відмінність SCA від ESB

З технічної точки зору SCA описує трохи іншу площину, ніж ESB і JBI (JSR 208 – Java Business Integration). Якщо ESB концентрується на інтеграції окремих сервісів і існуючих додатків, а також на використанні інфраструктурних сервісів трансформації й маршрутизації даних, то SCA призначений для реалізації внутрішньої архітектури додатків.

Попросту говорячи, сервісна шина підприємства – це концепція проміжного ПЗ, а сервісні компоненти – це концепція розробки бізнес-додатків.

Докладніше про те, як зробити правильний вибір між SCA і ESB, можна прочитати в статті Інтеграція: Oracle Service Bus vs Oracle SOA Suite.

Реалізації SCA

Ситуація з реалізацією SCA нагадує ситуацію зі специфікацією EJB у часи EJB 2 і більше ранні: специфікація є, є опис того, як її потрібно реалізовувати, є набір просторів імен, анотацій, інших артефактів, але кожний виробник програмного забезпечення однаково реалізує специфікацію по-своєму, вносить свої простори імен, конфігураційні файли й т.д. У підсумку композит, розроблений для однієї реалізації SCA, може не працювати під іншою реалізацією.

Реалізації SCA:

- Oracle SOA Suite, Oracle BPM Suite.
- JDeveloper – дизайнер для Oracle SOA Suite.
- IBM WebSphere Application Server V7.0 Feature Pack for SCA.
- IBM Rational Application Developer for WebSphere – дизайнер для IBM WebSphere AS Feature Pack for SCA.
- Apache Tuscany.
- Eclipse SOA Tools Platform Project (STP) – дизайнер з відкритим вихідним кодом.
- Infiniflow Distributed Service Framework (DSF) from Paremus.
- Service Component Architecture (SCA) Framework for SOA from Covansys.
- ActiveMatrix Service Grid from TIBCO.

- SCA Component for Ruby with IBM WebSphere Process Server.
- Fabric3.
- FraSCAti.
- The Newton Project.
- The Mule Project (MuleSCA).
- Eclipse Persistence Services Project (EclipseLink) – реалізація SDO.

Розробка структурної схеми

В SCA код бізнес-додатку може бути організований для SOA у вигляді компонентів, що реалізують бізнес-логіку. Ці компоненти експортують свої функції за допомогою інтерфейсів служб і можуть викликати функції інших компонентів теж за допомогою інтерфейсів служб, називаних посиланнями на служби.

Специфікація SCA визначає правила моделювання інтерфейсу служби. Інтерфейс служби – це границя між двома частинами додатка SOA. Інтерфейс служби вказує, що саме реалізує провайдер служби (SOA-SP) і що може викликати координатор (SOA-SC). Інтерфейс служби SCA – це справжній інтерфейс, що реалізований у вигляді документа WSDL або інтерфейсу Java

Реалізація провайдеру служби в SCA називається компонентом служби. Реалізація компонента служби може бути одним з наступних об'єктів:

- Об'єкт Java (POJO або SLSB (див. Як реалізувати службу в J2EE)).
- Неавтоматизоване завдання.
- Набір бізнес-правил.

Реалізація служби й клієнти служби

Реалізація служби – це конкретна реалізація бізнес-логіки для надання й/або споживання служб. Реалізація є підлеглою стосовно бізнес-процесу. Реалізація може надавати службу у вигляді набору операцій інтерфейсу, використовуваного іншими компонентами.

Реалізація служби може також використовувати інші служби, називані посиланнями на служби й, що вказують на залежність реалізації від сторонніх служб. Реалізація може мати одне або кілька властивостей, які можливо налаштовувати. Властивість – це значення даних, що може задаватися зовнішнім способом і впливати на функцію реалізації.

Звичайно служби SCA використовують дані для параметрів і значень, що повертаються, оформлені у вигляді документів, і ці параметри рекомендується представляти у вигляді об'єктів дані служби (SDO). Додаткова інформація наведена в розділі Ресурси. Служби, посилання й властивості – аспекти реалізації, що налаштовується. В SCA їхня сукупність називається типом компонента.

Посилання настроюється за допомогою зв'язування посилання із цільовою службою, що буде викликана при обігу реалізації до посилання. При настроюванні властивості також вказується значення даних для цієї властивості. В інфраструктурі SCA одна реалізація може використовуватися для компонування декількох компонентів, що відрізняються настроюванням посилань і властивостей. Компоненти і їхні служби використовуються іншими локальними компонентами або віддалено.

Компонування модуля

Модуль SCA – це сукупність жорстко зв'язаних компонентів, розроблювальних і розгортаються спільно в системі SCA. Він є основною одиницею для побудови нежорстко зв'язаних рішень у системі SCA. Модуль SCA містить ряд компонентів, зовнішніх служб, точок входу й провідників, що зв'язують їх між собою. Модулі надають реалізації служб у системі SCA.

Точки входу визначають відкриті служби, надавані модулем. Вони можуть використовуватися іншими компонентами усередині цього ж модуля або бути доступні

зовнішнім об'єктам. Вони застосовуються для публікації служб, надаваних модулем, із застосуванням зв'язування.

Зовнішні служби усередині модуля представляють вилучені служби, надавані іншими модулями. Вони є зовнішніми стосовно модуля SCA, що використовує цю службу. До зовнішніх служб можуть звертатися компоненти усередині модуля, як до будь-якої служби, надаваної компонентом SCA. Зовнішні служби використовують зв'язування для опису доступу до зовнішніх служб.

Створення проекту SCA

У цьому розділі описана процедура створення проекту SCA (Архітектура компонента системи).

Далі описано, як створюється проект SCA і як він використовується в контексті створення моделі бізнес-служби. Опис наведений у вигляді нумерованого списку, щоб проілюструвати лінійну послідовність подій.

У цьому прикладі передбачається наступне:

- Створено проект Studio.
- Створено проект WebSphere Integration Developer.
- У бізнес-сценарії реалізація бізнес-служби застосовує SCA.
- Це загальний опис. Уважається, що користувач розуміє, як виконувати описувані дії.

Для створення проекту SCA виконаєте наступні кроки:

1) У проекції Бізнес-служба створіть набір додатків.
2) Створіть у цьому наборі додаток.
3) Настройте службу процесу. У службі процесу необхідно вказати ролі.
4) Після створення полів необхідно додати й визначити канал. Наприклад, ця служба може бути зроблена доступної як Web-служба, якщо реалізовано канал між Web-службою й службою процесів.
5) Відкрийте проекцію Бізнес-інтеграція.
6) Відкрийте діаграму компонування. У цій панелі ви зможете зв'язати служби, настроїти всі кінцеві точки й інтерфейси служб, щоб створити потік процесу. Залежно від того, як визначений компонент потоку, користувач служби буде бачити яку-небудь частину операцій, а інші будуть виконуватися у фоновому режимі. Зверніть увагу, що компоненти можуть мати різні зв'язки, наприклад, SCA – інтерфейс. У рамках SCA можна привласнювати компоненти й кінцеві точки по необхідності, а не жорстко з'єднувати компоненти між собою.
7) Створіть діаграму компонування. Додайте в потік компонентів динамічного компоновника там, де це необхідно. Тим самим система зможе динамічно вибирати правильну кінцеву точку на основі позначка-даних, що втримуються в сховище.
8) Припускаючи, що кінцеві точки також будуть компонентами SCA, створіть для кожної окремі компоненти, але не намагайтеся їх приєднати до динамічного компоновнику.
9) Переконаєтеся, що кожний компонент має відповідний інтерфейс, і помістите поруч із ним експорт.
10) Підключите експорт до відповідного компонента.
11) Клацніть правою кнопкою миші на кожному експорті й виберіть **Згенерувати зв'язування** > **Зв'язування SCA**.
12) Налаштувавши всі експорти, збережіть діаграму компонування.
13) Виконавши всі описані дії, протестуйте модель у модулі Composition Studio, щоб познайомитися з інтерфейсами й роботою компонентів усередині процесу.
14) Відкрийте проекцію Бізнес-служба.
15) Імпортуйте модулі SCA з діаграми компонування як складену службу в проект Fabric. Зробіть це, клацнувши правою кнопкою миші на кінцевих точках, а потім клацнувши

на **Створити** > **Складена служба**. У спливаючому вікні виберіть проект, що містить компоненти SCA.

16) Відкрийте дерево кінцевих точок у лівій частині вікна. Там повинні бути показані кінцеві точки для всіх експортів, створених на діаграмі компонування. Результат також буде показаний у вікні Зміни в сховище в правій частині робочої області.

17) Двічі клацніть на кожній кінцевій точці, укажіть протокол SCA і потім укажіть середовище. Збережете всі зміни, щоб не було попереджень.

18) Для тестування служб опублікуйте зміни в сховище бізнес-служб. Після їхнього твердження обновите проект (клацніть правою кнопкою проекті у вікні Зміни в сховище й виберіть **Обновити проект**). Тепер поверніться в проекцію Бізнес-інтеграція й за допомогою функції Перевірити компонент переконаєтеся, що всі динамічні компоновники працюють. По закінченню перевірки знову відкрийте проекцію Бізнес-служба.

19) Розробіть стратегію для служби.

20) Для перевірки своїх припущень протестуйте стратегію за допомогою програми імітації динамічного компонування.

21) Перевірену службу можна опублікувати, відправивши зміни в сховище бізнес-служб.

Необхідно вести офіційну документацію високорівневої динаміки системи безпеки SCA-додатку за допомогою таблиці рішень по безпеці для процесу впровадження SCA. У цій таблиці за допомогою зацікавлених бізнес-учасників всі додатки діляться на три категорії, а саме:

1) Додатки, які будуть входити в архітектуру SCA.
2) Додатки, яким необхідно взаємодіяти з SCA-додатками.
3) Додатки, які не будуть входити в SCA або взаємодіяти з SCA-додатками.

Кожної окремої категорії для наочності добре привласнити визначений колір. Об'єкти в першій категорії позначені червоним, у другій – жовтогарячим, а в третій категорії – жовтим кольором.

Потім робоча група по безпеці ділить додатки за рівнем вимог до безпеки на три категорії – висока, середня й низька безпека. Наприклад, додатки або сервіси, що мають справу з інформацією з ринку й відомостями, які не піддаються розголошенню, потрапили б у більше високу категорію безпеки, тоді як додатки або сервіси, які звертаються тільки до даних, що перебувають у відкритому доступі, можуть бути поміщені в саму нижчу категорію.

З огляду на величезний обсяг інформації, який необхідно зібрати, кількість архітектурних артефактів, які необхідно написати, і конкретні сервіси безпеки SCA-додатку, які необхідно спроектувати, робочій групі по безпеці SCA-додатку варто дотримуватися стандартної схеми процедури Життєвий цикл розробки програмного забезпечення (Software Development Life Cycle, SDLC):

- Ідентифікація вимог до безпеки й обмежень.
- Виявлення й збір вимог до безпеки системи.
- Створення безпечного архітектурного проекту.
- Документація деталізованого безпечного проекту SCA.
- Реалізація SCA (включаючи керування SCA).
- Тестування.
- Розміщення.
- Обслуговування.

На перший погляд ці кроки можуть здатися очевидними, але робітники групи по безпеці рідко дотримують схеми SDLC.

Перш ніж робоча група приступиться до розробки рішень, вона повинна зібрати вимоги до систем. Існують як явні, так і неявні вимоги до реалізацій забезпечення безпеки. Що стосується явних вимог, гарною стартовою точкою буде збір вимог від кожної із

зацікавлених осіб. Відносно неявних вимог до безпеки корисно використовувати інфраструктури забезпечення безпеки, наприклад, тріаду конфіденційність, цілісність і відслідкуємість (confidentiality, integrity, and accountability, CIA); з обліком якої складається список конкретних вимог до всіх систем безпеки. Тріада CIA являє собою широко використовувану модель гарантування інформації (information assurance, IA), що визначає конфіденційність, цілісність і доступність як основні характеристики безпеки всіх інформаційних систем.

Члени робочої групи повинні продумати, як дана SCA-реалізація буде забезпечувати конфіденційність системи (приватність даних), і спроектувати точні схеми процесу із вказівкою докладного опису того, яким образом до повідомлень у процесі передачі будуть звертатися тільки авторизовані законні одержувачі, індивідуальні користувачі, процеси або пристрої. Розголошення повідомлень неавторизованим сутностям, наприклад, користувачам-зловмисникам, що здійснюють несанкціоноване перехоплення мережних пакетів, є порушенням конфіденційності, і SCA-реалізації повинні визначати, де й коли в границях всієї системи буде використовуватися криптографія.

Аналогічно, моделі безпеки SCA-додатку вимагають дотримання цілісності, або гарантії того, що повідомлення не було змінено в процесі передачі. Система безпеки SCA-додатку відповідає за забезпечення того, що інформація не була змінена в процесі передачі від джерела до одержувача (цілісність даних) і за гарантування того, що відправник цієї інформації є тим, за кого себе видає (цілісність джерела); і одержувач також є тим, за кого себе видає (цілісність одержувача). Цілісність даних може бути скомпрометована, якщо інформація навмисне або випадково ушкоджена або змінена до того, як неї прочитав законний одержувач. Цілісність джерела вважається скомпрометованою в тому випадку, якщо агент фальсифікує особисті дані й відправляє некоректну інформацію одержувачеві. Для забезпечення цілісності даних використовуються такі механізми, як алгоритм хешування й цифрові підписи.

Крім того, одним з вимог безпеки SCA-додатку є своєчасний і надійний доступ до сервісів даних для авторизованих користувачів (доступність). SCA-реалізації повинні гарантувати, що ці ресурси або інформація будуть доступні, коли в них виникне необхідність; це означає, що доступ до ресурсів може бути здійснений на швидкості, достатньої для того, щоб віддалена система могла виконати своє завдання запропонованим образом. Безумовно, можливі випадки, коли заходи щодо захисту конфіденційності й цілісності прийняті, але атакуючий проте може зробити ресурси менш доступними, чим потрібно, або взагалі недоступними. Зокрема, коли як брокер повідомлень використовуються компоненти SCA-системи, такі як ESB, то для забезпечення її доступності й надійності необхідно вказати в документації вимоги до безпеки SCA-додатку, що необхідно використовувати протоколи високої доступності, мережні архітектури з резервуванням і апаратне забезпечення системи, що не має ні однієї одиночної точки відмови. Робоча група по безпеці SCA-додатку повинна забезпечити всеосяжне виявлення всіх зазначених областей і гарантувати, що відповідні контрольні приклади будуть задокументовані й зможуть проілюструвати визначені вимоги.

Після того як робоча група по безпеці SCA-додатку приділила якийсь час обговоренню всіх описаних вимог, члени групи повинні з'ясувати, чи не можна виконати їх за допомогою інструментів сторонніх виробників. Вони повинні написати програми сервісів безпеки SCA, які будуть задовольняти конкретним вимогам. Щоб не винаходити колесо, краще й корисніше ознайомитися із уже наявними моделями й довідатися, які розробки вже були зроблені до того, як дана робоча група перейшла до етапу високорівневого проектування. Нижче представлений список і опис звичайний використовуваних службових сервісів, які можуть придатися в SCA-реалізації. Більш докладно приводиться список:

1) сервіс аудита загального призначення;
2) сервіс авторизації для керування доступом;
3) сервіс забезпечення конфіденційності;

4) сервіс конверсії повноважень доступу;
5) сервіс поновлення повноважень доступу;
6) сервіс делегування;
7) сервіс спостереження за периметром міжмережного екрана;
8) сервіс установлення особистості;
9) сервіс зіставлення особистості;
10) сервіс забезпечення інформаційної цілісності;
11) міждомений сервіс безпеки;
12) сервіс забезпечення неможливості відмови від авторства;
13) сервіс маршрутизації й QoS (гарантованої якості обслуговування);
14) сервіс настроювання політик безпеки;
15) сервіс зміни політик;
16) сервіс забезпечення приватності;
17) сервіс для роботи із профілем (сервіс користувальницьких профілів);
18) сервіс забезпечення якості встановлення особистості;
19) сервіс захисту від атак відмови в обслуговуванні (denial of service, DoS);
20) сервіс керування забезпеченням безпеки;
21) сервіс узгодження протоколів;
22) сервіс оцінки доступності сервісів безпеки;
23) сервіс єдиного входу в систему;
24) сервіс установлення довіри.

Можливо, вам знадобляться не всі ці сервіси. Співробітники робочої групи по безпеці SCA-додатку повинні зрівняти вимоги з кожним сервісом, потім створити модель безпеки SCA для всіх сервісів, необхідних для задоволення вимог.

Після того як будуть виконані описані дії й буде зібрано досить інформації, можна перейти перегляду стандартів WS-Security і з'ясувати, які з них застосовні до вашої конкретної реалізації безпеки SCA-додатку.

Як тільки моделі стануть деталізованими, необхідно вивчити докладні стандарти безпеки SCA-додатку, що входять в WS-Security, і зрозуміти, як вони співвідносяться один з одним і з вимогами до моделі безпеки SCA-додатку. Ці стандарти безпеки будуть використовуватися для формування безпечних повідомлень у всієї SCA-реалізації.

Опис технології WS Security

Надаючи вільно зв'язані сервіси, сервіс-орієнтована архітектура дозволяє гнучко реагувати на постійно мінливі ділові процеси. При цьому необхідно приділити увагу не тільки функціональним аспектам, але й створенню гнучкої інфраструктури безпеки, оскільки зміни ділових процесів роблять на неї серйозний вплив. Приміром, залучення нових ділових партнерів або включення конфіденційних відомостей у важливі корпоративні процеси вимагає адекватного стандартизованого рішення для забезпечення безпеки.

Як основна технологія забезпечення безпеки повідомлень на базі SOAP (Simple Object Access Protocol) міцно закріпився стандарт безпеки служб Web (Web Services Security, WS Security), ратифікований OASIS, організацією по розвитку стандартів структурованої інформації. WS Security складається із цілого пакета специфікацій і безлічі механізмів, які комбінуються відповідно до необхідного сценарію застосування.

До честі творців стандартів у рамках SCA вони приділили підвищену увагу безпеки при розробці цих стандартів. Механізми безпеки органічно вбудовуються в концепцію Web-сервісів і дозволяють не тільки уникнути основних проблем, але й істотно підвищити ефективність як механізмів захисту, так і засобів керування політикою безпеки.

Стандарти

Основний пул стандартів безпеки Web-сервісів розробляється в рамках консорціуму OASIS. Структуру специфікацій безпеки SCA можна зобразити у вигляді наступної ієрархічної конструкції.

Розглянемо ці стандарти:

1) Базові стандарти (SOAP Foundation) містять у собі специфікації XML Signature і XML Encryption, які визначають відповідно формати ЕЦП і шифрування SOAP-транзакцій. Дані специфікації ніяк не обмежують список алгоритмів шифрування й ЕЦП, що робить вбудовування українського ДСТУ в SCA-архітектуру неважким завданням. Також до базових понять можна віднести інформацію в складі SOAP-заголовка (security-token, маркер безпеки), використовувану для автентифікації й авторизації запиту. Наприклад, security-token може містити в собі сертифікат X.509 і/або ім'я/пароль. Одним з видів security-token є SAML (Security Assertion Markup Language), що включає в себе інформацію про статус автентифікації, авторизації й атрибутах учасників транзакції. Це дозволяє забезпечити побудову відносин довіри (trust) в SCA-архітектурі й виключити необхідність автентифікації/авторизації для кожного запиту.

2) WS-Security визначає базові механізми й формати використання security-token у складі SOAP-запитів. Основною метою WS-Security є абстрагування реалізації політик безпеки Web-сервісів від конкретних методів (наприклад, протоколів автентифікації й авторизації). За допомогою уточнюючих специфікацій, описаних нижче, WS-Security дозволяє досягти сумісності методів реалізації політик безпеки, описаних з використанням даних стандартів.

3) WS-Policy визначає шаблони й правила опису політики безпеки для Web-сервісів.

4) WS-Trust описує правила організації довірених відносин між учасниками Web-взаємодії.

5) WS-Privacy визначає формати політики конфіденційності при обміні SOAP-повідомленнями.

6) WS-SecureConversation регламентує правила безпечного обміну повідомленнями в SCA-архітектурі.

7) WS-Federation є специфікацією, що визначає встановлення довірених відносин між різними доменами безпеки.

8) WS-Authorization описує формати опису правил розмежування доступу до Web-сервісів.

Отже, стає ясно, що безпека в SCA-архітектурі описується досить великим набором специфікацій. Втішно, однак, що даний набір є невід'ємною частиною пула стандартів SCA і розробляється одночасно з ним. Це дає підстави думати, що додатки в складі Web-сервісної архітектури можуть створюватися безпечними вже на стадії проектування.

Архітектура

Розглянемо тепер типову архітектуру безпеки Web-сервісів, що застосовується в більшості рішень корпоративного рівня.

Ключові завдання, покладені на таку архітектуру:

– Керування доступом до Web-сервісів і однократна автентифікація (Single Sign-on, SSO). Призначено для забезпечення однократної автентифікації, авторизації й аудита Web-сервісів.

– Централізоване керування політикою безпеки. Дозволяє мінімізувати необхідність дублювання зусиль для застосування політики безпеки для кожного Web-сервісу за допомогою використання централізованої інфраструктури безпеки, не вимагаючи при цьому переробки самих Web-сервісів.

– Уніфікація процесу моніторингу. Дозволяє проводити аудит роботи Web-сервісів, що показує, які користувачі (додатка) здійснювали доступ до Web-сервісів, які дії вони виконували і які дані при цьому передавали.

– Маршрутизація запитів до Web-служб. Дозволяє, аналізуючи вміст запиту, проводити його перетворення й перенапрямок до того або інший Web-сервісу.

Схема керування захистом в SCA-архітектурі

До складу такої схеми входять наступні компоненти:

- менеджер політик (Policy Manager);
- компоненти застосування політики: агенти (Agents) і шлюзи (Gateways);
- панель моніторингу (Monitor).

Менеджер політик – це графічний інструмент для визначення нових політик безпеки й експлуатації, зберігання політик, а також для керування поширенням і відновленням політик на агентах і шлюзах.

Компоненти застосування політик діляться на шлюзи (Policy Gateways) і агенти (Policy Agents). Шлюзи політик установлюються перед групою додатків або сервісів, перехоплюючи запити до цих додатків з метою застосування політик, підвищуючи безпеку вже встановлених додатків і додаючи в них нові правила. Агенти політик забезпечують додатковий диференційований рівень безпеки й розміщаються на серверах додатків, що забезпечують виконання додатка або сервісу. Таким чином, забезпечується можливість автентифікації й авторизації запитів до Web-сервісів по наявним на підприємстві репозитаріям користувачів (наприклад, LDAP-каталог).

На панелі моніторингу адміністратор може задати рівні якості обслуговування для кожного додатка, визначити правила видачі попереджень і повідомлень, якщо додаток перевищить заданий рівень якості обслуговування.

Таким чином, архітектуру безпеки SCA можна побудувати без переробки безпосередньо Web-сервісів. Це одне з основних достоїнств наявності стандартів безпеки, що є частиною загального пула стандартів SCA.

Базові концепції

OASIS прийняла стандарт WS Security у березні 2004 р. як доповнення до протоколу SOAP. До теперішнього часу він визнаний цілком зрілим і придатним до застосування. WS Security не визначає ніяких нових технологій, а опирається на вже існуючі стандарти, приміром, XML Encryption, XML Signature, сертифікати X.509 або різні криптографічні алгоритми. Базова концепція ґрунтується на механізмах повідомлень, тому замість захисту, орієнтованої на транспорт, можливе забезпечення безпеки від краю до краю (End-to-End Security), приміром, за допомогою протоколу SSL. Такий підхід необхідний, щоб уникнути виникнення наскрізних комунікаційних структур у межах SCA, а також забезпечити передачу асинхронних повідомлень або використання проміжних станцій (приміром, сервісної шини підприємства – Enterprise Service Bus, ESB).

Основне завдання WS Security – забезпечення цілісності, конфіденційності й автентичності повідомлення і його відправника при одночасному збереженні відкритості для розширень. Основними елементами стандарту є наступні базові механізми: токени безпеки, шифрування, підписи й оцінки про час.

Токени безпеки (Security Token). Автентифікація відправника – базова передумова для забезпечення контролю доступу (Access Control) з боку сервісу, а крім того, вона необхідна для організації обліку й контролю. Підтвердження ідентифікації (Credentials), без яких неможлива автентифікація, передаються усередині повідомлення у вигляді токенів. Сама автентифікація не входить до складу WS Security – це самостійний процес провайдеру послуг. Для різних форматів токенів OASIS пропонує окремі специфікації у вигляді профілів WS Security. Так, «Профіль токена з ім'ям користувача» (Username Token Profile) регулює алгоритм широко розповсюдженого методу автентифікації користувача за допомогою ідентифікаційного номера (User ID) і відповідного пароля.

Ідентифікація додатків або ділових процесів звичайно здійснюється за допомогою сертифікатів, і в цьому випадку управляти паролями на стороні клієнта не потрібно. Обіг із сертифікатами для зазначеного методу автентифікації описується в профілі X.509 Certificate Token Profile. Існують і інші профілі, приміром, для використання токенів мови розмітки тверджень безпеки (Security Assertion Markup Language, SAML) або Kerberos.

Двійкові або базовані на XML токени безпеки потрібні не тільки для автентифікації. Вони виконують ще одну функцію, являючи собою основу для транспорту або прив'язки ключів (Keys), застосовуваних у криптографії.

Шифрування

Щоб забезпечити захист конфіденційних даних, використовується криптографічне шифрування. Оскільки протокол SOAP базується на XML, то WS Security не визначає новий стандарт, а використовує специфікацію XML Encryption з W3C. Зашифровані дані і їхня метаінформація, у свою чергу, включаються в повідомлення у вигляді структур XML. Однак, відповідно до специфікації SOAP, не можна шифрувати елементи «конверт» (Envelope), «заголовок» (Header) і «тіло» (Body), оскільки вони задають структуру повідомлення й повинні бути читаємі завжди.

Принципово розрізняють два механізми шифрування: симетричне й асиметричне. При симетричному шифруванні (метод «секретного ключа» – Secret Key) для шифрування й дешифрування використовується загальний ключ, завжди доступним обом сторонам. При асиметричному шифруванні (алгоритм із відкритими ключами – Public Key) для шифрування й дешифрування застосовуються різні ключі, що істотно скорочує витрати зусиль на їхній розподіл: особистий ключ (Private Key) залишається у власника, а загальний ключ (Public Key) поширюється вільно. Однак у порівнянні із секретними ключами механізм відкритих ключів працює значно повільніше, тому обидва підходи часто поєднують, у результаті чого з'являються нові гібридні варіанти. Клієнт генерує симетричний ключ сеансу (Session Key) і використовує його для симетричного шифрування більших обсягів даних. На закінчення симетричний ключ шифрується за допомогою асиметричного алгоритму, вкладається в повідомлення й надається в розпорядження сервісу.

Підпис (Signature)

Для підтвердження цілісності повідомлень застосовуються підписи. Вони дозволяють розпізнати неправомірні модифікації: зміна, видалення або додавання даних. Реалізація цього підходу в рамках WS Security опирається на стандарт XML Digital Signature від W3C. Принцип підписів заснований на створенні контрольних сум за допомогою спеціальних алгоритмів (дайджет). Результати приєднуються до повідомлення й передаються в частково зашифрованому виді. Сервісна сторона формує контрольну суму й порівнює неї зі значенням, присланим клієнтом. Оскільки в XML різні способи написання логічно ідентичні, перед формуванням контрольної суми необхідно зробити нормалізацію даних. Для цього використовуються стандартизовані алгоритми XML Canonicalization, також запозичені з W3C.

Крім того, підпису надають можливість установлення автентичності відправника. Цю інформацію можна використовувати в юридичних цілях для встановлення авторства.

Оцінка про час (Timestamp)

Ідея послуг у рамках SCA має на увазі, що сервіси повинні робити визначену дію й у такий спосіб підтримувати взаємодію без обліку стану (Stateless). Однак даний принцип комунікації без установлення сеансу відкриває простір для атак скидання (Replay), що коли атакує повторно відправляє або повідомлення цілком, або окремі їхні частини. Щоб перешкодити таким атакам, необхідно гарантувати унікальність повідомлень, для чого кожне з них одержує свій ідентифікаційний номер (Message ID), що сервіс перевіряє на предмет його унікальності. Тому ідентифікаційні номери вже отриманих повідомлень необхідно зберігати. Термін дії, а виходить, і час зберігання окремих ідентифікаційних номерів повідомлень на стороні сервісу обмежується оцінкою, що втримується в повідомленні, про час.

Крім використання традиційної структури оцінок про час у заголовку безпеки (Security Header), токен з ім'ям користувача пропонує власне керування оцінками про час щоб уникнути несанкціонованого повторного використання даних для автентифікації. Ідентифікаційний номер повідомлення повинен відповідати специфікації WS Addressing. А токени з ім'ям користувача одержують випадкове криптографічне значення (Nonce).

У рамках SCA кожний зі згаданих чотирьох базових механізмів охоплює лише один аспект забезпечення безпеки. Сформувати цілісне рішення можна лише за умови взаємодії всіх компонентів. Цілком традиційна комбінація механізмів безпеки на основі повідомлень (WS Security), орієнтованих на транспорт (SSL).

Автентифікація

Будь-який контроль доступу на стороні сервісу припускає автентифікацію клієнта. Сервісній стороні необхідно мати відомості про підтвердження ідентифікації. У випадку методу з користувальницьким ідентифікаційним номером і паролем WS Security надає механізм токенів з ім'ям користувача, де пароль є конфіденційною інформацією, тому необхідно запобігти його зчитуванню в процесі транспорту. Шифрування необхідно, навіть якщо механізм, визначений у специфікації токенів з ім'ям користувача, припускає передачу пароля тільки у вигляді контрольної суми. При використанні контрольної суми, що читається, виникає погроза атаки методом підбора пароля (Brute Force) шляхом перевірки всіх можливих комбінацій, оскільки паролі обмежені по довжині й набору символів.

Крім того, у випадку застосування контрольної суми пароля сервісній стороні знадобиться пароль відкритим текстом. Тому даний підхід у багатьох випадках неприйнятне або адміністрування паролів зажадає додаткових заходів безпеки.

Конфіденційність

Запобігти розкраданню пароля під час пересилання повідомлення покликане шифрування токену з ім'ям користувача. У деяких випадках досить застосувати широко розповсюджений протокол SSL. Однак необхідно врахувати, що внаслідок принципу з'єднання двох точок, властивого SSL, використання проміжних вузлів, приміром, сервісної шини підприємства (Enterprise Service Bus, ESB), неможливо, і захист даних після їхньої передачі не забезпечується.

У той же час механізм шифрування WS Security надає метод на основі повідомлень: вихідні дані шифруються й заміняються за допомогою алгоритму шифрування XML. Додатково в повідомлення вкладається метаінформація, приміром, про використані алгоритми або ключі, і тепер воно може передаватися навіть за допомогою незахищених протоколів (приміром, HTTP), а конфіденційність даних не піддається погрозі.

Цілісність

У використаному як приклад сценарії відсутній зв'язок між токеном з ім'ям користувача, що перебуває в заголовку SOAP, і даними в тілі SOAP. У результаті виникає погроза підміни ключових елементів повідомлення. Зокрема, зашифрована інформація про користувача, зазначена в заголовку, може бути постачена підробленим запитом сервісу. Однак ця проблема легко вирішується за допомогою підписів. Механізми підписів, використовувані в WS Security, «скріплюють» трохи просторово розділених блоків даних, з яких складається повідомлення, що дозволяє перевірити цілісність усього повідомлення або окремих його частин. У контексті безпеки на базі повідомлень підпису виконують роль елементарних конструктивних компонентів і зачіпають не тільки тему цифрових підписів.

Унікальність повідомлення

Для того щоб запобігти повторному відправленню повідомлення (атака Replay), на сервісній стороні необхідно перевірити унікальність повідомлення. Для цього до повідомлення, представленому в стандартизованому виді, додається ідентифікаційний номер. Стандарт WS Addressing, визначений в W3C, передбачає, серед іншого, завдання ідентифікаційного номера повідомлення, що допомагає встановити його унікальність. Визначена в рамках WS Security структура вказує час створення повідомлення й закінчення строку його дії.

На закінчення потрібно відзначити, що ідентифікаційні номери повідомлень, як і оцінки про час, повинні бути прив'язані до існуючих блоків даних (інформація про користувачів і дані повідомлень). Для цього потрібно розширити діапазон охвату підпису, що дозволяє включити нові елементи при контролі цілісності.

Підписи і їхні завдання

Завдяки своїй інфраструктурі на основі повідомлень, сервіси Web підтримують можливість включення будь-яких проміжних інстанцій (Intermediaries) між кінцевими точками. С допомогою такої архітектури можна розширити функціональність сервісів Web. Крім того, ця архітектура стає основою для організації поділу відповідальності за реалізацію властивостей сервісу, особливо вимог, не пов'язаних з функціональністю (якість сервісу – Quality of Services, QoS). При виклику сервісу повідомлення із запитом і відповіддю повинні пройти через проміжні інстанції, причому кожна витягає з повідомлення дані, необхідні для виконання її завдань, і, якщо знадобиться, постачає його додатковою інформацією. Відповідно, необхідно, щоб визначені частини повідомлень були придатні для читання й зміни проміжними інстанціями. Так, за допомогою даних WS Addressing з повідомлення можна управляти функціями маршрутизації в межах ESB.

Для забезпечення конфіденційності й цілісності повідомлення, з одного боку, і читаності й розширюваності, з іншої, до механізмів безпеки пред'являються підвищені вимоги. Приміром, шифрування всього повідомлення за допомогою протоколу SSL перешкоджало б гнучкому використанню проміжних інстанцій. Крім того, стандарт SOAP вимагає, щоб конверт, заголовок і тіло повідомлення представлялися в незашифрованому виді.

Підписи виконують кілька важливих завдань для забезпечення всебічної безпеки в рамках такої вільно зв'язаної архітектури. Крім загальновідомої ролі цифрового підпису, вони надають механізми для перевірки цілісності й автентичності частин повідомлення. Через основну роль підписів необхідно бути в курсі їхніх базових принципів.

Цілісність даних

Підпису, крім іншого, дозволяють перевірити цілісність окремих блоків даних і розпізнати маніпуляції з повідомленнями (зміна, видалення й додавання даних). Для цього за допомогою спеціального криптографічного алгоритму створення хешу (приміром, SHA1, MD5) розраховуються контрольні суми для важливих блоків даних (Message Digest). Хеш-алгоритми – необоротні функції, і відновлення вихідних даних за відомим значенням хешу неможливо. Крім того, його величина для різних даних не повинна збігатися (відсутність колізій). Для перевірки хеша приймаюча сторона ще раз розраховує контрольну суму й порівнює отриманий результат із присланим. Якщо обоє значення ідентичні, то цілісність даних дотримана, тоді як в інших випадках велика ймовірність змін повідомлення. Однак цей механізм не дозволяє встановити, які саме зміни внесені, оскільки підпису повідомляють тільки про вірний або невірний результат.

Принцип підписів базується на формуванні контрольних сум обома сторонами (відправником і одержувачем), тому однакова форма подання даних є обов'язковою умовою. Приміром, для того щоб різне написання XML не привело до різниці контрольних сум, варто ввести проміжний етап – нормалізацію XML (Canonicalization).

Однак одного доказу цілісності окремих блоків даних недостатньо для підтвердження автентичності всього повідомлення – потрібно забезпечити єдність окремих блоків. Для цієї мети створюється загальна контрольна сума шляхом об'єднання значення хешу для всіх блоків даних. У результаті здійснюється криптографічний зв'язок блоків, що не залежить від їхнього положення усередині повідомлення: таким чином, загальна контрольна сума дає можливість перевірити автентичність усього повідомлення. Крім того, так можна розпізнати маніпуляцію зі значеннями хешу окремих блоків даних. У процесі транспорту повідомлення загальна контрольна сума захищається від зміни за допомогою криптографічного механізму шифрування. Для реалізації автентичності повідомлення можна застосовувати симетричне шифрування (приміром, HMAC). При цьому ключ, спільно використовуваний відправником і одержувачем, або передається заздалегідь, або створюється відправником у момент передачі, а потім відправляється в зашифрованому виді разом з повідомленням.

Крім перевірки цілісності даних і автентичності повідомлень, підпису надають можливість автентифікації відправника всього повідомлення або його частин.

Це властивість відомо як цифровий підпис. У цьому випадку застосовується не симетричний алгоритм шифрування загальної контрольної суми, а асиметричний алгоритм із застосуванням відкритих ключів: відправник використовує власний ключ для шифрування значення хешу, а прочитати його можна лише за допомогою відкритого ключа, сертифікат якого надає інформацію про власника особистого ключа. Якщо сертифікат, а виходить, і відкритий ключ, викликає довіру, то з його допомогою можна визначити відправника повідомлення.

Виводи

На перший погляд, набір стандартів і реалізація архітектури безпеки в SCA здаються нетривіальними. Але його переваги переважують всі складності опису й реалізації. До них відносяться:

- ❖ Відділення політики безпеки сервісів від самих сервісів дозволяє побудувати універсальні сервіси захисту для всіх бізнес-додатків без необхідності втручання в бізнес-логікові й "прошивання" функцій безпеки в код бізнесів-додатків.
- ❖ Чітке розмежування експертизи. Розроблювачі сервісів формують бізнес-логіку, архітектори й адміністратори визначають політику безпеки й керування.
- ❖ Єдина точка керування політикою ІБ.
- ❖ Зниження витрат на адміністрування, оскільки зміни в політику безпеки вносяться централізовано, а не в кожному Web-сервісі. Крім того, аудит безпеки для всіх сервісів ведеться з єдиної точки адміністрування.
- ❖ Спрощення підтримки й внесення змін у середовище керування й забезпечення безпеки Web-сервісів за рахунок використання єдиних сервісів безпеки для всіх Web-сервісних додатків.

Визначено, що такий значний набір переваг SCA з погляду безпеки послужить достатнім стимулом для співробітників підрозділів ІБ підтримати зусилля своїх колег з IT-підрозділів по побудові Web-сервісної архітектури.

Одним з найважливіших завдань забезпечення інформаційної безпеки в сервіс-компонентних архітектурах (SCA) є захист потоків корпоративних даних, переданих по каналах загального користування, у тому числі й через Internet. Перспективним методом надійного захисту інформації є метод кодування даних.

Для рішення цього завдання необхідно здійснити кодування інформації на виході з локальної мережі й декодування вхідних у неї даних. Ці функції реалізуються спеціальними програмними або програмно-апаратними засобами. Якщо захист сегмента корпоративної мережі вже забезпечений міжмережним екраном, природно покласти на нього також виконання функцій кодування й декодування.

Для реалізації можливостей кодування/декодування повинне бути виконане попередній (початковий) розподіл ключів. Сучасні технології пропонують для цього цілий ряд методів. Після розподілу ключів з'являється можливість здійснення процесу виробітку спільних секретних ключів, що обслуговують сеанс спілкування абонентів.

У результаті кодування весь обмін даними між територіально-віддаленими локальними мережами є захищеним і для користувачів виглядає як обмін усередині однієї локальної мережі, при цьому від користувачів не потрібно застосування яких-небудь додаткових захисних засобів.

Комплекс кодування міжмережних потоків

Програмний комплекс кодування міжмережних потоків (ККМП) реалізує функції кодування міжмережних інформаційних потоків у мережах передачі даних протоколу TCP/IP для забезпечення обміну інформацією між територіально-віддаленими локальними мережами. Це забезпечується за допомогою організації віртуальних захищених мереж (Virtual Private Networks – VPN).

Комплекс виконує наступні функції:

- ❖ Кодування міжмережних потоків. Функції кодування міжмережних інформаційних

потоків у відкритих мережах передачі даних виконуються шляхом організації VPN. Кожна мережа в складі VPN захищена своїм модулем, що кодує, установлюваним у точці її з'єднання із зовнішніми мережами. Інформація, що захищається, кодується на передавальному модулі й декодується на приймаючому, тобто передається у відкритому виді в межах локальних мереж і в кодованому – за їхніми межами. Кодований трафік передається по протоколу IPsec.

– Створення контуру безпеки. Розроблена система дозволяє сформувати контур безпеки, що поєднує IP-адреси всіх абонентів, що мають доступ у віртуальну захищену мережу. Абонентами VPN можуть бути цілі мережі, підмережі й окремі робітники станції. Крім того, що кодує модуль може бути встановлений на окрему робочу станцію.

– Вибіркове кодування трафіку. Формування контуру безпеки служить для поділу трафіку на кодуємий і некодуємий потоки.

– Модуль, що кодує. Розроблена система робить виділення пакетів, які необхідно кодувати, на підставі IP-адрес відправника пакета й одержувача пакета й, крім того, перевірки інтерфейсу, через який проходить пакет.

– Управління ключовою системою. У розробленій системі реалізована несиметрична ключова система, коли потенційні учасники обміну даними використовують пари довгострокових секретних й відкритих ключів кодування. Кодування здійснюється на основі сеансових ключів, автоматично сформованих за допомогою довгострокових ключів і що мають обмежений час життя. Комплекс здійснює всі необхідні дії по управлінню ключами: генерацію й розподіл довгострокових ключів, виробіток сеансових ключів абонентів, сертифікацію відкритих ключів у довіреному центрі, планову й позаштатну зміну ключів кодування.

– Реєстрація подій, моніторинг і управління міжмережними потоками. Розроблена система здійснює збір і зберігання статистичної й службової інформації про всі штатні й позаштатні події, що виникають при автентифікації вузлів, передачі кодованої інформації, обмеженні доступу абонентів ЛОМ. Засоби моніторингу проводять збір і аналіз протоколів реєстрації від всіх модулів комплексу по кодованому каналі.

– Захист з'єднань із мобільними клієнтами. До складу віртуальної захищеної мережі можуть входити мобільні користувачі – віддалені комп'ютери, що підключаються по виділеним або каналам зв'язку, що комутуються. Основною відмінністю Мобільного клієнта є динамічно-призначувана IP-адреса. Носієм ключової інформації для них є електронний ключ eToken.

Склад Комплексу

Комплекс складається з наступних компонентів:

1. Набір шлюзів кодування.
2. Центр генерації ключів.
3. Центр розподілу ключів.
4. Центр реєстрації мобільних клієнтів.
5. Центр підготовки електронних ключів мобільних клієнтів.
6. Мобільний клієнт.
7. Центр моніторингу.
8. Програма контролю цілісності.

Шлюз із модулем, що кодує/декодувальним

Шлюз є основним модулем комплексу, що виконує функції маршрутизації, фільтрації й кодування пакетів. Кожний Шлюз призначений для закриття визначеної групи локальних мереж. На комп'ютері-шлюзі встановлюється ядерний модуль с функціями кодування й декодування й запускається програма автентифікації. Функціями шлюзу є:

- ❖ Фільтрація трафіку (розподіл на кодуємий/некодуємий потоки).
- ❖ Кодування трафіку (кодуємий потік).
- ❖ Автентифікація з іншими Шлюзами.

❖ Реєстрація подій у Центрі моніторингу.

❖ Забезпечення власного захисту.

Центр розподілу ключів

Центр розподілу ключів здійснює управління контуром безпеки, а також виконує наступні функції:

– Одержання зі змінного носія відкритих ключів Шлюзів.

– Видачу будь-якому Шлюзу відкритих ключів будь-яких інших Шлюзів і інформації про відповідні сегменти структури мережі.

– Розсилання Шлюзам повідомлень про зміни структури закритої мережі.

– Вироблення і виконання процедури зміни сеансових ключів.

– Зберігання інформації про структуру мережі.

Центр реалізований у вигляді програмного комплексу, що виконує функції зберігання й видачі відкритих ключів кодування по мережному запиті від модулів кодування. Центр розподілу ключів може бути встановлений або на окремому (виділеному) комп'ютері, або разом з одним зі Шлюзів кодування.

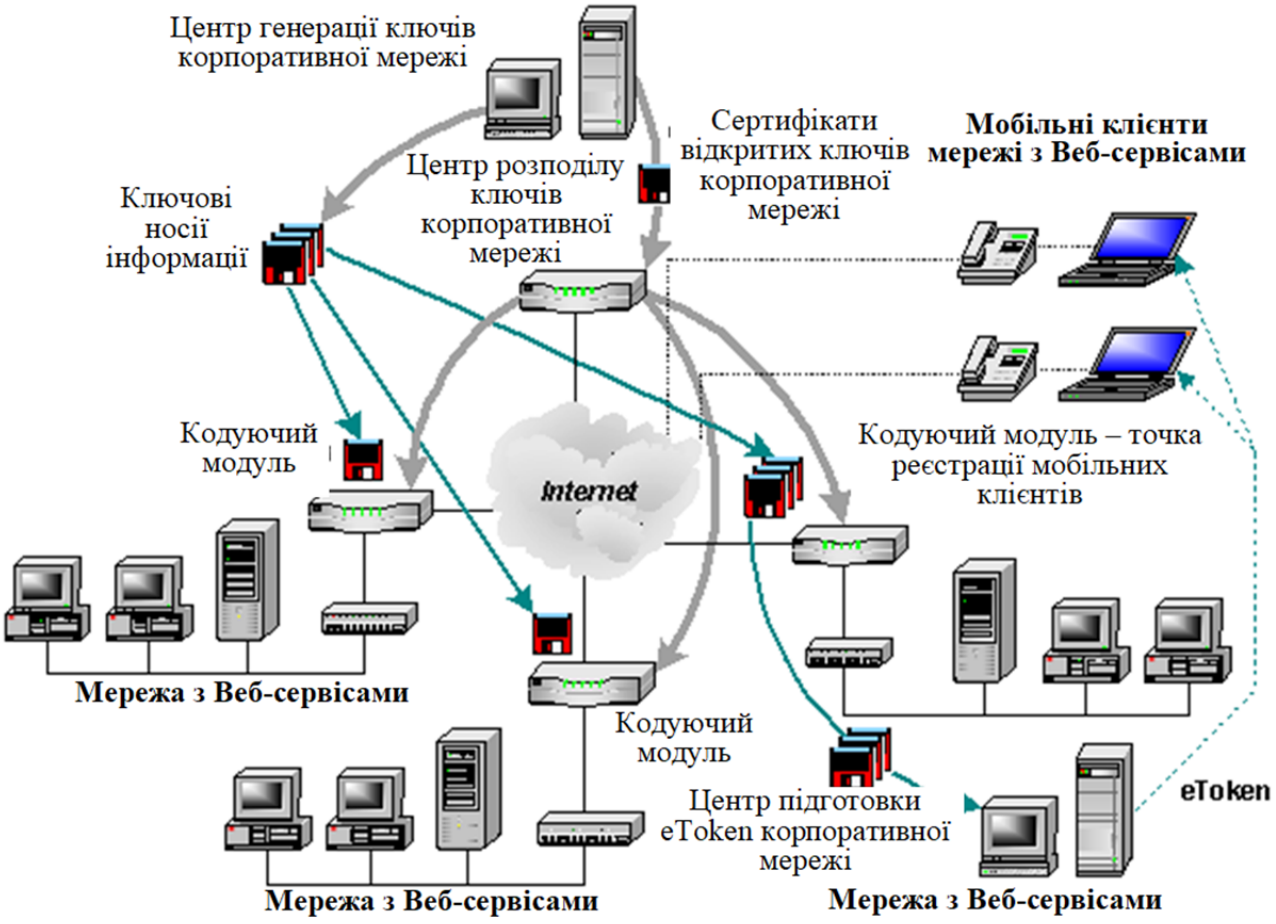


Рисунок 2 – Структурна схема системи

Центр генерації ключів

Даний модуль служить для генерації пар комплементарних ключів, а також є репозитарієм всіх відомих системі ключів. У функції Центра генерації ключів входить:

– генерація пар відкритого й секретного ключів модулів, що кодують;

– генерація пари ключів для сертифікації (еталонного завірення) відкритих ключів модулів, що кодують;

– генерація сертифікатів відкритих ключів, підписаних секретним ключем сертифікації;

– приміщення підписаних сертифікатів відкритих ключів на змінні носії;

– зберігання еталонних копій сертифікованих відкритих ключів в архіві.

Центр генерації ключів – програма, що виконується на ізольованому автоматизованому робочому місці.

Центр реєстрації ключів

Центр реєстрації ключів служить репозитарієм всіх відомих системі ключів. У його функції входить:

– Введення зі змінного носія відкритого ключа.

– Введення зі змінного носія закритого ключа Адміністратора безпеки.

– Підпис нового ключа ключем Адміністратора безпеки.

– Приміщення підписаного відкритого ключа в архів довгострокового зберігання й на змінний носій.

– Зберігання еталонних копій сертифікованих (зареєстрованих) відкритих ключів.

Центр реєстрації ключів виконаний у вигляді програми, що виконується на ізольованому автоматизованому робочому місці й призначеної для сертифікації (еталонного завірення) відкритих ключів.

Центр реєстрації мобільних клієнтів і Мобільний клієнт

Для забезпечення доступу до корпоративних даних, які захищаються, мобільних абонентів, не підключених до локальних мереж, які захищаються, використовується Центр реєстрації мобільних клієнтів і програмне забезпечення мобільного клієнта комплексу.

Центр реєстрації мобільних клієнтів являє собою спеціальний модуль, що кодує, для підключення довільної кількості мобільних клієнтів.

Мобільний клієнт являє собою програмний модуль, що працює під управлінням ОС Windows і використовуючий апаратні ключі для автентифікації абонента в VPN.

Центр моніторингу

Центр моніторингу являє собою мережне автоматизоване робоче місце із установленим на ньому набором програм, що здійснюють збір і аналіз протоколів, що надходять від всіх модулів комплексу.

Програма контролю цілісності

Комплекс містить у собі засобу формування й перевірки контрольних сум файлів. Ці засоби реалізовані у вигляді Програми контролю цілісності, що призначена для визначення й повідомлення системного Адміністратора про зміну, додавання й видалення файлів.

Адміністрування комплексу

Настроювання й адміністрування компонентів комплексу здійснюється централізовано з робочого місця Адміністратора безпеки за допомогою графічного інтерфейсу або командного рядка. Віддалене управління здійснюється по захищеному каналі. Комплекс забезпечує автентифікацію Адміністраторів і розмежування доступу до функцій адміністрування.

Основні особливості комплексу

Основними особливостями розробленої системи є:

– Повнофункціональна схема управління ключами, що дозволяє здійснювати динамічний розподіл ключів з використанням довіреного центра сертифікації, перевірку дійсності ключової інформації й оповіщення систем кодування про компрометацію ключів.

– Висока надійність функціонування, забезпечувана засобами контролю цілісності, протоколювання й аудита, стійкості до збоїв і відновлення у випадку збоїв і відмов.

– Прозорість кодування переданих даних для абонентів і використовуваного ними програмного забезпечення.

– Висока продуктивність (робота в мережі 100 Мбіт/с без істотного впливу на пропускну здатність).

– Забезпечення необхідної якості сервісу (QoS) і підтримка роботи із сервісами, що пред'являють високі вимоги до величин тимчасових затримок (IP-телефонія, відеоконференцзв'язок).

– Можливість використання в комплексі з міжмережними екранами, антивірусними рішеннями й засобами контекстного аналізу.

Використання відкритих стандартів – протокол тунелювання мережних пакетів відповідає стандартам IETF IPsec.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів забезпечення безпеки корпоративної мережі від кібератак. 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 корпоративної мережі від кібератак. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем забезпечення безпеки корпоративної мережі від кібератак; Досліджена система забезпечення безпеки корпоративної мережі від кібератак; На основі отриманих результатів досліджень створена програмна реалізація системи забезпечення безпеки корпоративної мережі від кібератак.Розроблені під час виконання роботи алгоритми дозволяють успішно вирішувати завдання забезпечення безпеки корпоративної мережі від кібератак. 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. 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 621.833

О. Бондаренко, магістр гр. АТ19М
Центральноукраїнський національний технічний університет

ІДЕНТИФІКАЦІЯ ДЕФЕКТІВ ДЕТАЛЕЙ МЕХАНІЧНИХ ТРАНСМІСІЙ АВТОМОБІЛІВ

Встановлено, що найбільш значущими факторами, що впливають на рівень віброакустичного сигналу агрегатів трансмісій є зношення підшипників, бічних поверхонь зубів, порушення мащення в зачепленні, заїдання зубів, викришування, зколювання, тріщини і поломки зубів. Більшість інших факторів є пов'язаними з ними причинно-наслідковими залежностями, це обумовлено особливостями функціонування агрегатів трансмісій. Віброакустичні сигнали є джерелами діагностичної інформації та можуть бути використані при ідентифікації дефектів деталей агрегатів трансмісії та встановленні технічного стану агрегатів.
віброакустичний сигнал, трансмісія, коробка передач

Постановка проблеми. Трансмісія автомобіля є важливим агрегатом при передачі крутного моменту від двигуна до коліс. Агрегати трансмісії повинні функціонувати у всіх режимах експлуатації автомобіля. Втрата працездатності коробки передач призводить до втрати працездатності автомобіля в цілому. У зв'язку з цим, до технічного стану даного агрегату необхідно пред'являти підвищені вимоги, а також необхідно вести систематичний моніторинг, що дає чітке уявлення про поточний технічний стан коробки передач і можливість прогнозування настання відмови даного агрегату трансмісії.

Аналіз останніх досліджень та публікацій. Проблематика, що вирішується в даній роботі була також досліджена в наукових працях [1-4].

Мета і завдання досліджень. *Метою роботи* - є розробка методики віброакустичного діагностування дефектів механічних коробок передач автомобілів при їх експлуатації та ремонті.

Для досягнення поставленої мети вирішувалися наступні задачі досліджень:

1. виконати оцінку впливу дефектів і пошкоджень елементів конструкцій коробок передач на їх віброакустичні характеристики;

2. проаналізувати фактори, що визначають значення віброакустичних характеристик коробок передач;

3. оцінити ступінь інформативності віброакустичних сигналів при характерних дефектах.

Об'єкт дослідження – механічні коробки передач автомобілів.

Предмет дослідження – коливальні процеси, породжувані дефектами деталей коробок передач.

Методи досліджень базуються на методах обробки віброакустичних сигналів.

Механічні трансмісії, які встановлюються на сучасні автомобілі, мають багато загальних елементів конструкції, таких як шестерні, вали, підшипники. Тому, можливо виділити загальні несправності механічної коробки передач, характерні для будь-якої конструкції чи моделі автомобіля.

Умовно їх можна розділити на несправності власне коробки передач і несправності механізму перемикання передач. До загальних несправностей коробки передач відносяться:

- зношення муфт синхронізаторів;

- зношення шліцьових з'єднань муфт синхронізаторів;
- зношення шестерень;
- знижений рівень масла в коробці;
- зношення підшипників ведучого, веденого та проміжного валів;
- ослаблення різьбових з'єднань кріплення коробки передач;
- зношення сальників.

Основними причинами зазначених несправностей є:

- порушення правил експлуатації (використання неякісного масла, робота автомобіля з несправним зчепленням);
- низька якість комплектуючих;
- граничний термін служби коробки передач;
- некваліфіковане проведення робіт з технічного обслуговування і ремонту коробки передач.

Деякі несправності коробки передач можна встановити за зовнішніми ознаками:

- шум коробки передач;
- ускладнене перемикання передач;
- мимовільне вимикання передач;
- підтікання масла.

Шум в коробці передач може проявлятися в різних умовах - в нейтральному положенні, при включенні передач, при роботі коробки. Кожен з цих шумів свідчить про певні несправності механічної коробки передач.

При діагностуванні не завжди можливо поставити точний діагноз по зовнішнім ознакам, тому що одній і тій же зовнішній ознаці може відповідати декілька несправностей коробки передач. Тому, встановлення конкретної несправності проводиться, як правило, при демонтажі і розбиранні коробки. Однак, демонтаж та розбирання коробок передач дуже трудомісткий процес, що потребує спеціального обладнання та кваліфікованих виконавців. Тому, якісне діагностування коробок передач без демонтажу та розбирання з постановкою точного діагнозу є актуальним завданням сервісу автомобілів.

Зубчасті передачі та підшипники коробок передач - найбільш поширені механізми машин і агрегатів, зважаючи на свою надійності і довговічності. В процесі роботи навіть справна коробка виробляє шум і вібрацію, вимірявши які можна вирішувати питання визначення його технічного стану.

В процесі експлуатації неодмінно відбувається поява дефектів шестерень, надмірний розвиток яких може призвести до порушення роботи або поломки приводу.

Віброакустична діагностика дозволяє здійснювати безрозбірний контроль, при якому скорочуються витрати ресурсів і часу. Технічний стан будь-якої зубчастої пари може бути оцінений за допомогою аналізу вібросигналів [1]. Таке ствердження справедливе як для одиничної зубчастої пари, так і для складних багатовальних зубчастих приводів (редукторів, мультиплікаторів).

Віброакустичний сигнал має складну структуру, що залежить від динаміки механізму і набору комплектуючих його вузлів, містить корисну складову і перешкоди, які перешкоджають точній розшифровці інформації, що міститься в сигналі. По-перше, енергія, що виділяється в процесі зубчатого зачеплення не дуже велика; по-друге, місця установки вібродатчиків, в силу конструктивних особливостей приводів, значно віддалені від зони зубчастого зачеплення.

В результаті шлях передачі енергії вібрації зубчастого зачеплення значний і сигнали в ньому сильно загасають. Тому, для підвищення інформативності необхідно використовувати спеціальні програмні і апаратні засоби, висококваліфікованих діагностів, а також враховувати конструктивні і навантажувальні особливості конкретного об'єкта при розробці методики контролю.

Найбільшого поширення набули методи спектрального, кепстральних і синхронного аналізу вібрації, а останнім часом - вейвлетного аналізу.

До дефектів багатовальних коробок передач відносяться як дефекти виготовлення і складання, так і дефекти, що з'являються в процесі експлуатації, що порушують умови функціонування зубчастого зачеплення. Дефекти виготовлення і складання визначають вихідні характеристики віброакустичних процесів для подальшого порівняння їх з поточними характеристиками в експлуатаційний період.

Експлуатаційні дефекти контактуючих поверхонь зубів є додатковими збуджуючими факторами, які призводять до зміни властивостей віброакустичного сигналу зубчастого приводу. До таких дефектів відносять абразивне зношування робочої поверхні зубів, викришування зубів, заїдання робочих поверхонь, тріщини і злам зубів.

Найшвидшим і тому небезпечним видом пошкодження зубів є їх руйнування, що починається з появи тріщини і закінчується сколом або поломкою зубів. Крім того досить частим експлуатаційним дефектом є порушення режиму мащення контактуючих поверхонь, що приводить до шумового наповненню спектра вібрації. Зміни, до яких призводять дефекти зубчастих коліс, стосуються всіх характеристик вібрації, в тому числі і спектра коливань, при цьому змінюється енергетичне співвідношення компонент спектра.

Абразивне зношування зубчастого зачеплення відноситься до категорії розподіленого експлуатаційного дефекту [2, 3, 4]. Призводить до збільшення бічного зазору, до відривання профілів зубів в зачепленні і ударному режиму збудження коливань. Це приводить до збільшення енергії гармонійного ряду частот, кратних частоті зачеплення, і перерозподілення енергії між компонентами цього ряду на користь високочастотних компонент.

Вплив на характер вібрації абразивного зношування контактуючих поверхонь виражається в зменшенні шумової компоненти і збільшенні амплітуд гармонійного ряду частот зубчастого зачеплення кінематичного вузла [5]. Рівномірне абразивне зношування завжди супроводжується зростанням загального рівня спектральних складових вібрації практично у всьому діапазоні вимірюваних частот.

Загальне збільшення рівнів спектральних компонентів, особливо в високочастотної області, визначає ступінь розвитку зношування поверхонь зубів, що при сильному зношуванні призводить до появи в спектрі широкосмугових областей з високим рівнем шуму, які можуть поглинати складові основних частот збудження. Однак, кожна зубчаста пара характеризується своїми частотами збудження: частотами обертання валів, зубцеву частотою і їх гармоніками [3].

Викришування зубів (піттинг) часто стає причиною вторинних руйнувань, тому важливо своєчасно діагностувати даний вид пошкодження. Розвиток локального пошкодження типу ямок викришування супроводжується зміною віброакустичного сигналу як в діапазоні робочих частот, так і за його межами - в зоні високочастотних резонансів механічної системи, викликаними амплітудною модуляцією коливального процесу в зубчастій передачі періодичною послідовністю ударних імпульсів, що виникають при попаданні дефекту в зону контакту [2]. Зміни в віброакустичному сигналі зубчастої передачі при виникненні ямок викришування спостерігаються як на вимушених, так і на власних частотах [4].

У роботах [3, 4] зазначено, що вищерблення призводить до збільшення деформації зубів, а точніше - до зростання його контактної складової. В силу цього жорсткість зачеплення передачі в момент контактування зуба, що має дефект, зменшується, що відбувається один раз за оборот валу. Піттинг призводить також до флуктуації тиску в момент контактування пошкодженого зуба, наслідком чого є збільшення глибини амплітудної модуляції - зростання амплітуд. При піттингу, тобто втомно-контактного викришування, бічних поверхонь зубів відбувається поява періодичних сплесків вібрації, модулирующих основний процес збудження коливань.

Заїдання робочих поверхонь зубчастих коліс - це найбільш поширений вид руйнування при високих температурах, який з часом напрацювання може приймати лавинний характер, в результаті чого передача виходить з ладу. Заїдання зазвичай

супроводжується нерегулярними викидами в тимчасовому сигналі, флуктуаціями амплітуд гармонік зубцевої частоти. Важливо, що перераховані ознаки можуть супроводжуватися появою і інших пошкоджень зубчастих коліс і не є характерними ознаками заїдання.

Однак досліджуючи модуляцію на зубцевих частотах, а точніше зміну рівнів (глибину модуляції) спектральних складових на частотах обертання валів, можна розпізнавати заїдання на початковому етапі [5].

Тріщини і злам зубів зубчастих коліс - найбільш небезпечний вид ушкодження зубчастих коліс, який може привести до відмови всього зубчастого механізму при попаданні продуктів руйнування в зачепленні, підшипників або інших робочих органів механізму. При появі тріщини в основі зуба (або в іншому місці) жорсткість зачеплення в момент контактування з цим зубом різко падає. Це призводить до передчасного входу в зачеплення наступної пари зубів, що супроводжується ударом [2, 4]. У віброакустичному сигналі з'являються імпульси, амплітуда яких буде рости зі збільшенням тріщини. Причому число імпульсів за один оборот колеса буде дорівнює числу пошкоджених зубів.

Крім коливань на вимушених частотах в діапазоні вібрації присутня яскраво виражена реакція механічної системи на власних частотах на вплив періодичної послідовності ударних імпульсів при попаданні локального дефекту в зону контакту зубів [2].

До дефектів підшипників слід віднести овальність і гранування доріжок кочення, різнорозмірність тіл кочення, відхилення їх форм від розрахункових, відхилення форми від сферичної. Можливе погіршення параметрів шорсткості поверхні тіл кочення також є дефектом, що впливає на силу тертя, збільшує рівень випадкових складових вібрації підшипника.

Вплив дефектів підшипників на вібрацію валів коробки передач призводить до появи складових вібрації на частотах, кратних частотах обертання валу. Такий самий вплив надають неспіввісність валу коробки передач і внутрішнього кільця підшипника, їх овальність або гранність. Зношення тіл кочення, відхилення їх форми від номінальної призводять до появи вібрації на частотах, кратних частотах обертання сепараторів і частотам обертання тіл кочення.

Дефекти зносу поверхонь кочення підшипників впливають на низькочастотні і високочастотні складові вібрації коробок передач. Вплив на високочастотні складові полягає не тільки в тому, що в процесі зношування збільшується коефіцієнт тертя кочення і інтенсивність випадкової вібрації, створюваної силами тертя, але і в тому, що при взаємодії дефектних поверхонь кочення виникають періодичні удари, що супроводжуються зростанням інтенсивності сигналу, як на вищих гармоніках, так і на його випадкових складових.

Вплив зношування на низькочастотну вібрацію підшипників кочення, (і агрегату в цілому), проявляється на тлі інших дефектів не відразу, а лише після того, як величина зношування перевищить якесь граничного значення, тобто на одному з останніх етапів експлуатації підшипника, характеризується високою швидкістю зносу. Складний склад спектра збуджуючих сил може привести до того, що через резонанс окремих вузлів коробки передач інтенсивність гармонік вібрації, створюваних силами ударного збудження і збігаються з резонансними частотами, різко зростає і може бути визначальною в загальному рівні вібрацій.

У підшипниках зі збільшеним через зношування поверхонь кочення радіальним зазором можливе виникнення незатухаючих коливань валів коробки передач.

Сили тертя в підшипниках є причиною появи випадкових складових вібрації, що вносять помітний внесок у загальний рівень вібрації коробки передач. У підшипниках кочення сили тертя і створювана ними вібрація залежать від сил нормального тиску на поверхні кочення і коефіцієнта тертя кочення. Цей параметр, а також рівень вібрації викликаний ним, залежать від ряду параметрів підшипника, в тому числі від чистоти обробки поверхонь кочення, від кількості та якості мастила, від наявності та характеру зносу поверхонь кочення. Тиск на одне тіло кочення, яке контактує одночасно з обома кільцями

підшипника, яка надається валом коробки передач, залежить від дефектів складання підшипникової опори, що супроводжуються збільшенням цих сил і числа тіл кочення, що контактують з обома кільцями. У той же час сили тертя не залежать від швидкості відносного обертання кілець підшипника. Отже, створювана ними вібрація має досить складну залежність рівня від швидкості обертання валів коробки передач.

Частка енергії, що витрачається на подолання сил тертя, перетворюється в енергію вібрації. Так як коефіцієнт тертя кочення, залежить від сили нормального тиску і числа тіл кочення, що контактують з обома кільцями, то випадкова вібрація, створювана силами тертя, матиме амплітудну модуляцію.

Сприяти вирішенню проблеми виявлення дефектів коробки передач може вдосконалення засобів діагностики, що припускає впровадження в коло розв'язуваних ними завдань алгоритмів обробки сигналу, що знижують суб'єктивність прийняття рішення.

Діагностично значущі гармоніки спектра можуть перекриватися і накладатися один на одного, призводити до появи резонансних зон, що ускладнює процес діагностики.

При ускладненій ідентифікації дефектів в силу зазначеної причини ефективно себе показав метод синхронного накопичення, реалізація якого в функціональних можливостях засобів діагностики дозволяє розділити частотні складові від різних джерел. Крім того, слід провести вимірювання вібрації в декількох точках приводу і зіставити спектри; змінити навантаження передану приводом; в окремих випадках необхідно провести вимірювання при розгоні ведучого вала.

Точність оцінки поточного технічного стану, а також достовірність діагностики дефектів коробок передач по віброакустичному сигналу багато в чому залежить від досвіду діагноста, його знань про внутрішню будову вузла і природи вібраційних процесів. Незважаючи на значне поширення численних методів обробки і аналізу вібрації, програмних і апаратних засобів діагностики, постановка діагнозу містить велику частку суб'єктивності, процес діагностики тривалий і трудомісткий.

Наявність викладених проблем змушує продовжувати дослідження, спрямовані на розробку таких методів віброакустичного діагностики, які б дозволили підвищити її об'єктивність і ефективність, автоматизувати процес вимірювання, обробки і постановки діагнозу. Цьому сприяє розвиток обчислювальної техніки, систем програмування та комп'ютерної математики, що відкривають широкі можливості для реалізації поставлених цілей.

Висновки. В результаті аналізу літературних джерел виділено найбільш значущі фактори, що впливають на рівень віброакустичного сигналу коробок передач, це зношення підшипників, зношування поверхонь зубів, порушення мащення в зачепленні, заїдання зубів, викришування, зколювання, тріщини і поломки зубів. Більшість інших факторів є пов'язаними з ними причинно-наслідковими залежностями, це обумовлено особливостями функціонування коробок передач. Зміна віброакустичного сигналу може бути використана в якості діагностичної інформації при діагностуванні трансмісії.

Список літератури

1. Генкин, М.Д. Виброакустическая диагностика машин и механизмов /М.Д. Генкин, А.Г. Соколова. - М.: Машиностроение, 1987. - 228 с.
2. Асриян, Г.М. Возможности диагностирования вибрации сложных динамических систем / Г.М. Асриян // Колебания редукторных систем. - М.: Наука, 1980.-С.70-74.
3. Шаницын, А.А. Об изменении вибрации шарикоподшипника в процессе эксплуатации / А.А. Шаницын, М.К. Пальм // Динамика станков: Тез. докл. Всесоюз. науч. - техн. конф. / Куйбышев, политехи, ин-т. — Куйбышев, 1980, с. 325-326.
4. Баркова, Н.А. Современное состояние виброакустической диагностики машин / Н.А. Баркова. - Санкт - Петербург: Изд-во СПбВМА, 2002. — 260 с.
5. Лелиовский, К.Л. Совершенствование конструкции коробок передач автомобилей «ГАЗель» по их виброакустическим характеристикам- работы /К.Я. Лелиовский, В.В. Беляков, СМ. Огороднов // Известия вузов. Серия «Машиностроение». 2008. №8. С. 49 - 56.

УДК 629.1.01

І. Василенко, магістр гр. АТ-19 МЗ
Центральноукраїнський національний технічний університет

АНАЛІЗ ТЕХНОЛОГІЙ ВІДНОВЛЕННЯ З'ЄДНАННЯ «КЛАПАН-ВТУЛКА» ДВИГУНІВ ВНУТРІШНЬОГО ЗГОРАННЯ

Одним з важливих спряжень двигунів внутрішнього згорання, що мають недостатній ресурс є спряження „клапан-втулка". Підвищене зношування спряження „клапан-направляюча" відбувається внаслідок недостатнього мащення, що обумовлюється конструктивними особливостями клапанного механізму. Відомі методи відновлення та зміцнення поверхонь деталей, які передбачають нанесення зміцнюючих покриттів, мають високу вартість і не завжди використовуються при виготовленні деталей. Підвищити зносостійкість спряження „клапан-направляюча" можливо покращенням умов тертя шляхом створення на поверхні клапана мікрорельєфа. Це підвищує маслоємкість поверхні та дозволяє зменшити час на припрацювання та величину припрацювального зносу. Для нанесення мікрорельєфа на поверхню клапана доцільно використовувати електромеханічну обробку, цей метод має високу продуктивність та незначний механічний та тепловий вплив на деталь. Підвищення маслоємкості поверхні шляхом нанесення рельєфу методом ЕМО можливо як при виготовленні нових деталей, так і при ремонті стержня клапана до номінального або ремонтного розміру.
клапан, втулка, зносостійкість, електромеханічна обробка

Постановка проблеми. Одним з важливих спряжень двигунів внутрішнього згорання, що мають недостатній ресурс є спряження „клапан-направляюча". Інтенсивне зношення цих деталей приводить до підвищеної витрати масла, втраті компресії у двигуні, як наслідок, погіршення показників двигуна, та передчасного ремонту головки циліндрів.

Аналіз останніх досліджень і публікацій. Для вирішення проблеми розроблені технології підвищення зносостійкості даного спряження, що базуються на підвищенні міцності стрижня клапана за рахунок нанесення зносостійких хромових покриттів, поверхневого пластичного деформування, а також застосування антифрикційного матеріалу при виготовленні направляючої втулки [2, 8].

Конструктивні особливості даного спряження не дозволяють подавати масло в достатній кількості в зону тертя для того щоб уникнути граничного та сухого тертя. Збільшена кількість масла призведе до попадання його в циліндри двигуна, а також на поверхні головки клапана, що в кінцевому випадку обумовить виникнення нагару на поверхні поршня, сідла, фаски клапана.

Технологічні способи підвищення міцності деталей клапанів як правило значно підвищують вартість виготовлення та відновлення деталей, а також підвищують витрати пов'язані з механічною обробкою зміцнених поверхонь, також збільшується строк припрацювання спряження [6-8].

Одним з шляхів підвищення зносостійкості спряження „клапан-направляюча" є покращення умов мащення деталей. Отримати такі умови можливо шляхом отримання спеціального рельєфу на поверхні клапану, який дозволив би утримувати масло в зоні тертя, при цьому не допускати попадання масла в циліндри двигуна [6-8].

З трьох станів змащуваної поверхні (тертя без змащувального матеріалу, граничне і гідродинамічне мастило) для більшості пар тертя найбільш характерний граничний стан мастила, при якому товщина масляної плівки оцінюється величиною від десятих доль до декількох мікрометрів [3, 5]. При зношуванні або порушенні масляної плівки одночасно відбувається зворотний процес – її регенерація. Для цього необхідний деякий запас змащувального матеріалу, який може знаходитися в западинах мікрорельєфу або в спеціальних поглибленнях (кишенях) на поверхні тертя [3, 5, 9].

Створення на робочій поверхні деталей мікрорельєфів з регулярними геометричними характеристиками дозволяє з достатньою точністю аналітично розраховувати такі безпосередньо визначальні експлуатаційні властивості цих поверхонь параметри, як об'єм канавок (маслоємкість), опорну поверхню, кількість плям контакту і ін. [3-5, 9-13].

Оптимальна кількість і об'єм поглиблень в елементах рельєфу, у поєднанні з їх великим радіусом і значною поверхневою активністю наклепаного металу на ділянках западин, забезпечують не тільки достатню маслоємкість поверхні, але і хороше утримування мастила на обробленій поверхні.

Проте при збільшенні маслоємкості знижується несуча здатність поверхні, що негативно позначається на експлуатаційних властивостях оброблюваних деталей. Тому для кожних умов роботи рухомого сполучення необхідний свій раціональний мікрорельєф робочих поверхонь деталей.

Мета й завдання дослідження. Проаналізувати існуючі способи нанесення мікрорельєфу, вибрати та дослідити найбільш доцільний спосіб підвищення зносостійкості клапанів двигунів внутрішнього згорання.

Виклад основного матеріалу. Дослідженнями показано, що збільшення зносостійкості термічно необроблених деталей в порівнянні з шліфованими і загартованими пояснюється відмінністю форми і взаєморозташуванням мікронерівностей, а також більшою опорною поверхнею [1, 4, 5].

Дослідження опору зношування поверхонь, що мають мікрорельєф, показало, що опір зносу (за інших рівних умов і однаковій шорсткості) зростає із збільшенням радіусу закруглення вершин мікронерівностей, відношення r/Rz_{max}, ступеня однорідності і із зменшенням кута нахилу твірних мікронерівностей. Так, зносостійкість шліфованої поверхні 7-го класу шорсткості в 3,5 разу нижче за зносостійкість віброобкатаної поверхні того ж класу шорсткості [4, 9].

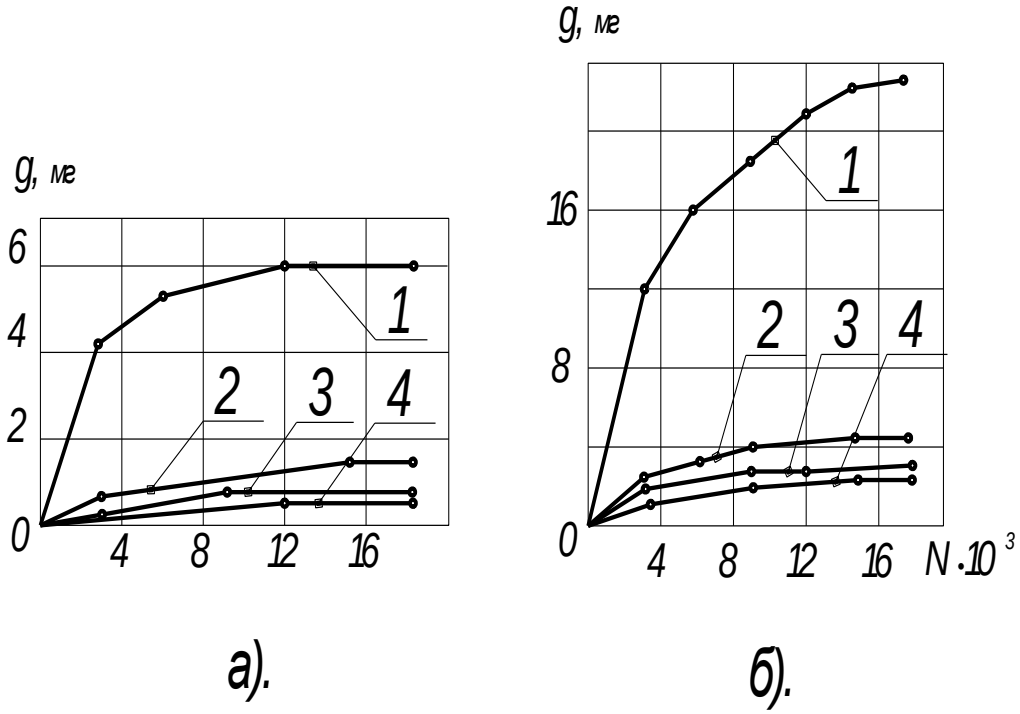
Оцінюючи роль зміцнення, супроводжуючого процес обробки деталей різанням, гладким і вібраційним обкатуванням, Ю. Г. Шнейдер [9-10] стверджує, що частка впливу на підвищення зносостійкості мікрорельєфу і зміцнення приблизно рівна відповідно 70 і 30%. Таке істотне підвищення зносостійкості за рахунок оптимізації мікрорельєфу при віброобкатуванні можна пояснити утворенням мікронерівностей форми, найбільш сприятливої для опору всім видам зношування. Проте цей висновок справедливий для деталей, твердість поверхні яких порівняно невелика (HRC 40). При обробці деталей з вищою твердістю роль мікрорельєфу позначається в меншій мірі, ніж зміцнення в результаті обробки поверхневою пластичною деформацією, оскільки в цьому випадку відбуваються структурні і фазові зміни в поверхневому шарі деталі, що призводить до додаткового зміцнення цього шару [4].

Нанесення мікрорельєфу виявилося вельми ефективним при обробці деталей з легованих сталей, які працюють в умовах граничного тертя.

На рис. 1 [3] показана залежність вагового зносу ролика легованої сталі, обробленої різними способами і що випробовується в парі з чавунною колодочкой (СЧ18). Найменший знос характерний для роликів, що мають рельєф.

Знос таких роликів виявився в 8-10 разів нижче, ніж шліфованих. Знос чавунних колодочок, що працюють в парі з обкатаними роликами; також опинився в 6-8 разів менше, ніж знос колодочок, що випробовуються в парі з шліфованими роликами.

При дослідженні зносостійкості пар тертя сталь – чавун було також виявлено вплив регулярного мікрорельєфу на одній з деталей на знос контртіла [3]. Колодочки з антифрикційного чавуну АСЧ-1 і ролики із сталі випробовувалися на машині тертя МІ-1М із швидкістю 1,33 м/сек при тиску 30 кгс/см^2 і змочуванні нижньої частини ролика у ванні з маслом марки «Індустріальне 20».



1 – шліфування; 2 – точіння; 3 – обкатування; 4 – поверхні з рельєфом, отриманим накатуванням (а – знос роликів з легованої стали; б – знос чавунних колодок).
Рисунок 1 – Залежність вагового зносу від числа циклів:

У проблемі підвищення довговічності деталей машин найважливішу роль грають антифрикційні властивості їх робочих поверхонь: зносостійкість, коефіцієнт тертя, припрацювання та інші. Протікання процесу зношування в часі характеризується трьома основними фазами: припрацювання (початковий), нормальний (встановлений), граничний (катастрофічний) знос. Встановлений знос тісно пов'язаний з процесом припрацювання, від умов припрацювання залежить знос періоду експлуатації.

Припрацювання визначає: величину загального зносу; темп і величину нормального зносу; утворення таких дефектів, як задирання, виривання з припрацьованих поверхонь, а також схоплювання, заїдання в процесі встановленого зносу; розміщення і витрата змащувальних речовин; температуру в зоні тертя. Для збільшення терміну служби, як знову виготовлених, так і відремонтованих агрегатів і машин в цілому, необхідно скоротити величину початкового зносу сполучень в період припрацювання до мінімуму.

Мікрорельєф припрацьованої поверхні в порівнянні з вихідною характеризується більшою однорідністю по висоті мікронерівностей, підвищеною опорною поверхнею, збільшеним числом плям контакту. Одним з основних чинників, що визначають припрацювання поверхні, є її мікрорельєф і в першу чергу розміри, форма і величина опорної поверхні.

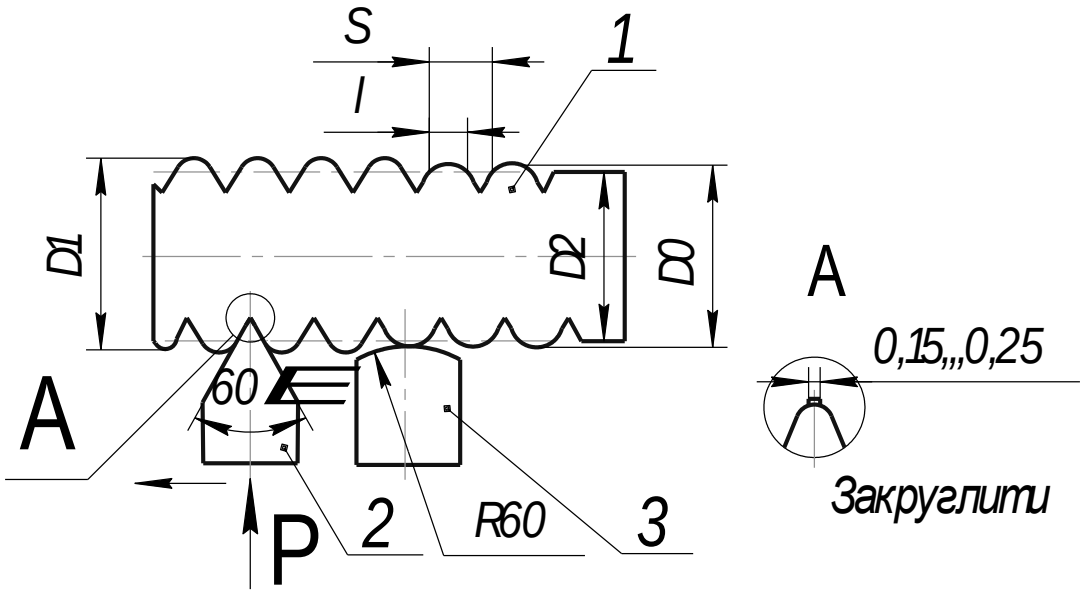
Одним з існуючих видів обробки, який дає можливість утворення поверхні з великою опорною поверхнею є електромеханічна обробка (ЕМО). Вона дозволяє сформувати мікрорельєф, що забезпечує при достатній маслоємкості поверхні і високому ступені однорідності мікронерівностей можливість його тонкого регулювання.

Матеріал клапанів – легована сталь, як правило має досить високу міцність та твердість, отже нанесення рельєфу традиційними методами поверхневого пластичного деформування ускладнене через значні зусилля, що необхідно прикладати до деталі. При дії високих зусиль невідворотно відбудеться деформація стрижня клапана та порушення його геометрії в цілому.

Електромеханічна обробка заснована на поєднанні термічної і силової дії на поверхневий шар оброблюваної деталі. Суть цього способу полягає в тому, що в процесі

обробки через місце контакту інструменту з виробом проходить струм великої сили і низької напруги, внаслідок чого виступаючі гребінці поверхні піддаються сильному нагріву, під тиском інструменту деформуються і згладжуються, а поверхневий шар металу зміцнюється .

Технологічний процес відновлення посадочних поверхонь нормально зношених деталей складається з двох операцій: висадки металу і згладжування посадочної поверхні до певного розміру (рис. 2). Принципова відмінність цих операцій полягає у відмінності контактної напруги. У першому випадку обробка проводиться пластиною *2* з твердого сплаву, ширина поверхні контакту якої чисельна менше подачі приблизно в 3 рази, а в другому випадку обробка проводиться твердосплавною пластиною *3,* ширина контакту якої значно перевищує подачу.



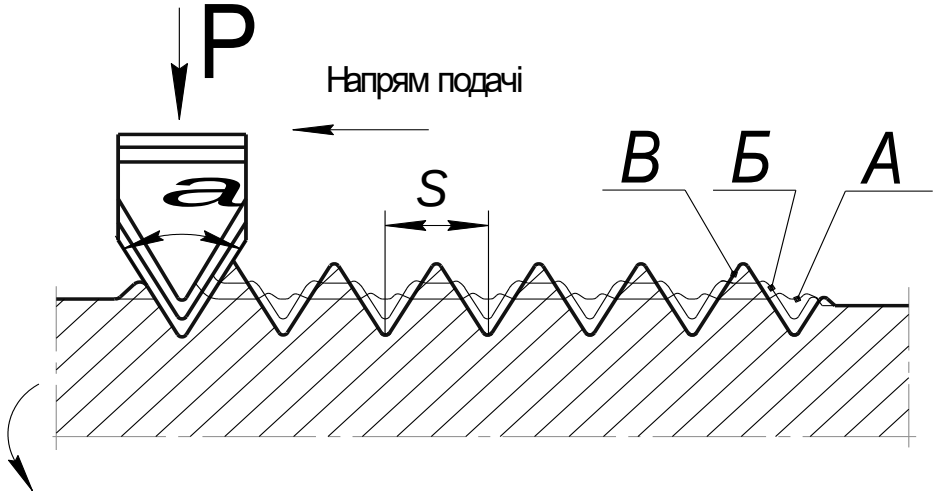
1 – деталь; 2 – висаджувальна пластина; 3 –згладжувальна пластина; D_1 – діаметр до висадки; D_2 – діаметр після згладжування; S – крок висадки; l – ширина висадки.

Рисунок 2 – Схема висадки і згладжування металу

При висадці на контактній поверхні утворюється гвинтовий виступ, а при згладжуванні цей виступ зменшується до необхідного розміру; первинний діаметр контактуючої поверхні збільшується.

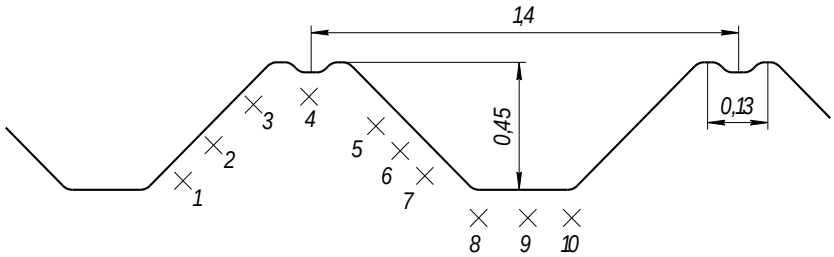
Схема утворення поверхні висадкою показана на рис. 3. Профіль може створюватися, як за рахунок збільшення сили *P,* так і за рахунок збільшення числа робочих ходів. У міру збільшення сили метал, що контактує з пластиною, піддається все більшій пластичній деформації і витискується назовні уздовж контура пластини, а остання, занурюючись у метал, утворює впадину, що збільшується в своїх розмірах. Таким чином, по мірі збільшення сили відстань між нерівностями виступу зменшується.

Послідовність утворення профілю посадочної поверхні приведена на рис. 4. На рис. 4, *а* показаний максимально висаджений для даної подачі профіль, а на рис. 4, *б,в* — зміна висадженого профілю в процесі згладжування. Згладжуванням досягається низька шорсткість поверхні, розмір і величина виступів можуть регулюватися числом повторних робочих ходів і тиском інструменту.



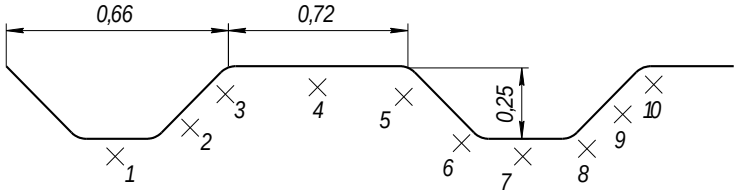
а – профіль поверхні після першого робочого ходу; б – після другого робочого ходу; в – після і-го робочого ходу.

Рисунок 3 – Схема утворення профілю поверхні, сформованої висадкою



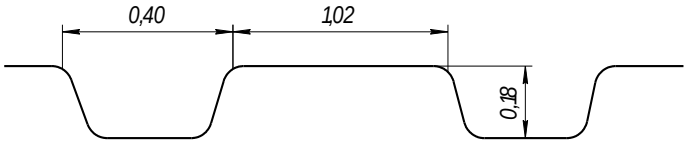
№ ділянки	1	2	3	4	5	6	7	8	9	10
Hμ, ГПа	3.34	3.25	2.86	1.97	3.24	3.15	3.47	2.96	3.38	3.46

а).



№ ділянки	1	2	3	4	5	6	7	8	9	10
Hμ, ГПа	3.60	4.20	4.73	5.69	4.69	3.40	3.65	4.28	4.40	4.67

б).



в).

а) висаджений; б) згладжений за два робочих хода; в) згладжений за три робочих хода.

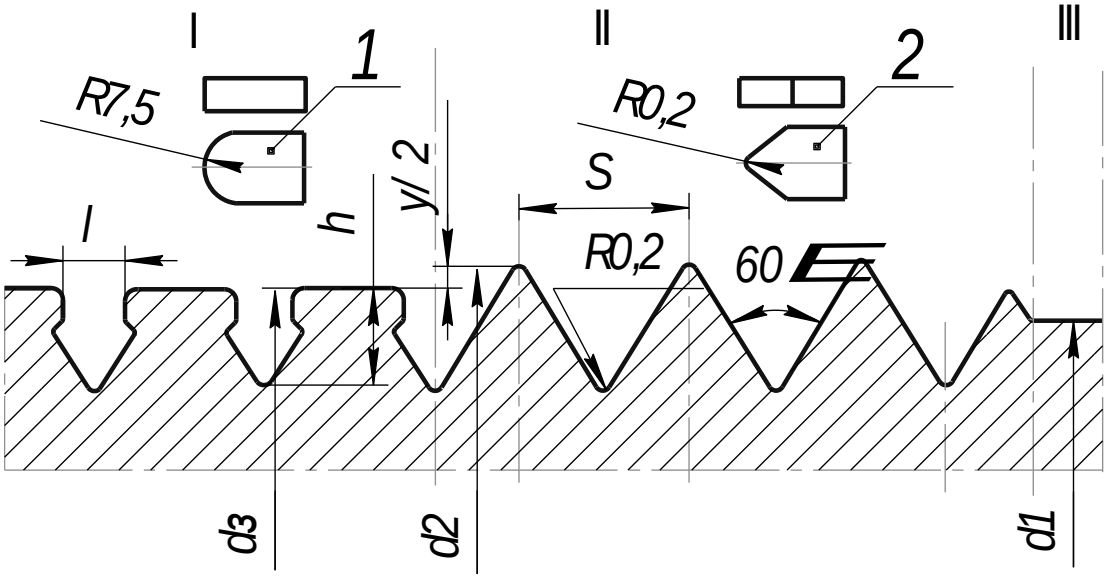
Рисунок 4 – Схема зміни профілю при висадці і згладжуванні сталі 50 і мікротвердість на різних ділянках перерізу профіля

Вимірювання мікротвердості в перерізах висадженого і згладженого профіля показує збільшення твердості окремих ділянок в 2...3 рази в порівнянні з твердістю серцевини. Точка *4* (рис. 4, *а*), що має найнижчу твердість після висадки, отримує найбільш високу твердість після згладжування (рис. 4, *б*). Це пояснюється тим, що при висадці точка *4* залишається майже нейтральною, а деформації піддаються бічні поверхні профілю і профіль впадини. Найбільш інтенсивній термічній дії згладжуванням піддаються гребінці виступів, які надалі складають поверхневий шар деталі.

Згладжування забезпечує: збільшення контактної поверхні деталі, що сполучається, і зниження її шорсткості; збільшення твердості і пружних властивостей контактної поверхні; необхідний натяг сполучення і його міцність.

Після згладжування в декілька робочих ходів переріз згладженого профілю наближається до прямокутного. Для підвищення маслоємкості стержня клапана пропонується виконувати на його стержні мікрорельєф, використовуючи технологію електромеханічної обробки.

Схема утворення повного профілю такого мікрорельєфу представлена на рис. 5. Рельєф утворюється за рахунок деформації металу з одночасним нагрівом струмом (I=400…700 А), який проходить через місце контакту інструмента і деталі. Подальше згладжування твердосплавною пластиною *1* досягається утворення грибоподібного профілю на вершинах різьби.



III- вихідна поверхня; II- профіль поверхні після висадки; I- профіль поверхні після згладжування; 1- згладжувальна пластина; 2- висаджувальна пластина.

Рисунок 5 – Утворення профілю поверхні:

Висновки:

1. Одним з важливих спряжень двигунів внутрішнього згорання, що мають недостатній ресурс є спряження „клапан-направляюча". Підвищене зношування спряження „клапан-направляюча" відбувається внаслідок недостатнього мащення, що обумовлюється конструктивними особливостями клапанного механізму.

2. Відомі методи відновлення та зміцнення поверхонь деталей, які передбачають нанесення зміцнюючих покриттів, використання матеріалів деталей з антифрикційними властивостями, виконання зміцнюючої обробки. До таких методів відносять гальванічні методи (хромування клапана), поверхневе пластичне деформування стержня клапана, виготовлення направляючої з композиційних та порошкових матеріалів. Як правило такі методи мають високу вартість і не завжди використовуються при виготовленні деталей.

3. Підвищити зносостійкість спряження „клапан-направляюча" можливо покращенням

умов тертя шляхом створення на поверхні клапана мікрорельєфа. За літературними даними нанесення мікрорельєфу дозволяє покращити умови мащення, підвищує маслоємкість поверхні та дозволяє зменшити час на припрацювання та величину припрацювального зносу.

4 Для нанесення мікрорельєфа на поверхню клапана доцільно використовувати електромеханічну обробку, цей метод має високу продуктивність та незначний механічний та тепловий вплив на деталь.

5. Підвищення маслоємкості поверхні шляхом нанесення рельєфу методом ЕМО можливо як при виготовленні нових деталей, так і при ремонті стержня клапана до номінального або ремонтного розміру та розгортанням направляючої.

Список літератури

1. Горохов В.А. Обработка деталей пластическим деформированием. К.: Техніка, 1978. 192 с.
2. Лизунов А.А., Трелин А.А. Семь раз отмерь, один отрежь! Правильный автосервис, №1, 2006. С. 22 - 26
3. Наливайко В.Н. Особенности образования регулярного микрорельефа на поверхности осциллируемой детали многошаровыми накатниками // В сб.: Проблемы конструирования и технологии производства сельскохозяйственных машин. Кировоград: 1991. С.57-58.
4. Одинцов Л.Г. Финишная обработка деталей алмазным выглаживанием и вибровыглаживанием. М.: Машиностроение, 1981. 160 с.
5. Суслов А.Г. Технологическое обеспечение параметров состояния поверхностного слоя деталей. М.: Машиностроение, 1987. 208 с.
6. Трелин А.А. Исследование технологических факторов, влияющих на качество ремонта головок блока цилиндров. ТРУДЫ ГОСНИТИ т. 98. М.: ГОСНИТИ, 2006. С. 62 – 66
7. Трелин А.А. Метрологическая оценка качества восстановления фасок седел с помощью ручного инструмента и станочного оборудования отечественного и зарубежного производства. МТС 3/2003. С. 45 - 49
8. Трелин А.А., Соловьев Р.Ю. Исследование влияния качества направляющих втулок в сопряжении «клапан-втулка» на ресурс двигателей при ремонте. М. Вестник МГАУ. Серия «Агроинженерия». Выпуск №5 (20), 2006. С. 119 - 123
9. Шнейдер Ю.Г. Образование регулярных микрорельефов на деталях и их эксплуатационные свойства. Л.: Машиностроение, 1972. 240 с.
10. Шнейдер Ю.Г. Эксплуатационные свойства деталей с регулярным микрорельефом. Л.: Машиностроение, 1982. 248 с.
11. Шнейдер Ю.Г., Бунга Л.А. Исследование процесса вибронакатывания // В кн.: Размерно-чистовая обработка деталей машин пластическим деформированием взамен обработки резанием. М.: НИИМАШ, 1965. С. 125-130.
12. Шнейдер Ю.Г., Кузьмин Ю.П., Букин Б.Н., Богданов Г.Н. Исследование процесса образования и расчет параметров регулярного микрорельефа //В сб.: Технологические методы повышения качества поверхности деталей машин. Л.: 1978. С.99-115.
13. Шнейдер Ю.Г., Кузьмин Ю.П., Сорокин В.М. и др. Новый государственный стандарт на поверхности с регулярным микрорельефом// Вестник машиностроение. 1982, №4. С.73-74.

УДК 32.019.51

А. Вогнівенко, магістр гр. ІС-19М
С. Орлик, д-р іст. наук, професор
Центральноукраїнський національний технічний університет

ОСОБЛИВОСТІ ІНФОРМАЦІЙНОГО СУПРОВОДЖЕННЯ ВИБОРІВ ЗА УЧАСТЮ ЗАСОБІВ МАСОВОЇ ІНФОРМАЦІЇ

У статті розглянуто особливості інформаційного супроводження виборчої кампанії засобами масової інформації. Звернута увага на процес формування інформаційного простору політики, стан та розвиток інформаційної культури, суть медіа-маніпуляції. Визначено роль і місце журналістської діяльності у виборчому процесі. Акцентовано увагу на ході проведення реформування друкованих ЗМІ заснованих органами державної влади, та/або органами місцевого самоврядування, іншими державними органами. Проаналізовано ступінь довіри українців до різних типів ЗМІ під час виборчої кампанії.
засоби масової інформації, виборчий процес, інформаційне суспільство, медіа маніпуляції, паблик рілейшнз, інформаційна культура, інформаційний простір

Постановка проблеми. У суспільно-політичному житті кожної країни, обрання президента країни, членів парламенту та органів місцевого самоврядування відіграє важливе значення для розбудови демократичних основ держави. В сучасному інформаційному суспільстві важливу роль займає відкритість і вільний доступ до інформації, особливо під час виборчого процесу, коли кожен громадянин має здійснити свій свідомий політичний вибір. Діюче вітчизняне законодавство наголошує на тому, що виборчий процес в Україні має здійснюватися на засадах публічності, свободи передвиборчої агітації, плюралізму та рівноправного доступу до ЗМІ. Враховуючи те, що медійний і політичний процеси мають спільну природу – інформаційну, саме ця обставина стає визначальною. Тож виникає необхідність нового трактування завдань і функцій ЗМІ у виборчому процесі, здійснення переосмислення проблеми місця та ролі ЗМІ в нових політичних реаліях. Адже політичний світ сучасної України постійно змінюється, особливо в демократичному напрямку розширення політичного дискурсу, яке супроводжується застосуванням широкого спектру впливу на свідомість громадян з метою привернення уваги громадськості до суспільно-політичних мір і заходів у сфері політичного життя країни.

Аналіз останніх досліджень і публікацій. Дослідженню проблем формування інформаційно-комунікаційного простору, PR-інструментарію та виборчих технологій у сфері політичної комунікації присвятили свої роботи ряд українських науковців: В. Березенко, О. Дубас, С. Дзенни, Т. Ігнатенко, В. Королько, Л. Кочубей, О. Курбан та ін.

Проблематика медіа-маніпуляції як виду психологічного впливу під час здійснення PR кампаній в рамках політичного (в т.ч. виборчого) процесу розглядало ряд українських та зарубіжних вчених: В. Бебик, Е. Брейнс, С. Блек, В. Мойсєєв, А. Назаретян, Ю. Нестеряк, Г. Почепцов, С.Рум'янцева, Г. Чернишина, Т. Жалко та ін.

Метою статті є розгляд основ та механізм інформаційного супроводження виборчого процесу засобами масової інформації.

Виклад основного матеріалу. З розвитком сучасного інформаційного суспільства відбувається віртуалізація інформаційного простору, що дозволяє штучно моделювати політичні події і створювати віртуальні політичні персони та фігури. Швидкий розвиток інформаційно-комунікаційних технологій, сприяє динамічному заміщенню політичної

реальності на медійну реальність. По суті, в інформаційному просторі відбувається домінування віртуальних образів – симулякрів. Тож, закономірно, що «перетворення іміджу на центральну категорію політичного процесу створюють оптимальне середовище для підтримки мінімального, але достатнього для здійснення владних повноважень інфобалансу між державою й суспільством, що є основою легітимації та стабілізації політичних відносин» [4, с. 226]. А як наслідок, в подібних умовах посилюється роль медіаторів, які транслюють повідомлення. Звичайно, у цьому значну роль відіграють традиційні друковані засоби масової інформації, так і ЗМІ, які використовують технічні засоби передачі інформації – радіо, телебачення, інформаційні електронні ЗМІ. Слід відзначити, що на сучасному етапі розвитку інформаційного суспільства особливого значення набувають саме електронні ЗМІ, котрі дозволяють встановити персональний інформаційний обмін з авторизованими суб'єктами масового політичного процесу.

У такому разі важливим для сучасного інформаційного суспільства стає питання стану та розвитку інформаційної культури, яка формується завдяки медіа- та інформаційній грамотності. На сьогодні надзвичайно актуальною виникає потреба більш активно вживати заходи для поширення інформаційної культури, котра визначально впливає на всі сфери соціально-економічного життя, а також впливає на ментальність і поведінку людей. Особливо це проявляється у ході передвиборчих кампаній. З цього приводу українським вченим В. Мойсеєв зазначається, що «формування політичної культури відбувається у процесі політичної практики і під впливом різноманітних комунікаційних зв'язків, серед яких важлива роль належить паблік рілейшнз» [7, с.149].

Не слід забувати і про маніпуляції, як вид психологічного впливу, який активно застосовується засобами масової інформації під час виборчого процесу. По суті медіа-маніпуляція – вид психологічного впливу, що здійснюється через пресу (газети, журнали, книги), радіо, телебачення, інтернет, кінематограф, відеозаписи, відеотексти, телетексти, рекламні щити та панелі, що поєднують телевізійні, телефонні, комп'ютерні та інші лінії зв'язку, соціальні мережі, що призводить до пробудження у об'єкта впливу намірів, які змінюють його бажання, настрої, поведінку, погляди тощо [6].

Дослідниця соціальних комунікацій Ю. Нестеряк доводить, що за допомогою ЗМІ, інформацію можна: спотворити за допомогою неповної, односторонньої подачі; відредагувати, додавши власні домисли і коментарі; інтерпретувати у вигідному світлі; приховати, разом з тим, акцентуючи увагу на окремих сторонах події, замовчуючи інші, що створює додаткову можливість маніпулювати аудиторією; створити «інформаційний шум»; подати навіть неперевірену інформацію, що є певним маніпулятивним прийомом; поширювати певний погляд на інформацію як її єдино вірний варіант [8]. До цього переліку можна додати ще один напрямок – поширення через ЗМІ дезінформації (фейків) та поширення чуток – як способів психологічного впливу, які полягають в навмисному наданні суперникам або електорату неправдивої, спотвореної інформації, що введе їх в оману щодо реальності стану справ.

Безперечно, велике значення у діяльності ЗМІ належить журналістській професії. Як відомо, діяльність журналіста має бути направленою на впровадження в масову свідомість певних оцінок явищ і фактів з метою досягнення впливу на неї. Така функція журналістики передбачає високий рівень відповідальності журналіста, і тому особливого значення набувають вимоги до професіоналізму журналістської діяльності. Багато українських журналістів свою працю спрямовують на зміцнення національних інтересів, дотримуються високих моральних і професійних стандартів. Водночас сьогодні в умовах впливу ринкових механізмів комерційні чинники в роботі ЗМІ загрожують етичним аспектам діяльності журналістів, підштовхують їх до використання різноманітних маніпуляцій суспільною свідомістю на догоду інтересам певних кіл і угруповань[5]. У такому випадку журналістам та редакторам ЗМІ необхідно розрізняти PR, передвиборну агітацію від поняття «інформаційного забезпечення виборів», яке полягає у висвітленні виборчого процесу.

Таким чином, на фоні виникнення вищевказаних нових характеристик інформаційного

простору політики, розвитку активного процесу віртуалізації політичного інформаційного простору, перед державними органами, експертами та й самими політиками ставиться завдання створення як законодавчих так і моральних запобіжників які б унеможливили та запобігли негативним політичним наслідкам.

Щодо порядку інформаційного супроводження виборчого процесу за участю ЗМІ, то Виборчим кодексом України визначено порядок висвітлення ЗМІ інформації «про перебіг виборчого процесу, події, пов'язані з виборами, базуючись на засадах достовірності, повноти і точності, об'єктивності інформації та її неупередженого подання.

Інформаційні агентства, засоби масової інформації, що поширюють повідомлення про перебіг виборчого процесу, події, пов'язані з виборами, не можуть допускати замовчування суспільно необхідної інформації, що стосується цих подій, якщо вона була їм відома на момент поширення інформації. Інформаційні агентства, засоби масової інформації зобов'язані поширювати інформацію про вибори відповідно до фактів, не допускаючи перекручування інформації. <…> Засоби масової інформації мають збалансовано висвітлювати коментарі кандидатів, партій (організацій партій) – суб'єктів виборчого процесу щодо подій, пов'язаних із виборами» [1].

Важливим під час передвиборчої кампанії є упорядкування механізму спростування у друкованих та інтернет ЗМІ, певних неточностей або неправдивої інформації щодо виборних кандидатів чи політичних партій. Діючим законодавством передбачено порядок спростування недостовірної або викривленої інформації про суб'єкта виборчого процесу у друкованих та інтернет ЗМІ (ст.57 Виборчого кодексу України» [1] та ст. 37 Закону України «Про друковані засоби масової інформації (пресу) в Україні» від 16.11.1992 р. №2782 (зі змінами та доповненнями) [9], яка застосовується для громадян, підприємств, установ і організацій (в т.ч. державних органів) у випадку необхідності реагування на опубліковану інформацію котра на їхню думку «не відповідає дійсності або принижує їх честь та гідність». У цьому напрямку вітчизняне законодавство повністю відповідає рекомендаціям №R(97)20 ухваленим Комітетом Міністрів Ради Європи 30 жовтня 1997 р. на 607-му засіданні заступників міністрів «Про "наклепницькі висловлювання"» [11].

Окрім процесів олігархізації ЗМІ, в Україні залишається проблема впливу на засоби масової інформації з боку органів державної влади та органів місцевого самоврядування, які були їхніми засновниками. З метою проведення реформування друкованих ЗМІ заснованих органами державної влади, та/або органами місцевого самоврядування, іншими державними органами у грудні 2015 р. було прийнято Закон України «Про реформування державних і комунальних друкованих засобів масової інформації»[10]. Цей Закон не поширюється на газети «Голос України» та «Урядовий кур'єр». Метою роздержавлення державних і комунальних друкованих ЗМІ визначено, сприяння: піднесенню свободи слова та демократичних основ суспільства на вищий рівень; розвитку регіональної журналістики та позбавлення можливості державним та місцевим органам влади впливати на редакційну політику друкованих видань, що гарантуватиме їм незалежність. Реформування друкованих ЗМІ та редакцій планувалося здійснити у два етапи: перший – протягом 2016р. та другий – 2017-2018 рр. Тобто до 1 січня 2019 р. таке реформування мало бути завершеним по всій країні. Проте цей процес затягнувся. За даними Держкомтелерадіо, станом на 1.01.2019 р., лідерами цього процесу було названо «Кіровоградську (з 28 друкованих ЗМІ та редакцій реформовано 25), Житомирську (з 28 – 24), Хмельницьку (з 27 – 23), Миколаївську (з 26 – 22), Полтавську (з 31 – 26) та Тернопільську (з 21 – 17) області. А найгірше ситуація з реформуванням склалася на Київщині (включно з столицею), Львівщині, Одещині, Дніпропетровщині, Івано-Франківщині та на Закарпатті»[14]. Такі перетворення залишають сподіватися на те, що зазначені друковані засоби позбудуться диктату з боку з боку «старих» засновників на процес формування редакційної політики та свободи слова – це особливо важливо у період проведення виборів у нашій країні. Звичайно, спокуса впливу органів державної та місцевої влади залишиться, адже ця проблема існує не лише в Україні, а й у країнах Європейського Союзу. Щодо висвітлення виборчого процесу друкованими ЗМІ, то

Рекомендацією Ради Європи №R(99)15 «Про висвітлення в ЗМІ виборчих кампаній»[12] та Рекомендацією №CM/Rec(2007)15 «Щодо заходів, пов'язаних з висвітленням виборчих кампаній у ЗМІ»[15] зазначається про необхідність забезпечення з боку органів державної влади неупередженого і рівноправного принципу їх роботи, наголошувалося на невтручанні органів влади у діяльність ЗМІ під час виборів та на обов'язок органів влади забезпечити захист від нападів, залякування та інших протизаконних засобів тиску на ЗМІ: «Органи державної влади повинні утримуватись від втручання в діяльність журналістів та інших працівників ЗМІ з метою впливу на вибори. <…> Органи державної влади повинні вжити відповідних заходів для ефективного захисту журналістів та інших працівників засобів масової інформації та їх приміщень, оскільки це набуває більшого значення під час виборів. Водночас цей захист не повинен перешкоджати засобам масової інформації у виконанні їх роботи»[15]. Окрім того, з метою забезпечення прозорості та доступу до ЗМІ під час виборів, встановлено вимогу, щоб у випадках коли ЗМІ мають приналежність якимось політичним партіям або політикам, про повідомлялося про це громадськість[15].

Важливою і актуальною залишається довіра українців до різних типів ЗМІ, адже саме цей показник впливає на активність їх застосування під час виборчої кампанії. За результатами соціологічного опитування USAID-Internews «Ставлення населення до ЗМІ та споживання різних типів медіа у 2019 році», презентовані 22 жовтня 2020р. в Укрінформі. «У 2019 році українці стали набагато менше довіряти ЗМІ – довіра до всіх традиційних медіа впала на 11% у порівнянні з 2018 роком. Довіра коливається між 19% до загальнонаціональної преси, 22% – до місцевого радіо та 49% – до загальнонаціональних телеканалів. <…> Популярність і охоплення аудиторії телеканалами знизився до 66% в порівнянні з 77% минулого року. Ці дані підтверджують, що традиційні медіа невпинно трансформуються в цифру, що також є глобальним трендом у медіа-індустрії»[3]. Водночас, за даними цього опитування встановлено, що загальнонаціональним інтернет-медіа довіряє 51% українців, а частка українських інтернет-користувачів починаючи з 2015 р. зросла на 14% та досягла 85% користувачів. Підвищився і показник кількості респондентів, які використовують соціальні мережі для отримання новин – 68%, що на 15% вище, порівняно з даними 2018 року (53%). Якщо прослідкувати зміну динаміки стану довіри українців до ЗМІ у попередніх роках, то лише у 2018 р. вона збільшувалася (на 10%, порівняно з 2017 р.), а у 2015 – 2017 роках вона невпинно зменшувалася «довіра до всеукраїнських телеканалів зменшилася з 61% у 2015 до 54% у 2017 році; довіра до всеукраїнських радіостанцій погіршилася з 39 до 33%, а до всеукраїнських газет – з 34 до 28% за той же період» [2]. На цей негативний процес вплинуло багато факторів, в т.ч. заполітизованість журналістської діяльності, часті медіа-маніпуляції, знаходження інформаційного простору у постійні атаці «інформаційної війни» з бору Російської Федерації (збільшення фейкової інформації) тощо.Якщо розглядати проблему рівня довіри населення до ЗМІ у розрізі їхніх типів, то із табл. 1 видно, що друковані ЗМІ як загальнодержавні, так і регіональні, стрімко втрачають рівень довіри (відповідно з 34% у 2015 р. до 19% у 2019 р.; з 36% у 2015 р. до 20% у 2019 р.), а от інтернет видання намітили динаміку до збільшення довіри (по загальнонаціональним з 47% за 2015 р. до 51% за 2019р.; по регіональним з 40% за 2015 р. до 44% за 2019 р.). На фоні тенденції зменшення користувачів друкованих ЗМІ, читачів регіональних друкованих видань поступово зменшується (з 70% у 2016 р. до 65% у 2019р.), а що стосується загальнонаціональних видань то вона не стабільна і спрямовується у бік зменшення – якщо порівнювати з 2015р. то відбулося зменшення з 61% впав до 56% у 2019р., а якщо порівнювати з 2017 р., то спостерігається певне збільшення (з 50% до 56%) (див. табл.2).

Таблиця 1 – Динаміка рівня довіри у розрізі типів ЗМІ[13]*

* Дослідження було виконано соціологічною компанією InMind на замовлення міжнародної неприбуткової організації Internews, що реалізує «Медійну програму в Україні» за фінансової підтримки Агентства США з міжнародного розвитку (USAID).

Тип ЗМІ	2015	2016	2017	2018	2019
Довіра до загальнонаціональних ЗМІ					
ТБ	61%	58%	54%	61%	49%
Інтернет	47%	52%	48%	58%	51%
Друковані	34%	31%	28%	33%	19%
Радіо	39%	36%	33%	39%	22%
Довіра до регіональних ЗМІ					
ТБ	51%	52%	46%	56%	41%
Інтернет	40%	45%	42%	52%	44%
Друковані	36%	33%	31%	35%	20%
Радіо	35%	32%	30%	34%	19%

Таблиця 2 – Аудиторія друкованих ЗМІ[13]*

Тип друкованого ЗМІ	2015	2016	2017	2018	2019
Загальнонаціональні	61%	55%	50%	58%	56%
Регіональні	63%	70%	68%	69%	65%
Зарубіжні	-	-	-	-	2%

Висновки. Таким чином, на сучасному етапі суспільно-політичних відносин, засоби масової інформації виступають не лише як ретранслятори передачі інформації від політика до населення, а стають вирішальним фактором у виборчому процесі і активно впливають на його результати. Тож з метою сприяння розвитку свободи слова та демократичних основ суспільства; забезпечення розвитку журналістики та позбавлення можливості державним та місцевим органам влади впливати на редакційну політику друкованих видань, що гарантуватиме їм незалежність в Україні була проведена реформа державних і комунальних друкованих ЗМІ.

На сьогодні надзвичайно актуальною є потреба більш активно вживати заходи для поширення інформаційної культури, яка формується завдяки медіа- та інформаційній грамотності. Особливо ця проблема актуалізується у ході передвиборчих кампаній, оскільки саме в цей період засоби масової інформації широкого застосовують різного роду медіа-маніпуляції. На фоні виникнення нових характеристик інформаційного простору політики, розвитку активного процесу віртуалізації політичного інформаційного простору, перед державними органами, експертами та й самими політиками ставиться завдання створення як законодавчих, так і моральних запобіжників, які б унеможливили та запобігли негативним політичним наслідкам. При цьому, враховуючи прагнення України до інтеграції в ЄС, необхідно дотримуватися європейських стандартів у напрямку реалізації демократичних заходів, пов’язаних із висвітленням ЗМІ виборчих кампаній, і тим самим підвищувати рівень довіри населення до медіа.

Список літератури

1. Виборчий кодекс України: Закон України від 19.12.19 р. №396. Дата оновлення: 24.10.2020. URL: https://zakon.rada.gov.ua/laws/show/396-20#Text (Дата звернення: 1.11.2020).
2. Довіра до ЗМІ в Україні зростає – нове опитування USAID-Internews щодо споживання ЗМІ. URL: https://internews.in.ua/uk/news/dovira-do-zmi-v-ukrajini-zrostaje-nove-opytuvannya-usaid-internews-schodo-spozhyvannya-zmi/ (Дата звернення: 1.11.2020).
3. Довіра українців до ЗМІ за рік знизилася на 11%. URL: https://www.ukrinform.ua/rubric-society/2803560-dovira-ukrainciv-do-zmi-za-rik-znizilasa-na-11.html (Дата звернення: 1.11.2020).
4. Дубас О.П. Інформаційно-комунікаційний простір: поняття, сутність, структура. Сучасна українська політика. Політики і політологи про неї. К., 2010. Вип. 19. С.226.
5. Карлова В.В. Вплив засобів масової інформації на формування української національної свідомості. URL:

http://academy.gov.ua/ej/ej6/txts/07kvvunc.htm (Дата звернення: 1.11.2020).
6. Медіа-маніпуляця. URL: https://uk.wikipedia.org/wiki/
7. Мойсеєв В.А. Паблік рілейшнз. Навчальний посібник. К.: Академвидав, 2007. 224с.
8. Нестеряк Ю. Державна підтримка ЗМІ: європейські традиції та українська практика. Вісник Київського національного університету. Журналістика. 2002. № 10. С.50–52.
9. Про друковані засоби масової інформації (пресу) в Україні: Закон України від 16.11.1992 р. №278. Дата оновлення: 01.10.2018. URL: https://zakon.rada.gov.ua/laws/show/5461-17#Text (Дата звернення: 1.11.2020).
10. Про реформування державних і комунальних друкованих засобів масової інформації: Закон України від 24 грудня 2015р. №917. Дата оновлення: 21.10.2018р. URL: https://zakon.rada.gov.ua/laws/show/917-19#Text (Дата звернення: 01.11.2020).
11. Рекомендація № R(97)20 про „наклепницькі висловлювання": Комітет Міністрів Ради Європи від 30 жовтня 1997 р. URL: http://www.coe.kiev.ua/docs/km/r(97)20.htm (дата звернення: 01.11.2020).
12. Рекомендація R(99)15 про висвітлення в ЗМІ виборчих кампаній: КМРЄ від 9 вересня 1999р. URL: http://www.coe.kiev.ua/docs/km/r(99)15.htm (Дата звернення: 01.11.2020).
13. Ставлення населення до ЗМІ та споживання різних типів медіа у 2019 р. URL: https://detector.media/infospace/article/171769/2019-10-22-stavlennya-naselennya-do-zmi-ta-spozhivannya-riznikh-tipiv-media-u-2019-r/ (Дата звернення: 01.11.2020).
14. Фініш реформування газет: ситуація в регіонах/ Тернопільський прес-клуб. URL: https://pressclub.te.ua/category/novyny/ (Дата звернення: 01.11.2020).
15. Recommendation CM/Rec(2007)15 of the Committee of Ministers to member states on measures concerning media coverage of election campaigns. Adopted by the Committee of Ministers on 7 November 2007. URL: https://wcd.coe.int/ViewDoc.jsp?id=1207243&Site=CM&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383 (Дата звернення: 01.11.2020).

УДК 504.54

А. Компанієць, магістр гр. ЕО-19 МЗ
Центральноукраїнський національний технічний університет

ЕКОЛОГІЧНА ОЦІНКА ЗНАЧЕННЯ РОСЛИН-ФІТОМЕЛІОРАНТІВ

У статті висвітлено необхідність використання рослин-фітомеліорантів для рекультивації відвалів гірничозбагачувальної промисловості. Швидке заростання відвалів сприяє зниженню рівня забруднення довкілля внаслідок пиловиділення місць розташування відходів збагачення.
ландшафти, грунти, протогрунти, збагачення, пиловиділення, рекультивація, рослинний покрив, фітомеліоранти, активізація екосистем

Актуальність теми. Природні форми рельєфу та рельєфоутворюючі відклади обумовлюють характер використання літосфери та земельних ресурсів в Україні.

Екологічна загроза середовищу існування людини назріває внаслідок накопичення твердих відходів у хвостосховищах та відвалах, які вже займають більш ніж 230 тис.га продуктивних земель, тобто ми втрачаємо орні землі зокрема. Ще 150 тис.га зайняті під розробкою корисних копалин, 40 тис.га - хвостосховищ, полів фільтрації і ставків-відстійників – 30 тис. га.

За даними Головного управління статистики у Дніпропетровській області, Кривий ріг посідає перше місце в області в загальному обсязі усіх розміщених промислових відходів, оскільки обсяг таких відходів щорічно становить більше 97%.

Більшість ділянок природного середовища розміщено в зоні інтенсивного антропогенного тиску, тому окремі райони області вже знаходяться в кризовому стані. В умовах індустріальної Дніпропетровщини лише на 0,5% території області збереглися природні екосистеми. Інша територія представлена модифікованими (81,3%) і в різному ступені трансформованими екосистемами. В умовах техногенезу екосистеми втрачають вагомі функції з відновлення і підтримки біорізноманіття та стійкості. Це відбувається через

перетворення верхньої частини літосфери, атмосфери і гідросфери, трансформації та знищення основи продуктивного ландшафту – грунтового покриву [1-4].

Аналіз останніх досліджень і публікацій. З розвитком напрямку відновлення територій відбувається виділення етапів, здійснюваних технічними прийомами (гірничотехнічна рекультивація), та біологічними методами (біологічна рекультивація). Рекультивація ділиться на три основних етапи: «підготовчий» («проектно-вишукувальний»), «основний» і «систематичний» або «цільовий».

Перший передбачає проведення дослідних і проектних робіт, визначення характеру підготовки і подальшого виду господарського використання. Другий включає в себе гірничотехнічну підготовку територій, що передбачає використання спеціальної техніки (бульдозерів, скреперів, самоскидів) з урахуванням запланованого цільового використання. Третій етап рекультивації забезпечує цільове використання: створення лісонасаджень, сільськогосподарських угідь, озеленення, забудову, рекреаційне використання. Першу стадію складають агротехнічні і фітомеліоративні заходи, заходи по відновленню родючості та продуктивності порушених земель, тобто біологічна рекультивація. Друга стадія – безпосереднє цільове використання з певними додатковими меліоративними заходами до повного відновлення продуктивності рекультивованих земель.

Н.Т. Масюк вводить поняття «фітомеліоративного періоду біологічного етапу рекультивації». Для цього використовують ряд рекомендованих рослин-фітомеліорантів, які є сприятливими для освоєння територій, що відновлюються, гарно приживаються, стимулюють грунтотвірний процес, нейтралізовують забруднення.

Рекультивація здійснюється з метою збереження земельного фонду країни, компенсації збитків, нанесених природньому комплексу, сільському та лісовому господарствам при експлуатації надр та для запобігання поширення негативного впливу порушених територій на грунтові, водні ресурси та повітря.

До технічного етапу відносяться: планування та формування відкосів, відвалів, терас, забезпечення стійкого стану відкосів та відвалів, утилізація порід та відходів, впорядкування земель до стану придатного для користування. Технічний етап виконується в процесі експлуатації підприємства окремими ділянками по мірі завершення гірничих робіт на цих ділянках та повного припинення деформацій та осідання гірничої маси.

Біологічний етап здійснюється після повного завершення технічного етапу та включає нанесення активного шару, внесення органічних та мінеральних добрив, висівання трав та озеленення, відновлення потенціалу земель, здійснення протиерозійних заходів. Дуже важливого значення набувають роботи з біологічної рекультивації у випадку, коли землі порушені гірничими роботами, були до цього високопродуктивними сільськогосподарськими територіями. Розробка родовищ корисних копалин супроводжується виведенням значних площ із господарського використання. До таких площ відносяться кар'єрні відпрацювання, відвали пустих порід, відходи рудопереробних фабрик [2,5,6].

Постановка завдання. Внаслідок вивітрювання, видування дрібнодисперсного мінерального пилу у великій кількості, особливо в сухі періоди літа і безсніжні зими, газовиділення та міграції токсичних сполук , - техногенні ландшафти та бедленди несуть небезпеку людському життю та здоров'ю. Крім того, пиловиділення знижує родючість полів. Пилові субстанції приносять на кожен гектар площі земельних угідь біля 0,54 г арсенікуму, 40 г плюмбуму, 163 г цинку, 27 г кобальту, 54 г нікелю, 12 г молібдену, 86 г купруму, 34 г хрому, 540 г кремнезему. Згідно даних, з відвалу висоти 20 м наноситься на поля шар пилу висотою 3,8 см, а з відвалу висотою 100 м – шар пилу у 9,96 см/рік, а це підвищує коефіцієнт забруднення пилом прилеглих територій (в 1,76-21 разів). Відвали є причиною поширення пилу на відстань 3 - 6 км.

Є проблема пиловиділення і на відвалах, відсипаних з гірських порід, що мають легкий механічний склад, які знаходяться поряд з полями, з 1 га яких переноситься до 500 т пилу в рік. Загибель сходів зернових культур трапляється за нанесення на сільськогосподарські угіддя шару пилового забруднення 4-5 см.

Пил хвостосховищ (шламосховищ) також є токсичним, його частки, дрібнодисперсні та гострі, - викликають силікоз, бронхіальну астму, та інші захворювання органів дихання. Зі шламосховищ виділяється пил 0,7-2,5 мг/с·м^2, причому радіус розповсюдження його до 5-9 км. При таких умовах з 1 га деградованих територій за рік відкладається 195,52-296,44 т, зі шламосховищ – 220,75-788,40 т пилу.

Тому головним завданням досліджень є розробка заходів для зниження пиловиділення відпрацьованих відвалів [1,2].

Виклад основного матеріалу. При біологічній рекультивації на техногенних об'єктах найпоширенішим способом утворення рослинного покрову є екстенсивний спосіб господарювання, або самозаростання протоґрунтів під впливом природних факторів грунтотвірного процесу. З часом трави на неудобрених гірських породах забезпечують майже таку продуктивність, як і на непорушених орних землях.

Хід природного заростання відвальних порід насамперед визначається їх хімічним і гранулометричним складом. Відвали залізорудної промисловості починають в невеликій мірі займатися рослинністю вже на другий рік. Та через щорічне зростання величини нормативів збору за забруднення атмосферного повітря і, відповідно, збільшення суми збору за викиди неорганічного пилу, екстенсивний спосіб господарювання на техногенних об'єктах не є прийнятним.

Потрібно впровадження інтенсивних способів закріплення пилоутворюючих поверхонь техногенних об'єктів, які не тільки забезпечують зменшення суми збору пропорційно зменшенню площ, на яких утворюється пил, але й вивільнять кошти, які можна направити на додаткові природоохоронні заходи на підприємствах. На токсичних пилових поверхнях техногенних ландшафтів пропонується проводити закріплення за допомогою органічних відходів. Запобігання розпиленню з техногенних поверхонь гірничих об'єктів базується на використанні водних розчинів хімічних речовин та озелененні (біологічна рекультивація) з використанням рослин-фітомеліорантів. [].

Активізація створення рослинного покриву на пилоутворюючих поверхнях, забезпечує надійне закріплення поверхонь протоґрунтів за період у 2-3 роки. Стійкий до несприятливих гідрометеорологічних умов рослинний покрив багатократно зменшує пилоутворення техногенних об'єктів, перешкоджає вітровій та водній ерозії задернованих площ і значно поліпшує стан атмосферного повітря у робочих зонах і на розташованих навколо селітебних територіях. У практиці рекультивації земель відомі способи продуктивного засвоєння породних відвалів без нанесення грунтового шару і підстилаючих суглинків.

Для впровадження в практику нових способів рекультивації відвалів на гірничотехнічному етапі використовується стандартне гірське устаткування і прості схеми його використання, а на біологічному етапі – прийнятні в сучасних умовах методи підвищення якості ґрунтів, що покривають відвал, недорогий і доступний насінний і посадковий матеріал, з відходів зерноочищення на елеваторах та отримані в ботанічному саду.

Відвали ІнГЗК, як свідчать результати наших досліджень, не придатні під сільськогосподарський, рекреаційний, водогосподарський і навіть будівельний напрямок рекультивації. Тому згідно алгоритму визначення напрямку рекультивації для них рекомендується лише захисний лісовий і санітарно-гігієнічний напрямок рекультивації, які виконуються шляхом висадки дерев, кущів і багаторічних трав для закріплення відвалів та зменшення пилоутворення і його розповсюдження. У сформованих жорстких умовах даних бедлендів це є оптимальним результатом, оскільки озеленення території також поліпшує екологічний стан природних об´єктів.

Протоґрунти поверхонь відвалів розкривних порід ПАТ «ІнГЗК» добре конденсують вологу з повітря, що обумовлено переважанням кварцитів в їх мінералогічному складі. Але показники пористості і коефіцієнт фільтрації розкривних порід, особливо глин і суглинків, істотно менший ніж у природних аналогів – чорноземів або глинистих сланців. Не сприяє

однорідності водного балансу протоґрунтів відвалів наявність великоуламкових компонентів у вигляді каменів і брил, а також щебеню у суміші з суглинками. За подібних умов поверхні відвалів не можуть забезпечити поглинання всіх атмосферних опадів і втрачають їх частину з поверхневим стоком.

Для підвищення родючості і поліпшення агрофізичних властивостей ґрунтів з подальшим створенням на них стійкого рослинного покриву за один вегетаційний період використовують сухі витримані знезаражені мулові осади стічних вод (ОСВ) для оптимізації мінерального живлення рослин відновлених ґрунтів на поверхні відвалів. Методом використання гідромоніторів наноситься суміш вологого осаду та насіння піонерної рослинності.

Внесення у протоґрунти відвалів і сухих пляжів хвостосховища знезаражених мулових осадів очисних споруд істотно збільшує можливості формування стійкого рослинного покрову, який перешкоджає пилоутворенню. Органічна речовина мулових осадів сприяє агрегуванню поверхні ґрунтів і зниженню темпів розвитку вітрової ерозії. Внесення мулових осадів значно збільшує ємність поглинання атмосферної вологи та осадків, зменшує їх випаровування, і таким чином виправляє водний баланс протоґрунтів та перешкоджає водній ерозії поверхні техногенних об'єктів. Метод активізації формування екосистем, що пропонується, базується на принципах функціонального управління водним та сольовим балансом, вуглецевими параметрами порушених гірничими роботами земель, забезпечений наявністю та дешевизною компонентів активізаційної суміші (насіння, вода, осади стічних вод) та розробленим обладнанням для його використання на порушених гірничими роботами землях.

Незважаючи на високу потенційну ефективність методу нанесення активізаційної суміші гідромонітором, необхідно з’ясовувати залежність продуктивності від технічних та технологічних чинників. Перевагою цього методу є те, що його можна використовувати в однаковому ступені незалежно від рельєфних умов з розрахунковою ефективністю від 1,8 тис.$м^3$ на 3,6 га на годину до 1,8 тис. $м^3$ на 4,5 га за годину, за умови тиску 0,5 МПа, швидкості подачі – 0,5 $м^3/с$ та норми нанесення – 50 $дм^3/м^2$. Даний метод активізації розвитку екосистем за рахунок збільшення вуглецевих параметрів екосистем та інтродукції фітокомпоненту шляхом дистанційного нанесення суміші осадів стічних вод, насіння рослин та води гідромонітором на автотранспортному засобі, є ефективним для нанесення активізаційної суміші з метою розвитку рослинного покриву при негативному відношенні концентрацій важких металів у пустих породах до фонової концентрації у ґрунтах.

Щодо якості витриманих ОСВ свідчить знезараження на відкритому повітрі завдяки тривалому впливу сонячного випромінювання, високих і низьких температур та інших факторів (табл. 1), зокрема відсутність яєць гельмінтів і низький індекс БГКП (при нормі - 10000 КОЕ/$дм^3$) в ОСВ.

Таблиця 1 – Якісні показники маси осадів стічних вод, що вносяться на відвалах ІнГЗК

Вологість, %	Вміст органічної речовини на суху речовину, %	Вміст фракції крупніше 50 мм, %	pH	Вміст поживних речовин на сухий продукт, %		Наявність життєздатних яєць гельмінтів, шт./кг	Індекс БГКП, КОЕ/$дм^3$
				N	P_2O_5		
22,4	17,5	<2	6,1	2,76	0,84	Відсутні	<900

Достатній вміст азоту і фосфору вказує на високу цінність даних ОСВ як добрива для ґрунтів відвалів ПАТ «ІнГЗК», які практично повністю позбавлені цих найважливіших для рослин поживних елементів. Органіка проходить мінералізацію за час зберігання на відкритих мулових майданчиках. Оптимальний вміст органічної речовини у ґрунтах слід вважати 10...20 %.

Тому допускається внесення знезаражених мулових осадів очисних споруд, навіть якщо в них будуть спостерігатися перевищення ГДК по окремим видам важких металів, так як завдяки міграції розчинних форм важких металів відбудеться усереднення ГДК мулових осадів та розкривних порід з наближенням останніх до фонових значень.

Внесення осадів стічних вод при висаджуванні дозволяє збільшити процент приживання та пришвидшує розвиток рослин майже вдвічі.

Встановлено, що на поверхнях техногенних об'єктів можуть приживатися кормові багаторічні злакові та бобові рослини, особливо, якщо попередньо збагатити бідні субстрати (протоґрунти) органічними речовинами, які входять до обеззаражених мулових осадів очисних споруд. Середній вміст важливих для рослин речовин в сухому залишку мулових осадів складає: Nзаг.-2...7%; P2O5 – 1,5...7%; K2O - 0,15...0,35%; гуміфіковані органічні речовини - 50...70 %. Після внесення мулових осадів відбувається підвищення вмісту гумусу і головних поживних елементів – азоту, фосфору, калію, а також поліпшуються водно-фізичні властивості ґрунту.

Для досягнення поставленої мети нами було проведене ботанічне тестування тільки тих трав, які прижилися на території даного міста, є доступними і недорогими, наприклад пирій повзучий, мокриця, люцерна, спориш і інші види трав. Методологічний вибір найбільш ефективних трав місцевого походження здійснювався за такими критеріями: морозостійкість, посухостійкість, за ґрунтовими особливостями, за строками цвітіння, затратами на посівний матеріал.

Дослідження показали, що незважаючи на жорсткі умови зростання, високу здатність піонерного заселення техногенних об'єктів мають більше 20 видів бур'янових рослин, які висівають насіння в осінній період, що сприяє активному їх розростанню у весняно-літній період. Відвали хвостів збагачення рослинність «освоює» вже на другий рік. Мікрорельєф, водний режим, форма відвалів, алелопатія проявляються аналогічно природним рельєфам і ландшафтам, з відміною щодо швидкості та видового різноманіття, адже зазвичай заростання відвалів відбувається, за зональним типом. Піонерні рослини мають чіткі ксероморфні ознаки – потужну кореневу систему, подушкоподібну надземну частину, опушення чи восковий наліт на листках і стеблах.

Виявлення амплітуди коливань екологічних показників у рослин, що вирощуються на техногенних токсичних поверхнях разом з різними агротехнічними заходами, зокрема внесення органіки будь-якого походження, допомагає обрати перспективні види рослин для біологічної рекультивації. Для встановлення асортименту рослинних представників, придатних для фітомеліорації техногенних відвалів, вченими і практиками досліджувалось понад 230 видів, а засолених червоних шламів - 160, з них визнано придатними для рекультивації відповідно 30 і 8 видів.

Оліготрофні види рослин мають перевагу, так як вони невибагливі до родючості ґрунтів (сосна звичайна, береза бородавчаста та ін.).

При активізації формування рослинності за рахунок нанесення доступної в даному регіоні суміші осадів стічних вод, насіння рослин та води відбувається злипання органічних часток та насіння до субстрату та проникнення суміші у глибші горизонти під дією напору, що створюється гідравлічною системою. За нанесення активізаційної суміші напровесні вже у перший рік утворення пилу зменшується в 2,5 рази, на другий рік в 5 разів за рахунок швидкого розвитку рудеральних (бур’янових) видів рослин зі значною біомасою. Але на третій рік проективне покриття біомасою рослин (а отже і ризик пилоутворення) знижується до показників першого року і так триває до 10 років. Це пояснюється зміною сукцесій, коли рудеральна рослинність змінюється, зокрема на буркуново-полинну чи злакову. В умовах самозаростання така зміна сукцесійних стадій заростання відбувається лише через 15-20 років. Окрім того на 4-5 рік помітно збільшується біомаса деревних та чагарникових рослин, яка і забезпечує подальше стабільне зменшення ризику пилоутворення. Вартість проведення активізації формування екосистем за рахунок нанесення суміші осадів стічних вод, насіння рослин та води в 6-10 разів дешевше за рекультивацію (вартість рекультивації 40-100 тис.

грн. / га, вартість активізації 7-10 тис. грн. / га). Продуктивність методу за умови розпилення суміші гідромонітором однією установкою складає 2-3 га за робочий день (8 годин) [2,4-7].

Висновки.

Таким чином, організаційно-технічні рішення для зменшення екологічних ризиків пилоутворення (у 2,5-5 разів) полягають у формуванні щільного рослинного покриву з використанням видів рослин-фітомеліорантів (проективне покриття 60-80%) з поступовим збільшенням надземної фітомаси та прискоренням зміни сукцесійних стадій природного заростання на 15-20 років.

Список літератури

1. Східний гірничо-збагачувальний комбінат [Електронний ресурс]. – Режим доступу: https://www.vostgok.com.ua/history
2. Експериментальні роботи з дослідження нових способів зниження або усунення процесів пилоутворення із сухих пляжів хвостосховища, пилоутворюючих поверхонь відпрацьованих відвалів та інших пилоутворюючих поверхонь об'єктів ВАТ «ІнГЗК». Звіт НДР № держреєстрації 01090006136. – КТУ: Кривий Ріг, 2009. – 45с.
3. Екологічний паспорт Дніпропетровської області / Державне управління охорони навколишнього природнього середовища в Дніпропетровській обл. – Дніпропетровськ, 2020. – 235 с.
4. Сметана О.М. Біогеоценотичний покрив ландшафтно-техногенних систем Кривбасу / О.М. Сметана, В.В. Перерва – Кривий Ріг: Видавничий дім, 2007. – 247 с.
5. Науково-методичні рекомендації щодо поліпшення екологічного стану земель, порушених гірничими роботами (створення техногенних ландшафтних заказників, екологічних коридорів, відновлення екосистем) / [А.Г. Шапар, О.О. Скрипник, П.І. Копач та ін.] – Дніпропетровськ: Моноліт, 2007. – 270 с.
6. ГОСТ 17.5.3.03–80 «Загальні вимоги до гідролісомеліорації»
7. Шапарь А.Г. Активизация самовосстановления биогеоценозов деградированных земель Ингулецкого ГОКа / Шапарь А.Г., Скрипник О.А., Палеха В.Н. [и др.]. // Проблеми природокористування, сталого розвитку та техногенної безпеки регіонів: міжнар. конф. - Дніпропетровськ, 2005. – С.147-148.

УДК 338.439

А. Коротка, магістр гр. ЕО-19М
С. Мартиненко, доцент
Центральноукраїнський національний технічний університет

«ЕКОЛОГІЧНА ОЦІНКА УТИЛІЗАЦІЇ ПОБУТОВИХ ВІДХОДІВ ПІДПРИЄМСТВОМ «ЕКОСТАЙЛ»

У статті розглянута проблема з складуванням та утилізацією твердих побутових відходів (надалі ТПВ) , яка значною мірою впливають на економічну та екологічну ситуацію в країні, оскільки полігони ТПВ займають площі цінних земель, спричиняють забруднення об'єктів довкілля.

Актуальність. Актуальним є те, що необхідно терміново впроваджувати новітні технології в галузі ресурсозбереження та використання видів відходів, більшість з яких піддається переробці та може бути використана в інших виробництвах.

Мета дослідження. Визначення засобів утилізації ТПВ підприємства «Екостайл» у м. Кропивницькому та надання рекомендацій по їх удосконалення спираючись на світовий досвід.

Для досягнення поставленої мети були передбачені такі **завдання**:

- вивчити стан питання поводження з відходами
- дослідити екологічний вплив полігону на навколишнє середовище;
- проаналізувати, чи дотримано вимоги по влаштуванню полігону ТПВ згідно

ДБН В.2.4.-2-2005;

- запропонувати оптимальну схему роздільного збирання та сортування ТПВ на базі ТОВ «Екостайл»;
- розглянути можливість отримання та використання біогазу

Об'єктом даного дослідження є полігон твердих побутових відходів в м. Кропивницькому.

Предмет дослідження- процеси, що відбуваються в навколишньому середовищі (ґрунті, воді та атмосферному повітрі) під впливом полігону твердих побутових відходів.

Результати дослідження.

Сучасний стан поводження з відходами в Україні та світі

На сьогоднішній день однією з найважливіших проблем людства – це поводження з відходами. Україна потрапила на 9 місце рейтингу країн з найбільшим обсягом сміття на одного жителя за версією американського агентства 24/7 Wall Street. В Україні ж найбільшу кількість ТПВ переважають густонаселені регіони. Але при цьому, лише 3/4 населення країни, користуються послугами з вивезення ТПВ.

Кожен рік накопичення твердих побутових відходів значно зростає. Загальна кількість відходів на одну людину становить близько 300 кг.

Починаючи з 2000-х років, роль ТПВ суттєво зростає, тому виникає питання необхідності прийняття заходів, які мають застосовуватися з поводження з ТПВ.

Рис. 1.1 – Структура ТПВ в Україні в %

Можна сказати, що ситуація в Україні виглядає таким чином:

- підвищення питомих обсягів утворення ТПВ (на 70% за період 2000 – 2010 років) попри зменшення кількості населення;
- підвищення частки фракцій, що переробляються, у структуррі ТПВ та, відповідно, розбудова потужностей у сфері переробки;
- низьке охоплення населення в сільській місцевості послугами зі збирання відходів;
- низький рівень переробки відходів (менше 8%) попри швидке зростання кількості міст, в яких реалізується їх родільне збирання;
- збільшення обсягу вивозу ТПВ на полігони та несанкціоновані звалища.

Накопичення відходів на полігонах та звалищах дає великий негативний вплив на навколишнє середовище. Адже, викиди звалищного газу негативно впливають за зміну клімату.

На жаль, більшість діючих полігонів вже застаріли і напевно в майбутньому вже не зможуть приймати зростаючий обсяг відходів. Зрештою , якщо така експлуатація відходів буде продовжуватись, то це спричинить значні екологічні наслідні, які згодом можуть позначитися на здоров'ї цілої нації.

Утилізація побутових відходів підприємством «Екостайл»

В лютому 2016 року Головним управлінням житлово – комунального господарства Кіровоградської міської ради було проведено конкурс з визначення виконавця послуг з вивезення твердих побутових відходів з території м. Кропивницького (колишній Кіровоград).

За результатом якого, ТОВ «Екостайл» було визначено переможцем та укладено договорі №6 від 01.03.2016р. на надання послуг з вивезення побутових відходів з території Подільського та №8 від 01.03.2016р.на надання послуг з вивезення побутових відходів з території Фортечного району м. Кіровограда.

Сміттєзвалище твердих побутових відходів міста Кропивницький займає площу 18,8697 га. Воно розташоване в яру на території колишнього вапняково- ракушнякового кар'єру.

Віддаленість від населеного пункту міста Кропивницький 0,39 км; від водотоків і водойм – 1,0 – 1,1 км; від водозабірних споруд – більше 2,0 км.

Глибина залягання підземних вод- 2,9 м та 9,52 м. Водоносний горизонт – безнапірний. Грунтові води- гравітаційні підземні води першого від поверхні Землі постійного водоносного горизонту, що залягають на першому водонепроникному шарі земної кори і утворюються головними чином шляхом інфільтрації (просочування) атмосферних опадів і вод річок, озер, водосховищ, зрошувальних каналів та шахтових водовідвідних канав. До них належать усі неглибоко залеглі безнапірні або з місцевим напором підземні води, які дренуються гідрографічною сіткою і формують грунтовий стік. У системі вертикальної зональності підземних вод вони займають верхній ярус і належать до зони інтенсивного або повільного водообміну. Режим їх тісно пов'язаний з гідрометеорогічними факторами (температура повітря, атмоферний тиск та кількість атмосферних опадів). По геологічному розрізу – яр складається із суглинків, супісків, частина схилів відходів обвалована. Дренажні канави- відсутні.

Перед захороненням відходів проводиться сортування. Сортувальна лінія з відбором вторинної сировини забезпечує сортування відходів.

Усі автомобілі перед в'їздом на сміттєзвалище проходять зважування на ваговій, візуальний огляд та радіометричний контроль.

Тверді побутові відходи завозяться на сортувальну лінію. Автомобілі висипають відходи на окрему ділянку та загружаються в бункер, з нього подаються по транспортній стрічці до розподільного бункера .

Відходи перед захороненням пошарово складаються, проводиться їх ущільнення, присипаються інертним матеріалом, поверхнево зволожуються.

Результат дослідження.

У липні 2018 року полігон підприємства «Екостайл» отримав ліцензію на право провадження господарської діяльності з захоронення побутових відходів. Згідно з постановою НКРЕКП від 04 квітня 2017 року № 467 про затвердження ліцензійних умов на право провадження господарської діяльності з захоронення побутових відходів ліцензіат повинен забезпечити наступні технологічні вимоги:

- Земельна ділянка, об’єкти, споруди, засоби механізації, призначені для захоронення побутових відходів
- Виробничо-технічна база, необхідна для експлуатації об’єктів, споруд, засобів механізації, призначених для захоронення побутових відходів
- Дотримуватися показників якості надання послуг з захоронення побутових відходів
- Окремий облік прийнятих побутових відходів, промислових відходів IV класу небезпеки, інших відходів
- Контроль за станом підземних вод, водойм, атмосферного повітря, ґрунтів і рослин, шумовим забрудненням в зоні можливого негативного впливу місця провадження діяльності
- Приймати на захоронення побутові відходи (крім рідких побутових відходів та небезпечних відходів у складі побутових відходів), залишок побутових відходів після їх перероблення; приймати промислові відходи IV класу небезпеки лише для використання як ізолювального матеріалу

- Не приймати побутові відходи, якщо вони змішані з іншими видами відходів
- Провадити зволоження полігону у пожежонебезпечні періоди.

Для удосконалення технології захоронення відходів, згідно стандартів ISO, ТОВ «Екостайл» збільшило щільність ущільнення сміття з 0,25-0,8 тон/м.куб за допомогою компактора. Це дозволило подовжити термін експлуатації сміттєзвалища на 15 років. В Україні захоронення відходів за допомогою такого компактора використовують лише в Києві, а віднедавна й у Кропивницькому.

Висновки. 1. Проведений аналіз літературних джерел, щодо поводження з твердими побутовими відходами , можна сказати, що світовий досвід поводження з відходами значно вищий ніж в Україні. Наша країна має досить застарілі методи утилізації.

2. Досліджено динаміку питомого накопичення відходів в Кіровоградської області. Можна сказати, що очікується значне зростання відходів на душу населення.

3. Досліджено технологічну схему збору та утилізації біогазу. Для інтенсивного нарощування виробництва біогазу та енергії з нього необхідно створити умови для розвитку цього виду бізнесу, які дозволили б залучати як 21 вітчизняні, так і іноземні інвестиції, використовувати передові закордонні технології, а також сприяли б розвитку вітчизняних аналогів на базі інноваційних рішень.

4. Проведена узагальнена оцінка дотримання правил, щодо використання полігонів підприємством ТОВ «Екостайл». Впровадження роздільного сортування відходів на території підприємства.

5. Запропоновані оптимальні шляхи поводження з твердими побутовими відходами у Кіровоградській області для їх подальшого використання як вторинної сировини. Виконана оцінка екологічного ефекту від реалізації запропонованого рішення.

Список літератури

1. Україна потрапила в топ країн з найбільшим обсягом сміття на людину. (Електронний ресурс)/ Режим доступу : URL : https://www.pravda.com.ua/news/2019/07/15/7220956/ - Загол. з екрану.
2. Тверді побутові відходи – утворення та переробка. (Електронний ресурс) / Режим доступу: URL : http://www.saleprice.com.ua/ua/publications/540.html - Загол. з екрану.
3. Технологія утилізації твердих побутових відходів. (Електронний ресурс)/Режим доступу: URL: https://core.ac.uk/download/pdf/11331278.pdf - (Загол.з екрану)
4. Экология города: Учебник. / Ф.В. Стольберг, В.Я. Шевчук, И.Г. Червanёв – К.: Либра, 2000. – 464 с.
5. Утилізація сміття. (Електронний ресурс)/ Режим доступу: URL: https://sites.google.com/site/utilizaciasmita111/ -(Загол. з екрану)
6. Стратегічний аналіз соціально-економічного розвитку Кіровоградської області. (Електронний ресурс)/ Режим доступу : URL : http://economika.kr- admin.gov.ua/files/sag0719.pdf (Загол. з екрану)
7. Регіональна доповідь про стан навколишнього природнього середовища Кіровоградської області 2019 року. (Електронний ресурс)/ Режим доступу: URL: http://ekolog.kr-admin.gov.ua/diialnist/stan-dovkillia-kirovohradskoi-oblasti/rehionalna-dopovid-pro-stan-navkolyshnoho-pryrodnoho- seredovyshcha-kirovohradskoi-oblasti (Загол.з екрану)
8. Стратегічний аналіз соціально-економічного розвитку Кіровоградської області. (Електронний ресурс)/ Режим доступу : URL : http://economika.kr- admin.gov.ua/files/sag0719.pdf (Загол. з екрану)
9. Відомості про підприємство. (Електронний ресурс)/ Режим доступу : URL : https://ecostyle.in.ua/pro-pidpriiemstvo/vidomosti-pro-pidpriiemstvo/ (Загол. с екрану)
10. Постанова про затвердження порядку ведення реєстру місць видалення відходів. (Електронний ресурс)/ Режим доступу: URL :
11. https://zakon.rada.gov.ua/laws/show/1216-98-%D0%BF#Text (Загол. з екрану)

УДК 621.43.06

М. Красота, магістр гр. АТ 19МЗ
Центральноукраїнський національний технічний університет

ТИПОВІ НЕСПРАВНОСТІ ЕЛЕКТРОМАГНІТНИХ ФОРСУНОК БЕНЗИНОВИХ ДВИГУНІВ

В роботі встановлено найбільш значимі фактори, що впливають на технічний стан електромагнітних форсунок. Виявлено типові дефекти та несправності форсунок, якими є обривання витків соленоїдів, міжвиткове замикання, руйнування конекторів, забрудення проточної частини форсунки, забруднення фільтрів, заклинювання клапана. Ці несправності приводять до погіршення екологічних та динамічних показників двигунів, а отже існує необхідність в проведенні достовірного діагностування ЕМФ при виконанні технічних обслуговувань та ремонтів.
форсунка, система живлення, забруднення

Постановка проблеми. Одним з найбільш відповідальних елементів системи паливоподачі сучасних бензинових двигунів є електромагнітна форсунка (ЕМФ).

Якісне протікання процесів дозування палива та створення паливної суміші багато в чому визначається технічними характеристиками ЕМФ. Застосовувані в двигунах з вприскуванням палива ЕМФ володіють великою кількістю важливих робочих показників, працюють в імпульсному режимі в складних умовах вібрації двигуна, підвищених температур і забруднення палива. Для підтримання необхідної швидкодії і точності дозування палива протягом всього терміну роботи ЕМФ висуваються жорсткі вимоги до досконалості їх конструкції.

Параметри ЕМФ в процесі експлуатації поступово знижуються. Це пов'язано з забрудненням фільтрів і проточної частини, зносом рухомих деталей, можливим міжвитковим замикання в обмотці котушки електромагнітна та іншими несправностями ЕМФ. Виникнення цих несправностей приводить до зміни енергетичних та екологічних характеристик двигуна, що пояснює необхідність періодичного контролю технічного стану ЕМФ.

Однак, існуючі методи оцінки працездатності ЕМФ володіють рядом серйозних недоліків. З одного боку, можливе проведення якісного всебічного діагностування ЕМФ, але виконання такої комплексної перевірки передбачає демонтаж ЕМФ з двигуна і використання складного і дорогого стендового обладнання , що не завжди економічно виправдано. З іншого боку, методи, що не передбачають виконання демонтажних робіт, не дозволяють отримати повну картину технічного стану ЕМФ, оскільки не дають можливість визначити абсолютні значення основних робочих показників ЕМФ і тому не отримали широкого практичного застосування.

Аналіз останніх досліджень та публікацій. Проблематика, що вирішується в даній роботі була також досліджена в наукових працях [1-7].

Мета і завдання досліджень. *Метою роботи* - є дослідження причин зниження технічного стану ЕМФ та шляхів виявлення цих несправностей.

Для досягнення поставленої мети вирішувалися наступні задачі досліджень:

1. дослідити типові несправності та забруднення ЕМФ та встановити причини їх виникнення;
2. проаналізувати фактори, що визначають зміну технічного стану ЕМФ;
3. визначити частоту зустрічання дефектів ЕМФ.

Об'єкт дослідження – електромагнітна форсунка системи живлення бензинового двигуна.

Предмет дослідження – процеси функціонування форсунок бензинових двигунів з електронною системою управління та зміна їх технічного стану.

Методи досліджень базуються на експериментальних методах виявлення несправностей електромагнітних форсунок.

Електромагнітна форсунка (ЕМФ) являє собою швидкодіючий гідравлічний клапан з електромагнітним приводом замикаючого елементу. У системах паливоподачі з електронним управлінням форсунки виконують дві функції:

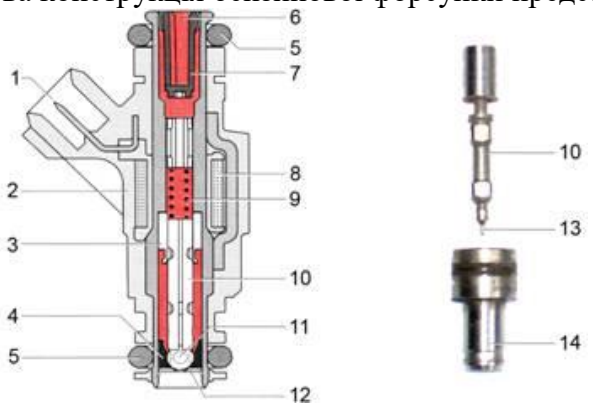
- дозують паливо відповідно з тривалістю електричних управляючих імпульсів, сформованих електронним блоком управління (контролером) по певному алгоритму, залежно від режимних параметрів роботи двигуна;

- розпилюють (диспергують) паливо до частинок необхідних розмірів для досягнення необхідного ступеня гомогенізації паливоповітряної суміші.

На сьогоднішній день всі нові автомобілі з бензиновим двигуном мають системи розподіленого вприскування. Однак при цьому виникають специфічні проблеми, пов'язані з експлуатацією цих систем, в основному через невисоку якість бензину (близько 40 % виробленого палива не відповідає чинним вітчизняним технічним регламентам) і недостатньо високої культури експлуатації автомобільної техніки [1]. Багато в чому ці проблеми і визначають експлуатаційні зміни робочих показників електромагнітних форсунок.

Електромагнітна форсунка є останньою і найважливішою ланкою на шляху бензину до циліндра. Циклова доза бензину, що вприскується до 2-літрового двигуна в режимі часткового навантаження складає всього 0,03 ... 0,04 мл. Сувора геометрія конструкції, мініатюрні розміри в сполученні «запірний елемент - сідло розпилювача» і прецизійне виготовлення забезпечують точність дози і дрібну дисперсність розпилу бензину при номінальній інерційності рухомих частин. Однак, це відбувається тільки тоді, коли всі внутрішні деталі інжектора ідеально чисті.

Електромагнітні форсунки системи живлення бензинового двигуна активізуються електричним струмом. Такі форсунки застосовуються в більшості сучасних двигунів з розподіленим уприскуванням бензину і можуть бути з нижнім, боковим або верхнім підведенням палива. При нижньому підведенні здійснюється постійний проток бензину через форсунку, що забезпечує її охолодження і запобігає утворенню бульбашок пари. При підвищеному тиску впорскування (300-400 кПа) ця проблема вирішується і без протоку палива через форсунку. Типова конструкція бензинової форсунки представлена на рис. 1.



1 - електричний роз'єм; 2 - корпус; 3 - напрямна втулка; 4 - сідло розпилювача; 5 - ущільнювальне гумове кільце; 6 - гідравлічний впускний роз'єм; 7 - сітчастий паливний фільтр; 8 - електрична обмотка; 9 - поворотна пружина; 10 - голка з запірним елементом; 11 - сферичний запірний елемент; 12 - пластина розпилювача з отворами; 13 - запірний елемент шток; 14 – розпилювач

Рисунок 1 – Будова електромагнітної бензинової форсунки

У процесі експлуатації технічний стан форсунок, що оцінюється значенням їх робочих показників, неминуче погіршується через забруднення елементів проточної частини, зносу замикаючого елементу і сідла, відхилення характеристик електромагнітної системи, засмічення індивідуальних сітчастих фільтрів та ін. [2, 3]. Ці експлуатаційні зміни робочих показників електромагнітної форсунки визначаються якістю і складом використаного палива, умовами експлуатації двигуна, особливостями зміни навантажень при роботі двигуна у складі транспортного засобу, культурою технічного обслуговування автомобільної техніки та ін.

Експлуатаційні зміни робочих показників форсунок (статичної та динамічної продуктивності, нерівномірності подачі палива в комплекті форсунок) здійснюють складний і взаємопов'язаний вплив на економічні та еколого-технічні характеристики двигуна, його пускові якості, на динаміку транспортного засобу.

Існуючі способи очищення електромагнітних форсунок (хімічні, ультразвукові) часто не дають бажаного ефекту і не дозволяють в процесі експлуатації відновити їх робочі показники до вихідних значень.

Необхідність очищення форсунок виникає або за фактом погіршення характерних характеристик двигуна, або після 20...30 тис. км пробігу при черговому ТО [2].

Статистика показує, що з необхідністю очищення інжекторів пов'язано більше половини всіх ремонтів систем впорискування бензину, а з урахуванням планово - профілактичних очисток це число сягає 80 ... 85 %. Таке часте звертання до інжекторів вимагає їх ретельної діагностики. Як правило, тестуються опір обмотки, баланс, герметичність, факел. Інерційність перевіряють не завжди, і частіше всього через відсутність потрібної апаратури. Проте встановити істинний стан електромагнітного інжектора можна тільки за сукупністю всіх параметрів, тому практика змушує шукати доступні діагностичні методи [2].

Сучасні електромагнітні форсунки виготовляються з допуском в 1 мкм і здатні відпрацювати до мільярда циклів.

Аналіз наукових джерел інформації дозволив отримати класифікацію несправностей електромагнітних форсунок (рис. 2) [2-7].

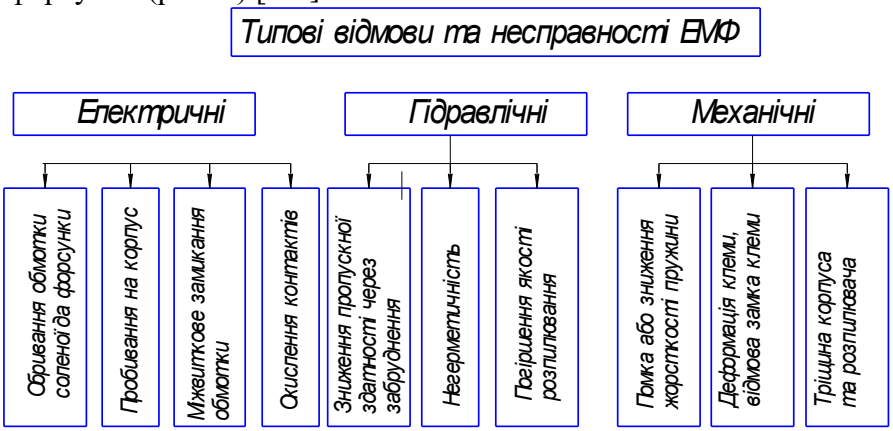


Рисунок 2 – Класифікація несправностей ЕМФ

Електричні дефекти (пробивання обмотки, міжвиткове замикання) можуть бути наслідком температурного впливу на форсунки, зокрема на ізоляційні матеріали обмотки. Обривання обмотки також може бути пов’язане з дією вібрацій при роботі двигуна. Окислення контактів конекторів пов’язане з корозією в результаті впливу оточуючого середовища.

Для гідравлічної групи основна причина несправностей полягає у вмісті в легких паливах домішок важких фракцій, а також дрібнодисперсних твердих часток, що ускладнюється незадовільним станом паливних фільтрів.

Механічні пошкодження є наслідком дії циклічних вібрацій двигуна та самої форсунки, тобто в результаті втомлення матеріалів.

За частотою зустрічання пошкоджень ЕМФ можливо привести наступну діаграму [6] рис. 3.

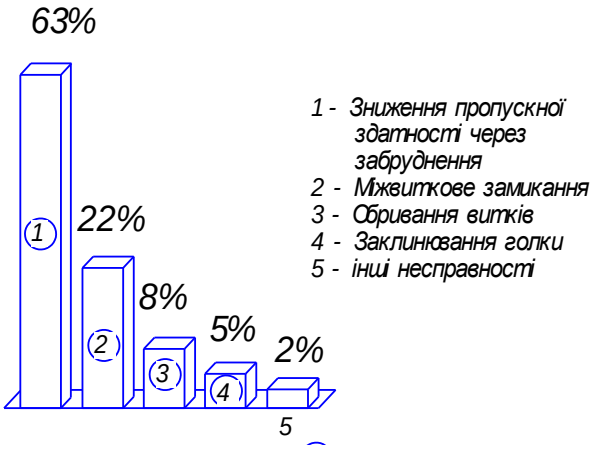


Рисунок 3 – Частота зустрічання дефектів ЕМФ

Таким чином, основною причиною порушення їх роботи є зниження пропускної здатності в результаті відкладення забруднень в процесі експлуатації, хоча на шляху механічних частинок стоять паливні фільтри, які відсівають частки крупніші 10-20 мкм.

Фільтри встановлюються в паливній магістралі і в самій форсунці.

У корпусі форсунки розташовані обмотка електромагніту і двоконтактний електричний роз'єм (рис. 1). Залежно від особливостей обмотки її опір може перебувати в межах від 2 до 16 Ом. Замикаючий елемент буває плоским, конічним і сферичним. Плоскі клапани, як правило, мають малу масу (0,5 г), що забезпечує необхідну для високотехнологічних двигунів швидкодію. Недоліком плоских клапанів є часте порушення герметичності внаслідок засмічення та зносу.

Належну герметизацію забезпечують клапани зі сферичною ущільнюючою поверхнею, але вони застосовуються переважно для форсунок в системах центрального вприскування бензину. Останнім часом найбільшого поширення набули форсунки з конічним ущільненням клапана ("Бош", "Лукас", "Мареллі"), що забезпечують стабільні показники в процесі тривалої експлуатації.

Конструкція і параметри розпиляючого елемента визначають факел палива, що формується залежно від місця встановлення форсунки на двигуні. При центральному вприскуванні кут факела доходить до 55 градусів. При розподіленому вприскуванні форма факела також визначається місцем розташування форсунки і конфігурацією впускного каналу. При встановленні форсунки в головці циліндра, поблизу від впускного клапана, кут факела зменшують до 25-45 градусів. У разі розташування форсунки у впускному трубопроводі, тобто на великій відстані від клапана, кут факела зменшують до 15-25 градусів – так, щоб основна частина палива на потрапляла на стінки впускного каналу.

Прохідний перетин сопла форсунки – кільцева щілина, утворена корпусом розпилювача і штифтом. З появою відкладень просвіт "заростає". Тиск же палива у форсунці на працюючому двигуні постійний, а час дії керуючого імпульсу і, відповідно, тривалість її відкриття визначаються електронним блоком керування (ЕБК).

Аналізуючи склад вихлопних газів, а точніше, частку в них кисню, ЕБК спочатку віддає команду форсункам збільшити подачу палива, збільшуючи час вприскування, але цей процес не може тривати надто довго. Крім того, з втратою герметичності погіршується відсікання палива. Замість того, щоб різко обірвати факел, відправивши всю порцію у впускний канал, форсунка закінчує уприскування плавно. Останні краплі не можуть "вистрілити" і залишаються на розпилювачі.

Водночас, паливо продовжує просочуватися із закритого розпилювача. Порушується і форма факела, а отже частина палива потрапить не в просвіт впускного каналу, а, наприклад, на його стінки, і в циліндр надійде менше бензину.

Також, відкладення погіршують однорідність розпилювання. З форсунок летять великі краплі, не встигаючи випаровуватися, перемішатися з повітрям і, як наслідок, згоріти в циліндрах. Словом, відбувається неузгодженість роботи системи уприскування. В результаті – з'являються симптоми: ускладнений пуск, нестійкий холостий хід, "провали" при розгоні, підвищена витрата палива, втрата потужності.

Для того, щоб уникнути забруднень виробники паливної апаратури удосконалюють конструкцію форсунок, застосовують нові матеріали, досягають дуже високої точності виготовлення. Нафтові компанії випускають високоякісні бензини з миючими присадками.

Висновки. В результаті аналізу літературних джерел виділено найбільш значущі фактори, що впливають на технічний стан форсунок. Типовими дефектами та несправностями форсунок є обривання витків соленоїдів, міжвиткове замикання, руйнування конекторів, забруднення проточної частини форсунки, забруднення фільтрів, заклинювання клапана. Ці несправності приводять до погіршення екологічних та динамічних показників двигунів, а отже існує необхідність в проведенні достовірного діагностування ЕМФ при виконанні технічних обслуговувань та ремонтів.

Список літератури

1. Овчинников Г.В. Влияние загрязнения и износа элементов электромагнитных форсунок на характеристики автомобильного бензинового двигателя: Автореф. дис. канд. техн. наук: 05.04.02. Владимир, 2009. 18 с.
2. Красота М.В, Шепеленко И.В., Матвиенко А.А., М. Муташаир Аль Соодани Салем. Исследование влияния загрязнений электромагнитных форсунок на параметры бензиновых двигателей/Конструювання, виробництво та експлуатація сільськогосподарських машин. Загальнодержавний міжвідомчий науко-во-технічний збірник. , вип. 43, ч. II, - Кіровоград: КНТУ, 2013, с. 125-134.
3. Бакайкин Д. Д., Гриценко А. В. Результаты экспериментальных исследований пропускной способности бензиновых форсунок// Вестник КрасГАУ. – 2012. – № 12. – С. 120–127.
4. Вереютин А.Ю. Методика диагностирования систем топливоподачи двигателей с впрыскиванием бензина: сборник научных трудов / А. Ю. Вереютин. Рязань. : РВАИ, 2006. Вып . 16
5. Браильчук А.П. Виброакустический метод экспресс-диагностики форсунок впрыска легких топлив / А.П. Браильчук, А.А. Трифонов, Р.С. Санов // Вестн. ХНАДУ. – 2006. – Вып. 34–35. – С. 208–211.
6. Овчинников Г.В. Влияние загрязнения и износа элементов электромагнитных форсунок на характеристики автомобильного бензинового двигателя. Автореф. дис. канд. техн. наук/Овчинников Г. В. – Владимир, 2009. – 18 с.

УДК 504.062

Ю. Кулікова, магістр гр. ЕО-19МЗ
Л. Коломієць, доцент
Центральноукраїнський національний технічний університет

ОЦІНКА ВПЛИВУ МІСЦЬ ВИДАЛЕННЯ ВІДХОДІВ НА СТАН ОБ'ЄКТІВ ДОВКІЛЛЯ

Проаналізовано питання впливу місць видалення відходів на грунти, підземні води, повітря та запропоновано вирішення даної екологічної проблеми
місця видалення відходів, полігони ТПВ, сміття, грунти, девастація ландшафту, метаногенез, фільтрат

Актуальність. Актуальним є проведення оцінки впливу місць видалення відходів на об'єкти довкілля для розробки природоохоронних заходів в галузі. Визначення напрямків вдосконалення технологій переробки та утилізації дозволить зменшити обсяги утворення відходів, що є особливо важливим через переповнення існуючих місць видалення відходів та неможливість відводити все нові площі для таких цілей, адже це означає виведення з

користування зокрема сільськогосподарських угідь на тривалий час, девастацію агроландшафтів, погіршення стану водних ресурсів, грунтів та повітря.

Постановка проблеми. Внаслідок стрімкого збільшення чисельності населення, різноманітності виробничих процесів та використання природних ресурсів утворюється значна кількість відходів виробництв та побуту, різноманітних за морфологічним та хімічним складом, тривалістю розкладання в довкіллі, впливом на навколишнє середовище та здоров'я людини. Існуючі підходи в системі поводження з відходами в Україні не передбачають обов'язкової відповідальності тих, хто їх утворює, чи накопичує, за послідуючу переробку та повторне використання. Це призводить до переповнення сміттєзвалищ та полігонів понад проектні можливості, що, в свою чергу, спричиняє забрудненння повітря, водних ресурсів, грунтів, девастації ландшафтів [1-2].

Мета дослідження. Визначити причини зміни стану об'єктів довкілля, які виявляються в зоні впливу місця видалення відходів.

Завдання: - встановити ландшафтно-трансформуючі чинники полігону ТПВ;

- вивчити вплив забруднюючих речовин, що утворюються в умовах смітєєзвалищ, на людей та об'єкти довкілля;

- виявити міграцію хімічних забруднень із тіла звалища в об'єкти довкілля;

- запропонувати заходи для зниження негативного впливу звалища.

Об'єкт дослідження: Вплив полігонів ТПВ на стан об'єктів довкілля.

Предмет дослідження: Зміни властивостей гідрографічної мережі та едафотопів територій, що прилягають до полігону ТПВ.

Результати досліджень.

В тілі звалища внаслідок особливостей морфологічного складу та умов зберігання відходів постійно утворюється фільтрат. На практиці система збору та відведення фільтрату на сміттєзвалищах в більшості випадків майже відсутня, тому негативний ефект від утворення даної субстанції з роками лише посилюється. Фільтрат просочується в підгрунтові та підземні води, мігрує до грунтів прилеглих територій. Внаслідок цього відбувається стійке забруднення всіх об'єктів довкілля, зі зміною умов господарського використання територій.

Для оцінювання екологічного і санітарно-гігієнічного стану вод було відібрано проби з криниці місцевого населення, та із моніторингової свердловини. В результаті відібраних проб на прилягаючих територіях та сміттєзвалищі виявлено перевищення деяких ГДК (табл. 1).

Таблиця 1 – Результати відбору проб води з криниці приватного сектора, що знаходиться за 200 м від звалища

№ п/п	Назва показника	Розмірність	ГДК	Результат
1	Запах при 20 С	бали	до 2	0
2	Прозорість	см	більше 20	більше 40
3	Водневий показник (pH)	од. pH	6,5-8,5	6,8
4	Завислі речовини	мг/дм^3	не норм.	3,9
5	Сухий залишок	мг/дм^3	до 1000	979
6	Жорсткість загальна	мг-екв/дм^3	до 7,0	10,9
7	Жорсткість карбонатна	мг-екв/дм^3	до 6,5	7,1
8	Гідрокарбонати (HCO_3^-	мг/дм^3	до 300	417
9	Хлориди (Cl$^-$)	мг/дм^3	до 250	193,6
10	Сульфати (SO_4^{2})	мг/дм^3	до 500	180,1
11	Нітрити (NO_2^-)	мг/дм^3	до 3,3	0,0
12	нітрати (NO_3^-)	мг/дм^3	до 45	35,7
13	Фосфати	мг/дм^3	не норм.	0,0

14	Амоній сольовий	мг/дм^3	до 2,0	0,9
15	Залізо загальне	мг/дм^3	до 0,3	0,31
16	Кальцій	мг/дм^3	не норм.	158,6
17	Магній	мг/дм^3	до 80	38,9

Окремі показники перевищують норми ГДК: прозорість, завислі речовини, жорсткість загальна, жорсткість карбонатна, гідрокарбонати, фосфати, залізо загальне, кальцій. Це пояснюється вертикальною та горизонтальною міграцією забруднень, стійкістю їх в довкіллі.

Хімічний аналіз фільтратів, проведений багатьма дослідниками, показує, що вони містять важкі метали, феноли, нафтопродукти, сірководень та інші сполуки в концентраціях, вищих за гранично допустимі норми. Цю тенденцію спостерігаємо і в межах нашого об'єкта досліджень. Джерелом забруднення фільтрату в основному є розкладання маси харчових відходів і окислювання металів, так як процес розпаду складних органічних речовин відбувається вкрай повільно. Виявлено, що фільтрат утворюється на ділянці захоронення відходів протягом всього року.

Негативний вплив звалищних фільтратів на довкілля проявляється в:

-інтенсивному вивільненні фільтратів на денну поверхню в підніжжі звалищного тіла;

-підтоплення і забруднення прилягаючих ділянок місцевості, які прилягають до основи звалища;

-забруднення гудронового середовища і зони аерації в межах полігону ТПВ і поблизу;

-зараження ґрунтових вод та значне зниження якості природних джерел питної води в районі експлуатації полігону ТПВ.

Для оцінювання показників фільтратів проаналізовано чотири відібраних проби у чотирьох різних місцях на території сміттєзвалища та подано середнє значення. Дані лабораторних досліджень фільтрату, що накопичується біля підніжжя сміттєзвалища показали, що він є водним розчином складного хімічного складу, який зумовлює екологічний стан поверхневих і підземних вод. Рідина темно-коричневого кольору, виділяє різкий неприємний запах, має високий вміст органіки (БСК5 – 155 мгО/дм3), нітратів (58,5 мг/дм3), хлору (1554 мг/дм3), а також украй незадовільний санітарно-мікробіологічний стан (табл. 2).

Більшість досліджуваних показників (амонійний азот, фосфати, нітрати, ХСК та ін.) мали перевищення ГДК, прийнятих для фільтратів звалищ.

Таблиця 2 – Показники проб фільтрату сміттєзвалища

№ п/п	Назва показника	Розмірність	Результат	ГДК
1	Запах при 20 С	бали	2,0	2
2	Прозорість	см	6	не норм.
3	Водневий показник (pH)	од. pH	5,9	6,5-9,0
4	Завислі речовини	мг/дм^3	168	380
5	Сухий залишок	мг/дм^3	12560	1000
6	Мінеральний залишок	мг/дм^3	7260	не норм.
7	Твердість загальна	мг-екв/дм^3	118,0	не норм.
8	Твердість карбонатна	мг-екв/дм^3	84,3	не норм.
9	Гідрокарбонати (HCO_3^-)	мг/дм^3	5142	не норм.
10	Хлориди (Cl^-)	мг/дм^3	1554	350
11	Сульфати (SO_4^{2})	мг/дм^3	995	500
12	Нітрити (NO_2^-)	мг/дм^3	13,6	3,3
13	нітрати (NO_3^-)	мг/дм^3	58,5	45

14	Фосфати	мг/дм^3	15,8	10
15	Амоній сольовий	мг/дм^3	113,5	38
16	Азот амонійний	мг/дм^3	92,5	30
17	Залізо загальне	мг/дм^3	75,8	2,5
18	ХСК	мгО/дм^3	165	81
19	БСК $_5$	мгО/дм^3	140	32
20	Нафтопродукти	мг/дм^3	0,85	10

Потрапляння у природні води фільтрату недопустиме, оскільки ГДК ХСК у прісних водах, зокрема рибогосподарського призначення, становить 50,0 мг/л О2, а БСК5 – 3,0 мг/л О2. Незважаючи на потужну самоочисну властивість біосфери, в місці скиду такого фільтрату сформується стійка зона токсикації водойми.

Оскільки полігон постійно заповнюється, то розпад органічних речовин в анаеробних умовах (включаючи фазу нестійкого утворення метану) протікає від декількох місяців до декількох років після депонування. Фільтрат, що утворюється в таких умовах розкладання ТПВ, характеризується значенням pH 5,9, високим значенням БСК (140 мг/дм3 О2), високим відношенням БСК/ХСК (0,8), високим вмістом амонійного азоту та заліза (92,5 та 72,8 мг/дм3).

Фільтраційні води полігонів ТПВ представляють серйозну екологічну небезпеку для довкілля (ґрунтові води, ґрунт, повітря) і здоров'я населення, спричиняючи алергії, астму, порушення ендокринної системи та ін. Великі кількості органічних кислот створюють достатні умови для існування всіх металів, здатних до комплексоутворення з органічними кислотами в формах різнозарядних комплексних сполук. Ймовірно, переважною формою присутності берилію, магнію, кальцію, стронцію, барію і хрому є катіонні комплекси, а міді, кадмію, ртуті свинцю, талію та ітрію – аніонні; для літію, алюмінію, титанів, ванадію, марганцю, заліза, нікелю, кобальту, цинку, цирконію та срібла – нейтральні комплексні сполуки. Показники БСК і ХСК фільтрату в десятки разів можуть перевищувати ці показники для звичайних стічних вод госппобутової каналізації.

Забруднення гідрографічної мережі за рахунок діяльності полігона постійно зростає, зважаючи на неможливість поки що припинити його заповнення, місто є на грані екологічної кризи [2-4].

Після проведення польового агрохімічного обстеження земель сільськогосподарського призначення, відбору зразків та лабораторного дослідження, порівняли отримані результати на ступінь забезпеченості ґрунтів на кислотність, вміст гумусу, мікроелементів та макроелементів: азоту, фосфору, калію, бору, марганцю, цинку. Також за отриманими результатами з'ясували, до якої групи відносяться землі за еколого-агрономічним станом.

Вміст гумусу на ґрунтах, становить - 3,2%, а це IV-а група – підвищений ступінь забезпечення.

Показник вмісту азоту, середній показник вмісту азоту в земельній ділянці становить – 158 мг/кг. Тому ступінь забезпеченості даним елементом – середня (III-га агрохімічна група).

Середній показник вмісту фосфору на даних ґрунтах становить - 105,8 мг/кг. Ступінь даного елемента рівна IV-тій агрохімічній групі (підвищена забезпеченість). Наступним показником для моніторингу ґрунтів є середній показник вмісту калію на даних господарських ділянках, він становить – 138,9 мг/кг, тому ступінь забезпеченості високий (V-та агрохімічна група).

Ступінь кислотності грунтів становить – 7,9. Більшість рослин потребують нейтральної реакції ґрунту.

Грунти області є родючі та цінні. Поруч зі сміттєзвалищем розташовані земельні угіддя місцевого сільського господарства. Кожної весни та осені майже все поле

виявляється вкрите шаром паперу та целофану, інших відходів, які розносяться сильним вітром та тваринами. Під час обробки землі техніка перемішує все сміття з ґрунтом.

В результаті проведеного аналізу виявлено, що основним джерелом забруднення ґрунту є фільтратні стоки полігону, які накопичуються у ґрунтах, та внаслідок значних атмосферних опадів, що викликають розмивання фільтрату, потрапляють у об'єкти довкілля.

На звалищах, споруджених без дотримання правил охорони довкілля (які не мають протифільтраційного екрану, системи відводу й очищення фільтрату), фільтрат вільно стікає по формах рельєфу, потрапляє у грунт, далі у ґрунтові і підземні води, що призводить до значного забруднення довкілля не тільки шкідливими органічними і неорганічними сполуками, але і яйцями гельмінтів, біологічними отрутами [ ].

Проби ґрунтів для оцінки їхнього екологічного стану відбирали на полі, розташованому за 100 м від полігону, в орному шарі грунту. Результати показали, що грунти є значно порушеними та їх використання за призначенням неможливе, оскільки отримана продукція з цих посівів загрожує здоров'ю людей. Вміст свинцю при ГДК 32 мг/кг складає в грунті 485 мг/кг. Аналогічно і по вмісту інших забруднювачів є різке перевищення (табл. 3).

Таблиця 3 – Хімічний аналіз грунтів агроландшафту поряд із полігоном твердих побутових відходів

	Показник	Методика вимірювання	Одиниці вимірювання	Вміст
1	pH водн.	ГОСТ 26423-85	-	7,9
2	Сульфатів	ГОСТ 26490-85	ммоль/100 г	0,7
3	Хлоридів (Cl^-)	ГОСТ 26428-85	ммоль/100 г	0,2
4	Загальний вмст солей (TDS)	ГОСТ 26423-85	ppm	868
5	Вміст гумусу	ГОСТ 23740-79	%	3,2
	Рухомих форм (Елементів живлення рослин)			
6	Вміст азоту	ДСТУ 7863:2015	мг/кг	158,1
7	Вміст P_2O_5	ГОСТ 26204-91	мг/кг	105,8
8	Вміст K_2O	ГОСТ 26204-91	мг/кг	138,9
9	Вміст Ca^{2+} обм .	ГОСТ 264877-85	ммоль/100 г	47,6
10	Вміст Mg^{2+} обм.	ГОСТ 264877-85	ммоль/100 г	1,85
11	Молібден (Mo)	ГОСТ Р 50685-94	мг/кг	4,1
12	Марганець (Mn)	ГОСТ Р 50685-94	мг/кг	120,0
13	Мідь (Cu)	ГОСТ Р 50683-94)	мг/кг	1,2
14	Цинк (Zn)	ГОСТ Р 50686-94	мг/кг	28,6
15	Кобальт (Co)	ГОСТ Р 50683-94	мг/кг	6,11
	Валовий вміст			
16	Свинець (Pb)	ГОСТ Р 50684-94	мг/кг	485
17	Хром (Cr)	ГОСТ 27593-88	мг/кг	19
18	Кобальт (Co)	ГОСТ Р 50683-94	мг/кг	45
19	Нікель (Ni)	ГОСТ 13047.1-81	мг/кг	89
20	Мідь (Cu)	ГОСТ Р 50683-94	мг/кг	67
21	Цинк (Zn)	ГОСТ Р 50686-94	мг/кг	693

На фоні хімічного навантаження зростає епідемічна небезпека грунту. В забрудненому грунті на фоні зменшення істинних представників грунтових мікробоценозів (антагоністів патогенної кишкової мікрофлори) і зниження її біологічної активності відзначається

збільшення кількості патогенних ентеробактерій, ентеровірусів і геогельмінтів, які виявилися більш стійкими до хімічного забруднення грунту, ніж представники природних грунтових мікроценозів. Як свідчать дані таблиці 4, є перевищення концентрації свинцю в грунті в 15 разів порівняно з санітарно-гігієнічними нормативами, нікелю – в 21 разів, цинку – в 30.

Таблиця 4 – ГДК важких металів, мг/кг та їх фактичний вміст в грунті

№ п/п	Показник	ГДК, мг/кг	Вміст, мг/кг	Перевищення ГДК, разів
1	Свинець (Pb)	32	485	15,2
2	Хром (Cr)	6	19	3,2
3	Кобальт (Co)	5	45	9
4	Нікель (Ni)	4	87	21,2
5	Мідь (Cu)	3	67	22,3
6	Цинк (Zn)	23	693	30,1

Оцінка несприятливих наслідків забруднення грунту при їх безпосередній дії на організм людини важлива для випадків геофагії у дітей, які проживають на таких територіях. Така оцінка розроблена за найбільш поширеною в населених пунктах ЗР – свинцем, вміст якого у грунті, зазвичай, супроводжується збільшенням вмісту інших елементів. При вмісту свинцю в грунті ігрових майданчиків на рівні 500 мг/кг і систематичного знаходження його в грунті, слід очікувати змін психоневрологічного статусу у дітей.

За даними вивчення розподілу в грунті деяких металів, найбільш поширених індикаторів забруднення міст, може бути складена орієнтовна оцінка небезпеки забруднення атмосферного повітря. Так, при вмісті свинцю в грунті, починаючи з 250 мг/кг, в районі діючих джерел забруднення спостерігається збільшення його ГДК в атмосферному повітрі (0,3 мкг/м3), при вмісті міді в грунті, починаючи з 1500 мг/кг, спостерігається перевищення ГДК її в атмосферному повітрі (2,0 мкг/м3).

Небезпека забруднених сільськогосподарських грунтів обумовлена тим, що: 1) з продуктами харчування в організм людини поступає в середньому 70% шкідливих речовин; 2)рівень транслокації визначає рівень накопичення токсикантів в продуктах харчування, впливає на їх якість.

Тому оцінку хімічного забруднення грунтів як індикаторів несприятливого впливу на здоров'я населення виконують за показниками, розробленими за спорідненими геохімічними та геогігієнічними дослідженнями довкілля [2,4-6].

Висновок. Результати досліджень об'єктів довкілля, що піддаються прямому та непрямому впливу полігонів, показали передбачуване значне перевищення вмісту хімічних елементів у грунті, оскільки під їх впливом відбувається забруднення грунту продуктами вилуговування, виділення різкого неприємного запаху, метаногенез та девастація. Це робить неможливим ведення сільського господарювання на все більш обширних площах угідь, межуючих зі звалищами. Так як з ряду причин неможливо змінити ситуацію щодо місця накопичення відходів, необхідно для збереження стану об'єктів довкілля та господарювання терміново провести еколого-технологічну реконструкцію полігону ТПВ та економічно обгрунтовані заходів з фітомеліорації, збору та очистки фільтрату, рекультивації і т.п.

Список літератури

1. Душкін С. С. Конспект лекцій з дисципліни «Технологія утилізації твердих побутових відходів» (для студентів 2, 5 курсів денної і заочної форм навчання за напрямом підготовки 6.060103 «Гідротехніка (Водні ресурси)» та слухачів другої вищої освіти спеціальності 7.092601 (7.06010808) «Водопостачання та водовідведення») / С. С. Душкін, М. В. Дегтяр; Харк. нац. акад. міськ. госп-ва. – Х.: ХНАМГ, 2011. – 86 с.
2. Мальований М. Аналіз екологічної небезпеки існуючих сміттєзвалищ та стратегія її мінімізації (на прикладі Грибовицького сміттєзвалища) / М.Мальований, В.Слюсар, А.Середа та інш.//Екологічна безпека та

збалансоване ресурсокористування . - № 1 (15). – 2017. - С.5-11.
3. Гайдін А.М. Хімічний склад фільтрату Львівського полігону твердих побутових відходів / А.М. Гайдін, В.О. Дяків, В.Д. Погребенник, А.В. Пашук // Природа Західного Полісся та прилеглих територій: зб. наук. пр. / Волин. нац. ун-т ім. Лесі Українки; [редкол.: Ф.В. Зузук та ін.]. – Луцьк, 2013. – № 10. – С. 43–49.
4. Управління та поводження з відходами. Частина 3. Полігони твердих побутових відходів: навчальний посібник /Петрук В. Г., Васильківський І. В., Іщенко В. А., Петрук Р.В. –Вінниця: ВНТУ, 2016. –137с.
5. Студінський В.А. Управління твердими побутовими відходами в містах України –К.: Видавництво «КІМО», 2006. –152 с.
6. Попович В. В. Фізико-механічні властивості едафотопів довкола техногенних водойм сміттєзвалищ та полігонів твердих побутових відходів у межах Західного Лісостепу України / В. В. Попович // Науковий вісник НЛТУ України: зб. наук.-техн. праць. – Львів: РВВ НЛТУ України. – 2012. – Вип. 22.14. – С. 106-110.

УДК 504.3.054

В. Куліш, магістр гр. ЕО-19М
С. Мартиненко, доцент
Центральноукраїнський національний технічний університет

ПОРІВНЯЛЬНА ЕКОНОМІЧНА ОЦІНКА МЕТОДУ ЛІХЕНОІНДИКАЦІЇ ТА ХІМІЧНО-ЛАБОРАТОРНОГО МЕТОДУ ДОСЛІДЖЕННЯ ЗАБРУДНЕННЯ АТМОСФЕРНОГО ПОВІТРЯ ВІД АВТОМОБІЛЬНОГО ТРАНСПОРТУ

Проаналізовано питання необхідності розвитку визначення стану забруднення атмосферного повітря методом ліхеноіндикації, який дозволить скоротити витрати на хімічно-лабораторні методи дослідження.
ліхеноіндикація, забруднення атмосферного повітря, моніторинг, автотранспорт

Відповідно, з розвитком міст кількість автомобільного транспорту також збільшується, цьому сприяє збільшення протяжності і розгалуженості автомобільної мережі доріг, а також висока завантаженість доріг поряд з постійним рухом все більшої кількості транспортних засобів. Велика протяжність і продуктивність автомобільних доріг дозволяє організувати місцеві автомобільні перевезення і високу швидкість доставки вантажів в будь-яку точку міста. У той же час дорожньо-транспортні мережі мають ряд негативних факторів, пов'язаних з деградацією навколишнього середовища. Істотний вплив автотранспорт складає на атмосферне повітря, яке забруднюється вихлопними газами двигунів, що містять складну суміш компонентів і забруднюючих речовин, у тому числі канцерогенних.

Актуальність. Забруднення повітря в міських районах часто є серйозною екологічною проблемою і тому вимагає постійного моніторингу та контролю. В Україні основну роботу з моніторингу стану атмосферного повітря здійснюють регіональні підрозділи Гідрометцентру, які підтримують функціонування стаціонарних постів моніторингу вмісту забруднюючих речовин. Крім того, окремі періодичні обстеження проводяться установами Міністерства енергетики та захисту довкілля України, Держпродспоживслужби, та ДСНС. Тому впровадження ліхеноіндикаційної системи моніторингу за станом атмосферного повітря в місті, як альтернатива стаціонарним постам спостереження є досить нагальним питанням.

Мета дослідження: провести розрахунок витрат на проведення моніторингу забруднення атмосферного повітря автотранспортом хімічно-лабораторним методом і

методом ліхеноіндикації, і на основі цих даних зробити висновок про економічну доцільність застосування методу ліхеноіндикації.

Завдання:

– провести вивчення та аналіз відомих джерел з проблеми впливу автомобільного транспорту на стан атмосферного повітря і методів визначення цього впливу;

– провести розрахунок витрат на проведення моніторингу забруднення атмосферного повітря автотранспортом хімічно-лабораторним методом і методом ліхеноіндикації;

– запропонувати схему можливих маршрутів дослідження стану забруднення атмосферного повітря ліхеноіндикаційним методом;

– зробити висновок про економічну доцільність застосування методу ліхеноіндикації.

Об'єкт дослідження: економічний ефект від запровадження нового методу контролю за станом атмосферного повітря.

Предмет дослідження: ліхеноіндикаційний метод дослідження стану забруднення атмосферного повітря, як аналог хімічно-лабораторним методам.

Результати досліджень.

Основним джерелом забруднення атмосферного повітря в місті Кропивницький (50%) є автомобільний транспорт. Наукові дослідники встановили, що вітчизняні автомобілі екологічно "брудніші" західних моделей. Однак ні для кого не секрет, що багато іномарки мають зношені двигуни і тому сильно забруднюють повітря. До сьогодні в якості палива використовується в основному вкрай шкідливий бензин, компонентом якого є свинець. Зазвичай автомобільні двигуни погано відрегульовані, тому їх газові викиди містять значну кількість вуглекислого газу, сажі.

Ситуація ускладнюється ще й тим, що автомобільні викиди концентруються в поверхневому шарі повітря, а саме в дихальній зоні людини. Для нормального життя організми потребують чистого повітря. У містах, де забруднення повітря досить значне, його прозорість помітно знижується. Відомо, що вміст в атмосферному повітрі становить: N_2 – 78,1%; O_2 – 20,9%; Ar – 0,95%; CO_2 – 0,032%. Антропотоксини — це газоподібні речовини, які є продуктами життєдіяльності людини. Одним зі сприятливих умов для їх утворення вважається наявність вуглекислого газу. Перевищення кількості вуглекислого газу над нормативними значеннями призводить до їх надмірного утворення. Тому вуглекислий газ є відносним показником ступеня чистоти повітря, в якому знаходиться людина. Вміст вуглекислого газу в атмосфері впливає на інтенсивність і спектр сонячного випромінювання, що досягає поверхні землі. Збільшення його кількості створює "парниковий ефект", викликає потепління клімату. Це також пов'язано з поширенням онкологічних захворювань [1].

Таким чином, розвиток цивілізації супроводжується значними змінами в стані природного середовища. Зокрема, автомобільний транспорт справедливо вважається одним з факторів, що негативно впливають на якість повітряного середовища. З цієї точки зору варто розглянути проблему використання (можливо, заміни) палива, масел та інших матеріалів, виконання проектно-пошукових робіт, вдосконалення системи управління автомобілем і т.д. важливо, щоб всі пошукові операції обов'язково будувалися на екологічній основі.

У Кропивницькому є три стаціонарних спостережних пункти, які дають досить великий обсяг інформації про стан атмосферного повітря, але їх просторове розташування, а також обмежений перелік досліджуваних домішок не дають повної картини забруднення атмосфери. На всіх трьох постах визначено обмежений перелік речовин-діоксид і оксид азоту, фенол і формальдегід, діоксид сірки, пил і окис вуглецю. Серед них перевищення гранично допустимих концентрацій спостерігається по діоксиду азоту, фенолу і формальдегіду. Вміст важких металів періодично контролюється тільки на 1 посту-на вулиці. Андріївської, 89, тому отримані значення їх концентрацій не можуть представляти стан повітря у всьому місті [2,3].

На стан атмосферного повітря впливають як природні, так і антропогенні чинники. Серед природних в першу чергу виділимо кліматичні фактори. Серед антропогенних чинників – промисловість, житлово-комунальне господарство і транспорт. Однак найбільший внесок в сумарне забруднення атмосфери міста чинить автотранспорт, а вплив окремих великих підприємств та котелень відчутний переважно локально, в ареалі їх розташування [4].

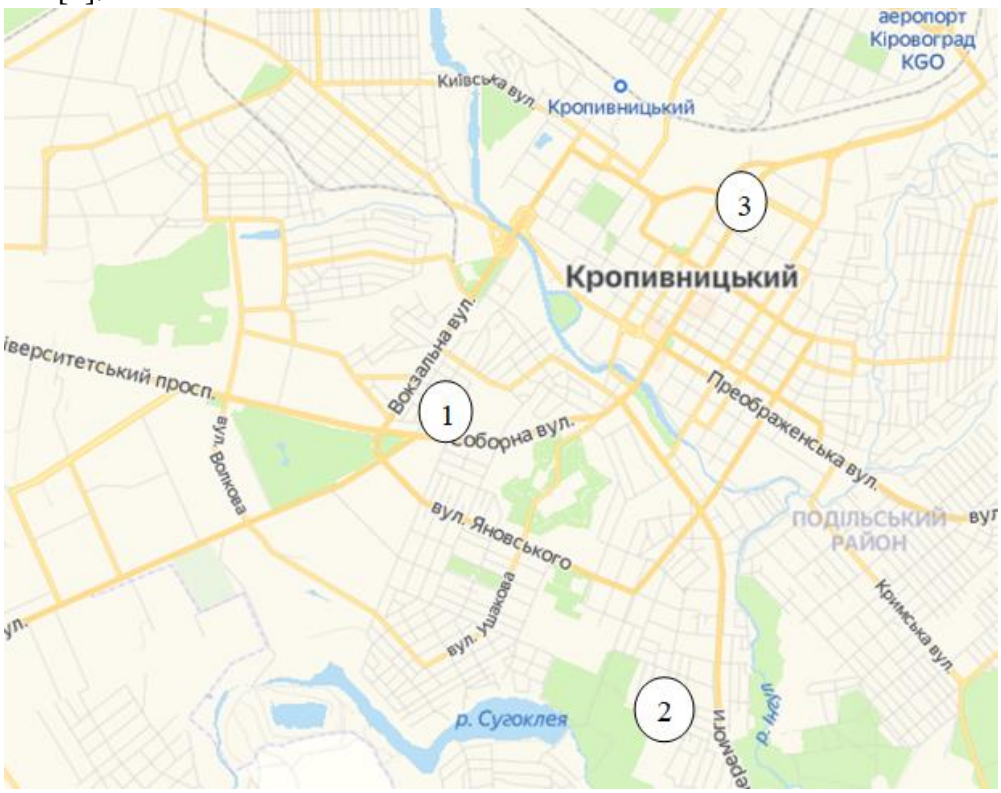


Рис.1. Схема розміщення стаціонарних пунктів спостережень в м.Кропивницький

На рис. 1 бачимо сучасну схему розміщення стаціонарних пунктів спостережень за станом повітря в м.Кропивницький. Пост №1 розташований на вул. Андріївська, пост №2 – на вул. Пугачова, №3 – на вул. В'ячеслава Чорновола. Як бачимо, постами охоплена тільки центральна частина міста, на окраєні міста зовсім немає стаціонарних пунктів, а саме там знаходяться найбільші промислові підприємства міста. Також у зону спостережень не потрапляють великі зони житлової забудови у цих районах. Крім того, лише пост №3 фактично співпадає із одним із ареалів найбільшого автотранспортного забруднення, а решта - не охоплені [5].

В цілому варто відзначити, що існуюча мережа моніторингу стану повітря в Кропивницькому потребує вдосконалення. Для цього пропонуємо: розширити мережу стаціонарних спостережних пунктів, розширити перелік досліджуваних речовин; автоматизувати визначення основних домішок, організувати маршрутні спостереження за станом повітря за допомогою пересувної лабораторії, а головне – застосувати метод ліхеноіндикації.

Практично всі ці види діяльності вимагають значних капітальних вкладень і поточних витрат. Пропонуємо розрахувати загальну вартість установки як мінімум 2 додаткових стаціонарних постів і однієї пересувної лабораторії в нашому місті.

Для вдосконалення традиційної системи екологічного моніторингу атмосферного повітря в місті необхідно встановити нові вимірювальні комплекси (наприклад, такі, як в додатку В). Капітальні витрати включають, перш за все, придбання комплекту обладнання для аналізу газових сумішей для стаціонарних і пересувних постів. Поточні пропозиції на українському ринку по обладнанню стаціонарних спостережних пунктів в основному пропонують комплектацію-металевий павільйон, метеорологічне обладнання

(анеморумбографи, датчики температури і вологості), електричне та інформаційне обладнання, а також власне газоаналізаторне обладнання (аспіратори, газоаналізатори, пилососи). Ціна такого комплекту становить близько 1 мільйона гривень. Ціна аналогічного зарубіжного комплексу Airpointer починається від 35 тисяч євро. Саме газоаналізаторне обладнання становить менше 60% від цієї суми, тому його покомпонентна покупка може бути більш вигідною. З іншого боку, в цьому випадку доведеться відмовитися від автоматизації, і, відповідно, витрачати гроші на зарплати спостерігачам-операторам і лаборантам. Але навіть якщо обмежитися більш простим обладнанням, яке забезпечувало б аналіз затвердженого переліку домішок (оксидів азоту, вуглецю, сірки, фенолу і формальдегіду), а також окремих важких металів і аерозолів, витрати на вдосконалення системи [6,7].

Наприклад, капітальні затрати складуть:

- придбання двох установок MDGC, по 218 540 грн. кожна – в сумі 437 080 грн.;
- 2 газоаналізатори ОКМТ-2-х кан., вимірювач токсичних газів (CO,H2,S ,SO_2, Cl_2) - по 35 800 грн. = 71 600 грн.;
- аналізатор АНТ-3, вимірювач концентрацій парів токсичних речовин (до 40 газів) – 64 815 грн.
- автотрасовий газоаналізатор 603 X01M – 55000 грн.
- аерозольний фільтр SteamJetAerosolCollector - 31700 грн.

Разом величина таких затрат (К) становитиме: 218 540·2 + 71600 + 74815 + 55 000 + 31 700 = 670 195 грн.

Поточні затрати складатимуть заробітна плата операторів, лаборантів, а також електроенергія. Ці величини зведені в таблиці 1.

Таблиця 1 - Поточні затрати утримання станції

Стаття витрат	Вартість, грн
Річна заробітна плата 2 операторів	56400
Річна заробітна плата 2 лаборантів	44 800
Електроенергія (3 кВт в день з 4 постів = 4380 кВт за рік)	7 358
Пальне для пересувної лабораторії (10л за маршрут, 36 виїздів на рік, по 25 грн./л)	10 620
Разом	119 178

Таким чином, технічне вдосконалення існуючої мережі моніторингу повітря потребує майже 0,7 млн. гривень капітальних вкладень та біля 120 тис.грн наступних щорічних витрат. Очевидно, що такі суми на моніторинг навряд чи можуть бути виділені з міського бюджету найближчим часом.

Оцінка витрат на моніторинг повітря засобами ліхеноіндикації

Для проведення класичної «пасивної» ліхеноіндикації в місті потрібне періодичне обстеження усіх мікрорайонів міста, вздовж найжвавіших доріг, а також у паркових зонах з метою моніторингу показників. Для цього було розроблено спеціальні маршрути, які дозволяють оптимально досліджувати максимальну кількість дерев за короткий проміжок часу (рис. 2). У таблиці 2 наведено деякі кількісні характеристики, потрібні для подальших розрахунків.

Таблиця 2 - Пропоновані маршрути обстежень

№	Колір маршуту обстеження	Загальна довжина, км	Оцінка потреб часу, год
1	Червоний	13	7,5
2	Чорний	24	11
3	Зелений	14	7
4	Синій	20	9
5	Голубий	3	1,5
Всього		64	36

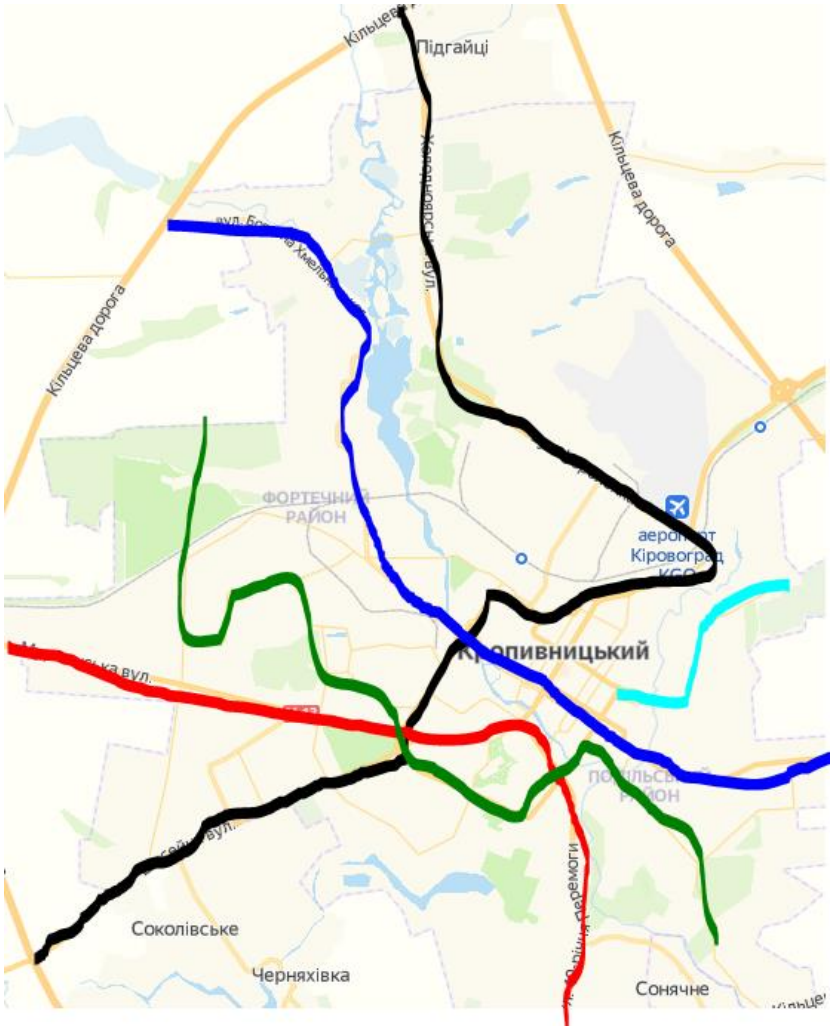


Рис. 2. Пропонована схема маршрутних ліхеноіндикаційних досліджень

Така конфігурація маршутів дозволяє оцінити стан забруднення атмосферного повітря вздовж основних автомобільних доріг міста. Загальна протяжність пропонованих маршрутів складає 64 км. Потрібний час розрахований, виходячи із власного досвіду проведення досліджень. Маючи навички, обстеження одного дерева займає менше 3 хвилин. Також приблизно враховано час на пересування та зупинки на маршруті.

Автомобільний маршрут є оптимальним по часу та можливості обстеження у віддалених мікрорайонах. Затрати, необхідні на його реалізацію визначаємо за формулою:

F=(L×(e/100)0×C [8,9], де

F – кількість коштів, затрачених на пальне;

L – загальна довжина маршрутів, км;

e– кількість літрів палива, що витрачає автомобіль на 100 км пробігу;

C – вартість пального за 1 літр, грн.

Протяжність маршрутів 64 км, витрата пального – 9 літрів/100 км (з врахуванням міського циклу, частих зупинок), середня ціна 1 л пального у жовтні 2020 року – 25 грн.

Відповідно:

$F = (64{,}0 \times 9{,}0/100)) \times 25 = 144$ грн.

Крім цього, оцінено затрати часу на проведення дослідження. Як зазначалось у таблиці 2, сумарні затрати часу на маршрутні обстеження – 36 годин. Втім, потрібно врахувати, що цей час затрачається двома працівниками – водієм та власне дослідником (лаборантом).

Крім того, після польових досліджень потрібна аналітична обробка отриманих даних кваліфікованим персоналом. Сумарні затрати на оплату праці персоналу представлені у таблиці 3[10].

Таблиця 3 - Оплата праці персоналу

Вид робіт	Персонал	Оплата праці, грн./годину	Затрачений час, годин	Нараховані кошти, грн.
маршрутні обстеження	водій	30,48	28,5	868,6
	лаборант	34,51	28,5	983,6
геопросторовий аналіз результатів	еколог	39,02	14	546,3
складання цифрових карт якості повітря	Інженер-картограф	44,14	10	441,4
Всього			81	2839,9

Всього на оплату праці при запропонованому дослідженні потрібно 2840 грн. З врахуванням вартості пального для маршрутних обстежень, загалом затрати складуть: 2840+144=2984 грн. Періодичність таких обстежень: 1 раз на рік (через повільний ріст лишайників – 1-4 мм/рік), проте вони дадуть адекватну усереднену картину забруднення повітря.

Таким чином, якщо навіть не враховувати витрати на побудову нових станцій досліджень, а взяти тільки витрати на рік на їх утримання і на проведення методу ліхеноіндикації. То метод ліхеноіндекації в 40 разів дешевше, ніж лабораторні дослідження. Економія в рік: 120000-2984=117016 грн. Але недоліком є те, що результати дослідження стану атмосферного повітря в лабораторії набагато точніші, ніж результати які отримуємо завдяки методу ліхеноіндикації.

Висновок. Метод ліхеноіндикації – це доступний, ефективний та недорогий спосіб оцінки екологічного стану атмосферного повітря в містах та промислових зонах, здійснювати її можуть учні чи студенти. Провівши необхідні економічні розрахунки та обгрунтування, ми оцінили високу доцільність та економічну ефективність впровадження систем пасивно ліхеноіндикації для екологічного моніторингу стану атмосфери у місті. Сумарні витрати на систему біоіндикаційного моніторингу суттєво нижчі за вартість навіть одного нового пункту інструментального контролю якості повітря.

Список літератури

1. Адаменко О. М. Екологія міста Івано - Франківська / Адаменко О. М., Крижанівський Є.І., Нейко Є.М., Русанов Г.Г., Журавель О. М., Міщенко Л.В., Кольцова Н.І. – Івано-Франківськ: «Сіверсія МВ», 2014.– 200 с.
2. Ашихміна Т. Я. та ін. Біоіндикація та біотестування - методи пізнання екологічного стану навколишнього середовища / Ашихміна Т. Я. // – К: Знання, 2015. – 450 с.
3. Бязров Л. Г. Трансплантація лишайників як метод ліхеноіндикації /Л. Г. Бязров // [Електронний ресурс]. – Режим доступу: bio.1 september. ru/article.php?1D=2002022107.
4. Экологический мониторинг: Учебно - методическое пособие. Изд. 3-е / Под. ред. Т.Я. Амихминой. - М.,

2016.
5. Мерленко І.М., Музиченко О.С.. Моніторинг довкілля. Лабораторний практикум до виконання занять для студентів спеціальності 6.070800 – «Екологія та охорона навколишнього середовища» денної та заочної форми навчання / І.М. Мерленко, О.С. Музиченко – Луцьк, 2017. – 176 с.
6. Моніторинг довкілля: Підручник / М.О. Клименко, А.М. Прищепа, Н.М. Вознюк. – К., 2016. – 234 с.
7. Кондратюк С.Я. Ліхеноіндикація: С. Я. Кондратюк, В. Г. Мартиненко, Л. В. Димитрова, Н. М. Корнелюк – К.; Кіровоград: ТОВ «КОД». – 2016. – 260 с.
8. Кравчук С.С., Романюк М.В. Ліхеноіндикація стану забруднення оточуючого середовища у м. Могилеві-Подільському та його околицях [Електронний ресурс] – Режим доступу: //www.lib.ua-ru.net/diss/cont/150403.html.
9. Курс низших растений : учебник для студентов ун-тов /Л.Л. Великанов, Л.В. Гарибова, Н.П. Горбунова, М.В. Горленко и др. – М.: Высшая школа,1998. – 504 с.
10. Кудовин А.С., Бязров Л.Г. Трансплантація лишайників як метод ліхеноіндикації [Електронний ресурс] – Режим доступу: // bio.1 september. ru/article.php?1D=2002022107.

УДК 621.431.3

А. Мурзагалієв, магістр гр. АТ 19МЗ
Центральноукраїнський національний технічний університет

ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ВІДНОВЛЕННЯ АВТОМОБІЛЬНИХ ДЕТАЛЕЙ ПЛАЗМОВИМ НАПЛАВЛЕННЯМ

В роботі визначено основні напрямки підвищення ефективності плазмового наплавлення. Плазмове наплавлення є ефективним способом відновлення деталей автомобілів. Встановлено, що додавання елементів-активаторів з різко відмінними параметрами електро- і теплопровідності, а також їх специфічні властивості активують процес отримання необхідних властивостей металопокриттів.
плазмове наплавлення, відновлення, порошковий матеріал

Постановка проблеми. Одним із основних напрямків підвищення довговічності та ресурсу автомобільного транспорту в сучасних умовах є вдосконалення економічних технологічних процесів відновлення деталей вузлів та агрегатів у поєднанні з використанням доступних і дешевих матеріалів при гарантованих високих показниках надійності відремонтованих виробів.

Вирішення цієї задачі стримується обмеженим використанням сучасних способів ремонту та відновлення деталей автомобільної техніки, основними з яких є деталі типу «вал». Різноманітність діючих сил і умов експлуатації цих деталей визначає великі розбіжності у значеннях зносу їх робочих поверхонь, на ремонт яких припадає 60 % існуючих технологічних процесів відновлення, серед яких найбільш перспективним є плазмові методи нанесення захисних шарів.

Останнім часом широко застосовується плазмове наплавлення порошковими сумішами з активуюючими добавками, що дозволяє отримати наплавлений шар із заданими фізико-механічними властивостями.

Аналіз останніх досліджень та публікацій. Вибором ефективних методів відновлення деталей почали займатися з появою промислових видів ремонту. Значний внесок у вирішенні цих питань внесли провідні фахівці в галузі ремонту, такі як: Черновол М.І., Карагодін В.І., Латипов Р.А., Молодик Н.В., Новіков О.М., Серебровский В.І, Шадрічев В.А., Червоіванов В.І., Ульман І. Е. та А.В. Грибенченко [1-5].

Мета і завдання досліджень. *Мета* досліджень - підвищення зносостійкості і довговічності відремонтованих деталей автомобілів шляхом вдосконалення технології плазмового наплавлення.

Для досягнення поставленої мети вирішувалися наступні задачі досліджень:

1. виконати аналіз недоліків плазмового наплавлення;

2. обґрунтувати склад порошку для плазмового наплавлення автомобільних деталей при їх відновленні.

3. удосконалити технологію відновлення деталей машин плазмовим наплавленням на прикладі валів автомобільних агрегатів

Об'єкт дослідження – технологічний процес плазмового наплавлення деталей автомобільних агрегатів за допомогою порошкової суміші.

Предмет дослідження – підвищення зносостійкості автомобільних деталей при їх відновленні та ремонті.

Методи досліджень базуються теоретичному аналізі технологічних методів наплавлення.

Підвищення зносостійкості відремонтованих деталей машин - одна з актуальних задач технічного обслуговування і ремонту автомобільного транспорту.

Підвищення ефективності вузлів тертя може бути досягнуто конструкційними, технологічними і експлуатаційними способами в число яких входять: відповідний вибір конструкторських рішень при проектуванні або підбір матеріалів, що характеризуються високим рівнем триботехнічних властивостей; вдосконалення способів обробки поверхонь, що труться, що забезпечують підвищення їх чистоти і твердості; створення умов для рідинного тертя; дотримання раціонального режиму мащення, а також запобігання контактуючих поверхонь від забруднень і інші. Причому в багатьох випадках визначальне значення, і, як наслідок, вирішальне внесок, набувають конструкція або матеріали трибоспряжень [1-4].

Таким чином, підвищення працездатності і довговічності машин і механізмів за рахунок зменшення частки передчасних відмов і збільшення їх надійності внаслідок зростання несучої здатності з’єднань деталей, яка визначається багато в чому застосовуваними матеріалами цих деталей, є надзвичайно важливим і перспективним напрямком, що відповідає сучасним тенденціям.

Аналіз літературних джерел показав, що при ремонті автомобілів ремонті значне число деталей типу «вал» відновлюється наплавленням. Особливо актуально відновлення дорогих валів автомобільних агрегатів. Останнім часом широко застосовується плазмове наплавлення порошковими сумішами з активуючими добавками [1-7], що дозволяє отримати наплавлений шар із заданими фізико-механічними властивостями.

Додавання елементів - активаторів з різко відмінними параметрами електро- і теплопровідності, а також їх специфічні властивості активують процес отримання необхідних властивостей металопокриттів.

Такими активаторами є кремній, бор і алюміній. Кремній і особливо бор мають високу розкислювальну здатність. Частинки активаторів в порошковій суміші стають центрами різко підвищеної дифузійної активності. Додатковим позитивним чинником застосування бору є його висока легуюча здатність.

Таким чином, пошук нових технологічних рішень щодо підвищення зносостійкості і довговічності деталей при відновленні способом плазмового наплавлення є актуальним завданням.

У даній роботі в основу досліджень покладено використання активуючого впливу хімічних елементів порошкових сумішей на процес формування щільних відновлювальних металопокриттів плазмового наплавленням з подачею порошку в робочу зону і оптимальних режимів формування шару.

Активуючі добавки при наплавленні порошкових сумішей впливають прямим впливом на процес припікання частинок основних компонентів один до одного і до основи за рахунок легування контактних ділянок.

Введення в порошкову суміш добавок призводить до дифузійних потоків, обумовлених градієнтами концентрації елементів і градієнтом температури. У разі прогрівання порошкової суміші з великою швидкістю нагрівання всієї маси частинок

порошку, висока ступінь неоднорідності електропровідності і теплопровідності контактів повиненн привести до істотно неоднорідного поля температур.

Тому додавання елементів-активаторів з різко відмінними параметрами електро - і теплопровідності, а також їх специфічні властивості в конкретних умовах активують процес отримання необхідних властивостей металопокриттів. Такими активаторами є кремній, алюміній і особливо бор.

Бор має високу розкислювальну здатність. Частинки його в порошковій суміші стають центрами різко підвищеної дифузійної активності. Бор з киснем утворюють склоподібні з'єднання, які оберігають матеріал шару та основи від подальшого окислення при високих температурах, обмежуючи доступ кисню в шар. При цьому створюється ефект «обмеженого простору», в якому діє механізм очищення поверхні в малих обсягах. Крім того, сполуки типу боросилікатного скла мають високу здатність зберігатися, не виявляючи ознак кристалізації при тривалому впливі високих температур. Додатковим позитивним чинником застосування бору є його висока легуюча здатність.

У представленій роботі при розгляді питань активування і оптимізації процесу нанесення тонкостінних металопокриттів покладені в основу такі положення:

- плазмове наплавлення є високоенергетичним процесом, що характеризується високою температурою нагрівання елементів порошкових сумішей, їх швидким охолодженням, високою швидкістю проходження металу уздовж фронту кристалізації і, отже, малою протяжністю фазних областей;
- висока температура нагрівання порошкоподібних матеріалів, що застосовуються, впливає на рухомість атомів, що призводить до превалюючого дифузійного процесу елементів в основний матеріал;
- застосування наплавлювальних порошкових сумішей на основі заліза і нікелю, що випускаються промисловістю, не дозволяє отримати щільне наплавлення для роботи в умовах пар тертя.

Розглядаючи ці умови, а також результати досліджень по активуванню в області наплавлення, була прийнята функціональна схема формування якісних нарощених шарів.

Проведені попередні досліди по здійсненню процесу формування шару плазмовим способом із застосуванням бору на поверхні деталей - зразків дали позитивні результати.

Якість наплавленого металу залежить від вибору режиму процесу наплавлення.

Висновки. Плазмове наплавлення є ефективним способом відновлення деталей автомобілів. Додавання елементів - активаторів з різко відмінними параметрами електро- і теплопровідності, а також їх специфічні властивості активують процес отримання необхідних властивостей металопокриттів. Такими активаторами є кремній, бор і алюміній. Кремній і особливо бор мають високу розкислювальну здатність. Частинки активаторів в порошкової суміші стають центрами різко підвищеної дифузійної активності. Додатковим позитивним чинником застосування бору є його висока легуюча здатність.

Список літератури

1. Воробьев, Е.А. Трибологические характеристики плазменных покрытий коленчатого вала двигателя, полученных с использованием электроэрозионных материалов/ Е.А. Воробьев, Е.В. Агеев, И.П. Емельянов // Мир транспорта и технологических машин. - 2016. - № 3(54). - С. 32-38.
2. Воробьев, Е.А. Совершенствование технологии восстановления коленчатого вала двигателя КамАЗ-740 плазменно-порошковой наплавки путем применения порошковых электроэрозионных материалов / Е.В. Агеев, Е.А. Воробьев, И.П. Емельянов // Мир транспорта и технологических машин. - 2016. - № 2 (53). - С. 53-61.
3. Грибенченко А.В. Исследование режимов плазменной наплавки при восстановлении цилиндрических деталей металлическими порошками./В.И.Федякин, В.И.Онищенко, А.В. Грибенченко //Проблемы научного обеспечения экономической эффективности орошаемого земледелия в рыночных условиях. /ВГСХА, Волгоград, 2001. - с. 226.
4. Грибенченко А.В. Исследования микроструктуры металлопокрытия, полученного при плазменной наплавке. /А.В. Грибенченко //Материалы VI региональной конференции молодых исследователей Волгоградской области. /ВГСХА, Волгофад, 2002. - с. 110.
5. Грибенченко А.В. Исследование влияния режимов плазменной наплавки и состава порошка на

формирование металлопокрытий. /В.И. Онищенко, А.В. Грибенченко //Материалы V I региональной конференции молодых исследователей Волгоградской области. /ВГСХА, Волгоград, 2002. - с.110-112.
6. Грибенченко А.В. Технология восстановления коленчатых валов двигателей ЯМЗ-240, А-41, ЗМЗ-53 плазменной наплавкой. //В.И. Онищенко, А.В. Грибенченко //Проблема агропромышленного комплекса. /ВГСХА, Волгоград, 2003. - с. 120-121.
7. Грибенченко А.В. Восстановление цилиндрических деталей методом плазменной наплавки с использованием ферромагнитных порошков. /А.И. Рядков, А.В. Грибенченко //Инженерные науки. Вып. 4. /ВГСХА, Волгоград, 2003. - с. 36-38.

УДК 651.012.12

А. Немненко, магістр гр. ІС-19М (1,4)
В. Барабаш, канд. пед. наук, доцент
Центральноукраїнський національний технічний університет

ПРОГРЕСИВНІ ПІДХОДИ ДО ЕФЕКТИВНОЇ УПРАВЛІНСЬКОЇ ДІЯЛЬНОСТІ НА ПІДПРИЄМСТВІ

У статті досліджено основні підходи до ефективного здійснення управлінської діяльності на підприємстві. А саме формування штрихкодування певних видів документів та особливості підписання вихідних листів електронним цифровим підписом. Також висвітлено електронних документообіг в його постійній видозміні, створення та реєстрація електронних документів.
сучасне підприємство, управлінська діяльність, електронний документообіг, електронні програми, штрихкодування, електронний цифровий підпис

Постановка проблеми. У час постійного вдосконалення усіх сфер життя, розвиток підприємств різного спрямування є особливо значущим. У період економічних зростань впровадження ефективних, а головне прогресивних підходів до управлінської діяльності дає можливість компаніям досягати необхідну результативність. Такі заходи можуть дати поштовх для удосконалення самого апарату документообігу, створення більш надійних умов для збереження автентичності документів.

Аналіз останніх досліджень та публікацій. Сучасні інформаційні технології є невід'ємною складовою прогресивних підходів ефективної реалізації управлінської діяльності різного роду установ.

Проблематикою електронного документообігу підприємства займається чимало дослідників, серед яких В. І. Волинець [1], О. Б. Кукарін [2], І. В Куршатова [3], А. В. Ткачов [7], М. В. Ларін [4,5], О. Матвієнко [6], Є. О. Плешкевич [8], М. Цивін [6] та ін.

Сьогодні в науковій літератури питання самих підходів вдосконалення управлінської діяльності та їх впровадження на підприємствах потребує глибокого і всебічного дослідження. Здебільшого такі наукові розвідки потребують суттєвого обґрунтування та вдосконалення, адже підґрунтям для появи нових заходів є в основному лише Закони України: «Про електронні документи й електронний документообіг» [10] та «Про електронний цифровий підпис» [9]. Тому така тема є досить актуальною і потребує додаткового дослідження.

Мета й завдання дослідження. Метою роботи є дослідження особливостей формування електронного цифрового підпису та штрихкодування для електронних документів.

Для досягнення поставленої мети визначено такі завдання:

- Визначити особливості створення та реєстрації електронних документів у певних цифрових програмах.
- Дослідити формування штрихкодування на певних видах документів.

– Встановити надійність електронного цифрового підпису для вихідних листів.

Об'єктом дослідження є електронний документообіг та підходи до його вдосконалення.

Предметом дослідження є формування штрихкодування та електронного цифрового підпису для електронних документів.

Виклад основного матеріалу. Функціонування електронних документів на сучасному підприємстві є прогресивним і затребуваним підходом в управлінській діяльності, оскільки електронні документи дають змогу перемістити центр ваги комп'ютерної технології із традиційних структурованих алфавітно-цифрових даних на потоки даних, які містять більші обсяги неструктурованого тексту, а також графіки, зображення, звук чи відео.

Закон України «Про електронні документи й електронний документообіг» так представляє сутність електронного документа – це «документ, інформація в якому зафіксована у вигляді електронних даних, включаючи обов'язкові реквізити документа. Він може бути створений, переданий, збережений і перетворений електронними засобами у візуальну форму, якою являється подання ЕД з відображенням даних, які він містить, електронними засобами або на папері у формі, придатній для сприймання його змісту людиною» [10].

Узагальнюючи наявні визначення вчених, можемо стверджувати, що електронний документ – це системний і послідовний прогрес, що відбувається в пам'яті ЕОМ, який перетворює цифровані дані, що знаходяться на «жорстких носіях», в зручну для сприйняття людиною форму. Як показує досвід роботи з електронними документами, користувач спілкується з «машиною» через інтерфейс, що надається йому операційною системою, програмами оболонками і програмами обробки даних, представлених на «жорстких» носіях, і сукупність даних, представлених на таких носіях (дискети, компакт-диски, вінчестери тощо). У такому разі користувач має змогу опрацьовувати необхідну інформацію тільки за допомогою комп'ютера, причому комп'ютер має бути включений, і на ньому має бути встановлена і запущена відповідна операційна система та програма. Як правило, така програма перетворює цифровані дані у візуальне відображення, що не тільки полегшує сприйняття представленої інформації, а й удосконалює весь процес документообігу будь-якого підприємства.

Важливо зазначити, що електронний документ – це віртуальний документ, оскільки існує тільки у момент роботи з даними як візуальна форма на екрані комп'ютера. При цьому слід врахувати, що такий документ, роздрукований на принтері, є лише друкарською копією, а це означає, що з електронним документом така копія ідентична лише за своїм змістовим наповненням, і її не можна вважати електронним документом. У такому разі оригіналом електронного документа буде примірник документа з наявними обов'язковими реквізитами. Реквізити представляють необхідні елементи чи дані в електронному документі (у першу чергу – електронний цифровий підпис автора), без яких він не може бути підставою для його обліку і не матиме юридичної сили.

Говорячи про прогресивні підходи в документаційній сфері, слід указати на важливі фактори ефективної управлінської діяльності, це, передусім, доступність системи електронного діловодства та документообігу установи всім структурним підрозділам та зручність і незмінність всієї системи електронного документообігу.

Все зазначене вище підтверджує необхідність і важливість використання електронно-інформаційних ресурсів на сучасному підприємстві, адже їх активне застосування надає можливість працівникам здійснювати свою діяльність на суттєво новому рівні.

Для введення електронного документообігу на підприємстві потрібна чимала кількість процесів і організованість самих його працівників. Перехід апарату підприємства від паперового документообігу до електронного супроводжується розробленням спеціальної не перебійної системи для всіх працівників підприємства. Це можливе завдяки відповідним електронним програмам, які містять в собі безліч процесів саме для впровадження електронного документообігу. Процеси створення, реєстрація, погодження, підписання,

виконання документів є основними в цих програмах. Всі вони налаштовуються фахівцями управління інформаційних технологій, які можуть навіть з неповної електронної програми зробити «продукт» високої та продуктивної якості. До прикладу, можна розглянути самий вигляд головної сторінки однієї із таких електронних програм, як 1С: Документообіг КОРП на рисунку 1:

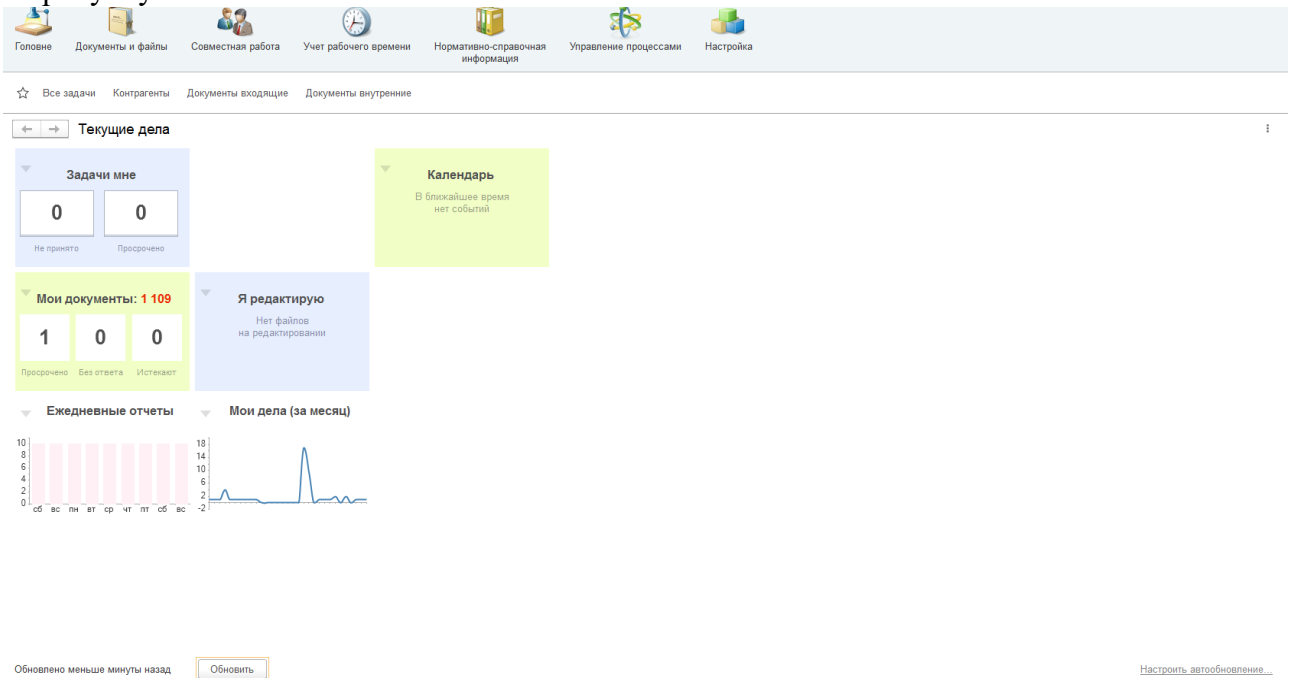


Рисунок 1. Головна сторінка програми 1С: Документообіг КОРП

Основною особливістю такого електронного документообігу є повний контроль виконання будь – якого документа. Керівник, який хоче досягнути порядку та відповідальності серед своїх підлеглих, вимагає повної прозорості у виконанні всієї роботи на підприємстві може без проблем контролювати будь-який процес у електронній програмі. А для працівників відділу діловодства така програма є надійним засобом збереження усіх документів, які підлягають реєстрації, швидкості їх пошуку, контролю виконання та отримання резолюцій керівників в один клік. До того ж, електронні програми дають змогу вести журнали реєстрації вхідних, вихідних та внутрішніх документів. А також для всіх видів документів автоматично присвоювати реєстраційні індекси, лише для звернень громадян реєстрація здійснюється вручну.

Та все ж, на будь-якому підприємстві аж ніяк не можуть бути присутніми лише електронні документи. Вхідні листи паперового формату завжди будуть надходити до установ і це не буде вважатися помилкою чи такі документи не будуть підлягати розгляду. До електронного документообігу переходять в основному великі і прибуткові компанії, а малі підприємства не можуть дозволити такий значний і затратний перехід, також при зверненнях громадян заяви пишуться і приймаються на аркуші паперу.

Тому при надходженні паперового документа на підприємство з електронним документообігом, він обов’язково вносить в картку вхідного документа, реєструється з автоматичним присвоєнням номеру, який переносить на аркуш документа, далі він сканується і прикріплюється до картки в електронній програмі. Після цього аналогічно такий документ направляється на розгляд та виконання.

Електронні програми з кожним періодом свого використання постійно вдосконалюються, як і сам електронний документообіг. У цих програмах тепер можна не лише здійснювати процеси документообігу, а й формувати штрих-код документів та налаштовувати електронний цифровий підпис. Саме штрихкодування документів є новим у сфері управління і здійснення документообігу. Адже раніше штих-код застосовувався лише для різних продовольчих товарів, а тепер його можна зустріти і на документах.

Штрихкодування має функцію підтвердження оригінальності документів, їх єдиного формату. Також він є зручним для пошуку документів у електронній програмі.

Процес штрихкодування можливо налаштувати в електронній програмі. Визначити розміщення штрих-коду на аркуші так, щоб він не заважав основному текстові документа. У більшості випадках його проставляють або у лівому верхньому куті аркуша нижче реєстрації, або у правому нижньому куті. Також у програмі є доречним налагодження відповідного розміру штрих-коду, щоб можливо було його розглянути без прикладання лупи. Штрих-код на документі має такий вигляд, як показано на рисунку 2:

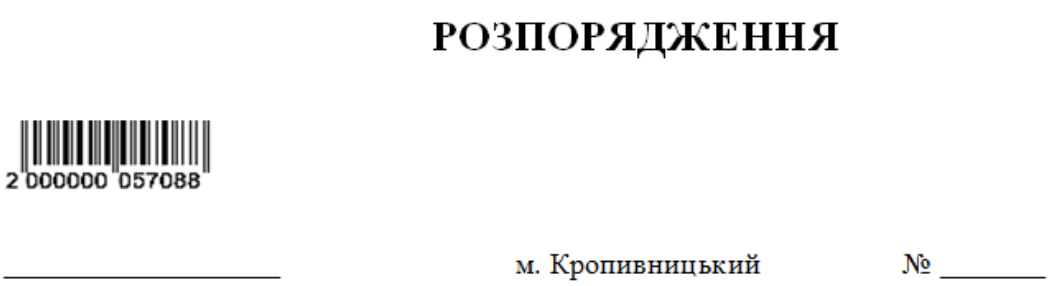


Рисунок 2. Формування документа зі штрих-кодом

Формування та налагодження електронного цифрового підпису для документів є одним із найбільш складних, але дієвих процесів у всій електронній програмі. Такий вид підпису дає можливість керівникові підписувати документи в одне натискання клавіші і тим самим підтверджувати повну автентичність будь-якого документа.

Здебільшого електронний цифровий підпис (ЕЦП) застосовуються саме для вихідних листів. Тобто після підписання такий документ надсилається працівникові відділу діловодства для формування та відправлення вихідного листа по електронній пошті. Самий процес формування листа з ЕЦП супроводжує не малу кількість етапів, а саме збереження листа в електронній програмі усіх відповідних файлів з електронним підписом, визначення його правильного розміщення на аркуші, внесення реєстраційного номеру вихідного листа, збереження у .pdf форматі та відсилання одержувачу по електронній пошті. Адресат, отримавши такого листа, має змогу переконатися у повній оригінальності листа, його юридичної цілісності.

Висновки. Отже, електронний документообіг є більш надійним та прогресивним аналогом паперового документообігу. Завдяки різним електронним програмам створення, реєстрація та виконання різних документів здійснюється набагато швидше і продуктивніше. Штрихкодування є одним із новітніх підходів, який надає електронним документам форму оригінальності. Електронний цифровий підпис дозволяє підтверджувати автентичність та юридичну силу документів. Ефективні підходи до удосконалення діяльності підприємства є універсальними, завдяки яким підприємство займає високий статус серед інших підприємств і установ.

Список літератури

1. Волинець В.І. Електронний цифровий підпис: сутність, принципи дії та порядок отримання. URL: http://dspace.tneu.edu.ua/ bitstream/316497/23292/1/111-112.pdf. (дата звернення 07.12.2020).
2. Кукарін О.Б. Електронний документообіг та захист інформації: навч. посіб. За заг. ред. Н.В. Грицяк. Київ: НАДУ, 2015. 84 с.
3. Куршатова І.В. Електронний документообіг і його особливості. Актуальні проблеми економіки. 2009. № 3. 237 с.
4. Ларин М.В. Некоторые проблемы эволюции управленческого документа. Вестник архивиста. 1999. № 6. 43

с.
5. Ларин М.В. Управление документацией в организациях. М.: научная книга. 2002. 288 с.
6. Матвієнко О., Цивін М. Основи організації електронного документообігу: навчальний посібник. К.:Центр учбової літератури, 2008.112с.URL: http://kul-lib.narod.ru/bibl.files/Teach/Teachposibnuk.pdf (дата звернення 07.12.2020)
7. Ткачев А.В. Правовой статус компьютерных документов: основные характеристики. М.: Городец-издат. 2000. 95 с.
8. Про електронний цифровий підпис: Закон України від 07.11.2018 р. № 852-IV. URL: https://zakon.rada.gov.ua/laws/show/852-15#Text (дата звернення: 01.12.2020).
9. Про електронні документи: Закон України від 22.05.2003 р. № 851-IV у редакції від 07.11.2018 р. URL: https://zakon.rada.gov.ua/laws/show/851-15#Text (дата звернення: 03.12.2020).

УДК 631.454

І. Ніковський, магістр гр. ЕО-19М
Л. Коломієць, доцент
Центральноукраїнський національний технічний університет

ЕКОЛОГІЧНЕ ЗНАЧЕННЯ ВНЕСЕННЯ ОРГАНІЧНИХ ДОБРИВ У ГРУНТ

Проаналізовано сучасний стан грунтів в умовах інтенсивного використання та втрати родючості. Розглянуто можливість удобрення за рахунок альтернативних джерел
грунти, гумус, елементи живлення, мінеральні та органічні добрива,, сидерати, агроекосистеми, агрофітоценоз, мікрофлора

Грунт є особливим утворенням, сформованим в процесі складних природних взаємодій компонентів біосфери та літосфери, під впливом живих організмів, атмосферних явищ та материнських порід. В сприятливій зоні лісостепу та степу грунтотвірний процес протікав особливо активно. Тривалий період позитивних температур, достатня кількість опадів вегетаційного періоду, багатий рослинний світ минулих епох забезпечили формування родючих чорноземів із високим вмістом органіки, елементів мінерального живлення рослин,

Актуальність. Збереження потенціалу родючості сільськогосподарських земель особливо важливе в наш час, коли кількість населення планети зростає, а паралельно збільшується потреба в продуктах харчування. Загострюється вимога сучасного суспільства щодо підвищення продуктивності орних земель, тобто отримання все більших врожаїв із тих самих площ посівів. Тому актуальним є збереження властивостей грунтів в умовах антропогенного тиску.

Мета дослідження: визначити доступні шляхи відновлення вмісту поживних речовин у грунті.

Завдання: - з’ясувати, яким змінам піддається грунт під впливом людської діяльності;

- виявити причини зниження вмісту гумусу;

- розглянути сидерацію як доступний і ефективний метод для відновлення балансу органічної речовини в грунті.

Об’єкт дослідження: показники грунтів в умовах ведення інтенсивного сільського господарства.

Предмет дослідження: зниження вмісту гумусу.

Результати досліджень.

Через постійний обробіток грунту та вирощування культурних рослин, що передбачає розпушення верхнього шару та утворення плужної підошви, в агрофітоценозах змінюється

природний хід процесів накопичення поживних речовин, мінералізації органічних решток, вологоутримання, умов для грунтової мікрофлори.

Якщо урожайність можна забезпечити мінеральними добривами, що вносяться у все більших дозах діючих речовин, то родючість – це більш вимоглива ознака славетних українських чорноземів. Найвагомішим багатством грунтів є гумус - органічна речовина, що накопичується завдяки фотосинтезу. Вміст гумусу наших чорноземів становить сьогодні до5%. За останню сотню років кількість гумусу в ґрунті зменшилася і становить приблизно 3-4%. Щорічно ґрунти України втрачають 14 млн.т гумусу через мінералізацію, та ще за рахунок ерозії біля 19 млн т. не лише в Україні але і в глобальному масштабі вміст гумусу зазнає негативної динаміки. Якщо на протязі 5-10 років це соті чи десяті долі, то за століття негативний ефект є більш помітним. Найбільше гумусу сконцентровано у верхньому шарі, де розкладається органіка, це якраз і є середовище розміщення кореневої системи рослин. Агроекологічні властивості грунту погіршуються внаслідок інтенсивного вирощування сільськогосподарських культур, недотримання сівозміни, відсутності зернобобових багаторічних посівів кормових культур, які дають грунту можливість відпочивати та відновлюватися. (табл. 1). Винос органічної речовини з товарною частиною врожаю, за колесами тракторів та комбайнів, через вітрову та водну ерозію є на сьогодні вже загрозливого мастабу [1-3].

Таблиця 1 – Особливості винесення елементів живлення сільськогосподарськими культурами, кг/т продукції

Культура	Продукція								
	Основна			Побічна			Основна з урахуванням побічної		
	N	P_2O_5	K_2O	N	P_2O5	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	-	-	-	-	-	-

Вчені Л.А.Гришина і Д.С.Орлов розробили градації забезпеченості ґрунту гумусом. Вміст гумусу в грунті визначається його відсотковим вмістом, а також запасами у тоннах на 1 га. Запаси гумусу класифікуються від дуже високих до дуже низьких (табл. 2).

Таблиця 2 - Параметри вмісту і запасу гумусу в грунтах

Запаси гумусу	Вміст гумусу, %	Запаси гумусу в шарі ґрунту, т/га	
		0-20 см	0-100 см
Дуже високий	>10	>200	>600
Високий	6-10	150-200	400-600
Середній	4-6	100-150	200-400
Низький	2-4	50-100	100-200
Дуже низький	<2	<50	<100

Середній вміст гумусу 4-6% означає запаси 100-150 т/га в шарі грунту 0-20 см, та 200-400 т/га в 0-100 см шарі. Накопичувалось таке багатство протягом мільйонів років, а от витрачається значно швидше.

Окрім того, що неправильна агротехніка, розпушення та переущільнення порушують стійкість грунтових структур, додаються ще й хімічні забруднювачі, - внаслідок вимушеної хімізації сільського господарства. Культурні рослини є значно більш вразливими до складних факторів довкілля, ніж їх дикоростучі предки. Сільськогосподарським культурам дошкуляють хвороби, шкідники, засухи, приморозки і т.п. Аби збільшити їхню виживаність в таких умовах, забезпечити високі врожаї, споживчі якості та інші бажані характеристики рослинницької продукції, на допомогу приходить арсенал сільгоспхімії. Це пестициди різних груп застосування, без яких неможливо отримати бажаний економічний ефект господарювання, але і споживати таку продукцію вже тепер буває небезпечно. Власне пестициди являють собою складні хімічні сполуки, зокрема хлорорганічні та фосфорорганічні, які діють в мікродозах, накопичуються в грунті, є доволі стійкими в довкіллі, тому потрапляють до підгрунтових вод, далі можуть рухатися до колодязів, джерел водокористування та водопостачання, несучи екологічну небезпеку здоров'ю живих істот, в першу чергу людини.

Внесення високих доз мінеральних добрив небезпечне баластними речовинами – хлоридами, сульфатами та ін. А ще під час багаторазових обробітків полів грунти забруднюються відпрацьованими вихлопними газами тракторів, комбайнів, автомобілів, мастилами та пальним. Через діяльність промислових підприємств грунти забруднюються важкими металами, фторидами, хлоридами, сульфатами, радіонуклідами [4-5].

При тривалому використанні землі, особливо через внесення пестицидів, у 2-6 разів зменшується кількість живих організмів у ґрунті, які мають велике екологічне значення (за даними Булахова В.Л. (1988). Це призводить до втрати структурності, переущільнення грунту, зниження процесів розкладання органічної речовини, зменшення шпаруватості, погіршення умов аерації і т.д.

З метою збереження грунтових ресурсів необхідно вносити не лише мінеральні добрива (хоча й без них за інтенсивного обробітку не обійтись), але обов'язково і органічні, в поєднанні з першими. Якщо є можливість, то дуже сприятливим є і саме органічне удобрення, але через відсутність тваринництва необхідних кількостей для повного внесення (30 т/га і більше залежно від стану грунту і культури, під яку вноситься), просто немає. Грунти, удобрені органікою, є більш структурними. Структурність ґрунту, в якому переважають агрегати грудкувато-зернистої структури розміром від 10 до 0,25 мм, має пухке складення, меншу щільність та більшу шпаруватість. Безструктурний ґрунт має лише капілярні шпарини, а структурний – поряд з капілярними й крупні пори, як між агрегатами так і всередині їх, які заповнені повітрям. Ґрунти природних екосистем мають чітко виражену зернисту структуру, а тому менше випаровують (і втрачають) вологи, на відміну від агроекосистем без внесення органічних дорив, які є безструктурними ґрунтами.

Як було зазначено, традиційних органічних добрив на сьогодні не вистачає. В таких умовах варто звернути увагу на значні досі непомічені резерви органіки, якої так потребують грунти агрофітоценозів. В конкретних місцевих умовах це можуть бути осади стічних вод

житлово-комунального господарства, пожнивні рештки соломи, стебел, соняшнику, листовий опад, вермикомпости, а також «зелені добрива», які можна виростити самому на тому полі, яке має потребу в відновленні органічної речовини. Є досить широкий випробуваний в господарствах України і не тільки перелік культур, придатних для сидерації. Це люпин, кормові боби, гірчиця, соя, озиме жито, навіть гречка. Посівний матеріал вказаних культур висівається згідно прийнятої технології, в оптимальну фазу приорюється, швидко розкладається та в процесі мінералізації відбувається вивільнення легкодоступних форм елементів живлення, чому сприяє поліпшення умов грунтового живлення мікрофлори, яка потребує органічної речовини.

Висновок. Оскільки грунтові ресурси гостро потребують збереження та відновлення, через негативну динаміку вмісту гумусу, потрібно кардинально міняти підхід у землеробстві та рослинництві, який поки що є більш споживацьким, ніж раціональним. Щоб зберегти грунти для наших нащадків, для їх підживлення в агроекосистемах треба застосовувати природоподібні процеси.

Список літератури

1. Крупеников И. А. Черноземы. Возникновение, совершенство, трагедия, деградации, пути охраны и возрождения / И. А. Крупеников. – Кишенеу : Pontos, 2008. – 288 с.
2. Гумусний стан грунтового покриву / С.Л. Синицький, Л.І. Павленко, О.Г. Хитрук, Ю.В. Боярко, С.В. Задорожна, С.В. Давиборщ, Т.І. Панфілова: Агроекологічний журнал, № 4, 2013. - с.61-64.
3. За ред. В.В.Медведєва Стан родючості грунтів України та прогноз його змін за умов сучасного землеробства. / - Х.: Штрих, 2001. -100с.
4. Сучасні технології відтворення родючості ґрунтів та підвищення продуктивності агросистем / за ред. Ю.О. Тараріко. - К.: Аграрна наука, 2004.
5. Добрива та їх використання: Довідник / Я.У. Марчук, В.М. Макаренко, В.Є. Розстальний, А.В. Савчук. – К., 2002. – с.: іл.

УДК 336.7

Т. Подплєтня, магістр гр. ФС-19МЗ
Центральноукраїнський національний технічний університет

ПІДХОДИ ДО ВИЗНАЧЕННЯ СУТНОСТІ РЕСУРСНОЇ БАЗИ БАНКІВ

Проаналізовано та узагальнено основні підходи до класифікації складових ресурсної бази банків. Визначено зміст поняття «структура ресурсної бази». Запропоновано інтегральну класифікацію складових ресурсної бази комерційних банків. Особлива увага звертається на характеристику видів складових ресурсної бази банку.

ресурсна база банків, джерела формування ресурсів, структура ресурсної бази банків, ресурси-витрати

Постановка проблеми. Стабільне функціонування та подальший розвиток банківської системи України перебувають у тісному взаємозв'язку із збільшенням обсягів банківських ресурсів. Від того, наскільки банки приділятимуть увагу формуванню ресурсної бази, залежить їх спроможність здійснювати активні операції та фінансова стійкість банківської системи загалом. Саме тому однією з необхідних передумов для ефективного функціонування банків та їх фінансової стійкості є стабільність і достатність їх ресурсної бази.

Успішне досягнення перспективних стратегічних цілей банку забезпечується за умов чіткої координації ролі ресурсної бази банку у системі стратегічного управління усіма його видами діяльності та ефективного формування складу та структури. Структура ресурсної

бази банку має принципову відмінність від аналогічної структури сучасних підприємств. Причина цього – особлива роль банку в економіці як фінансового посередника, його виняткове право прийняття внесків юридичних і фізичних осіб, унаслідок чого банк не може функціонувати переважно на основі лише своїх власних коштів.

Збалансована за складом та структурою ресурсна база банків є важливою передумовою їх прибутковості, підтримки достатньої ліквідності та довіри з боку всіх учасників ринку. Тому методологічно важливим є питання типології структурних складових елементів ресурсної бази банку та систематизація їх сукупності.

Аналіз останніх досліджень і публікацій. Вивченню питань сутності та складу ресурсної бази банків присвячені роботи багатьох вчених, зокрема: М. Д. Алексєєнко [1] значну увагу приділяє розкриттю сутності та структури банківських ресурсів; Т. Я. Андрейків та інші вчені [2] розглядають джерела фор-мування та роль фінансових ресурсів у процесі фор-мування банківського капіталу; О. А. Кириченко [3], Л. О. Примостка [4] акцентують увагу на методах управління банківськими ресурсами; С. К. Реверчук [5], Р. Швець [6] наголошують на важливості ресурсної- бази банків, формуванні оптимального складу і струк-тури, а також на ролі окремих складових ресурсів у здійсненні банківської діяльності. В. В. Кисельов [7], І. М. Парасій-Вергуненко [8] вказують на першочерговій важливості залучених ресурсів у формуванні ресурсної бази банків. Серед зарубіжних вчених питання теорії управління ресурсним потенціалом банку, ефективності використання банківських ресурсів досліджували у своїх працях Б. Бернанке, Р. Габбард, Д. Колліз, Г. Марковіц, Г. Мінські, Ф. С. Мишкін, Дж. Стігліц, Ж.-К. Тріше, які розглядали джерела їх формування загалом.

Невирішені частини досліджуваної проблеми. Однак в умовах поглиблення кризових явищ у світовій економіці і в Україні проблема формування ресурсної бази в банківській системі потребує ще поглибленого дослідження. Крім того, сьогодні не існує єдиної інтегральної класифікації складових елементів ресурсної бази банківських установ.

Об'єкт дослідження – наукові підходи до класифікації елементів ресурсної бази банків в Україні.

Метою статті є систематизація наявних методичних підходів до класифікації складових ресурсної бази банків як важливого елементу управління банківськими ресурсами та розробка на основі додаткових класифікаційних ознак інтегральної (узагальненої) класифікації їх ресурсної бази.

Для досягнення поставленої мети необхідно виконати такі завдання:

1. Узагальнити наявні підходи до класифікації складових ресурсної бази банків та виокремити основні класифікаційні ознаки, які наводяться вченими.
2. Сформувати інтегральну класифікацію складових ресурсної бази банків.
3. Визначити зміст поняття «структура ресурсної бази».
4. Окреслити можливі напрями удосконалення процесу формування ресурсної бази банків.

Виклад основного матеріалу. Питання класифікації складових елементів ресурсної бази банку є дискусійними і недостатньо висвітленими в економічній літературі. В основному з цією метою використовується один чи кілька критеріїв, переважно ознака власності, з виокремленням власного та залученого капіталу [7]. Водночас з таким підходом не можна погодитися, оскільки він істотно обмежує можливості пізнання сутності, закономірностей формування і функціонування ресурсної бази.

Прихильники іншого підходу до класифікації елементів ресурсної бази банку [3, 5, 8, 9], ґрунтуючись на їх багатоаспектності, не використовують класифікаційні ознаки, а подають перелік окремих складових ресурсної бази банку. Такий підхід, на погляд авторів даної роботи, не завжди забезпечує чіткість і взаємопов'язаність системи використовуваних елементів ресурсної бази банку.

Ще один підхід до класифікації елементів ресурсної бази банку заснований на використанні множини ознак класифікації [1, 2, 4, 6]. На думку авторів, цей підхід до

виявлення елементів ресурсної бази банку ускладнює упорядкованість елементів ресурсної бази банку, призводить до тавтології змісту деяких з них.

Суттєвими класифікаційними ознаками, які наводяться вченими, є такі:

- джерела формування ресурсів;
- термін знаходження ресурсів у розпорядженні банку;
- резидентність походження ресурсів;
- можливість прогнозування;
- місце мобілізації ресурсів тощо.

З огляду на вищевикладене автори вважають, що за доцільне сформулювати інтегральну класифікацію складових елементів ресурсної бази банківських установ, що дасть змогу окреслити можливі напрями удосконалення процесу формування їх ресурсної бази.

Спершу треба визначити зміст поняття «структура ресурсної бази». Більшість економістів розглядають під структурою капіталу співвідношення власних та залучених фінансових ресурсів, що використовуються банками у процесі своєї діяльності. Так, С. Росс, Вестерфілд і Б. Джордан розуміють під структурою капіталу «відношення заборгованості до акціонерного капіталу» [10], а І. А. Бланк визначає структуру капіталу як «співвідношення усіх форм власних та залучених фінансових ресурсів, що використовуються банком в процесі своєї діяльності для фінансування активів» [11]. Водночас, розуміючи під поняттям «капітал» в даному дослідженні саме ресурсну базу банку, автори роботи не можуть однозначно прийняти жодну з вищенаведених позицій у відношенні структури ресурсної бази та сформулюємо власне її визначення як «співвідношення між окремими статтями власного капіталу і зобов'язань банку (залучених і позичених коштів) та між окремими елементами ресурсної бази банку загалом із метою забезпечення стабільності та зниження витратності залучених та позичених ресурсів».

Виходячи з існуючих підходів до класифікації структурних елементів ресурсної бази банку, нами розроблена їх класифікація за найбільш суттєвими ознаками, яка має за мету вирішення стратегічного завдання банку: знайти джерела ресурсної бази з мінімальною вартістю, забезпечити здійснення активних операцій у визначених обсягах і напрямах, ефективно використовувати та управляти ресурсною базою.

Автори роботи розглянули детальніше запропоновану класифікацію елементів ресурсної бази банку за такими ознаками.

За ресурсною ознакою структурні елементи ресурсної бази банків можемо поділити на: трудові ресурси, фінансові ресурси, природні ресурси, матеріальні ресурси, інформаційні ресурси. У вітчизняній банківській практиці формування ресурсної бази передбачено переважно у грошовій формі, причому формування та збільшення статутного капіталу може здійснюватися виключно шляхом грошових внесків [12].

За направленістю ресурсних потоків відносно банку ресурси поділяють на:

- вхідні ресурси або ресурси-витрати. Вхідні грошові потоки банку створюють пасивну частину банківського балансу. Саме вони формують ресурсну базу і прибуток від його діяльності. Прикладом вхідних грошових потоків є грошові надходження на кореспондентські рахунки банку, в тому числі кошти, які надходять на розрахункові і поточні рахунки клієнтів, залучені депозити та міжбанківські кредити в момент надходження, інші пасиви. До вхідних необхідно віднести також потоки розміщених активів і процентного прибутку за користування ними в момент повернення;
- ресурси, створені у процесі діяльності або ресур-си-результати. До них нами віднесені активи банку, що виникають як наслідок розміщення акумульованих первинних ресурсів; прибуток від його діяльності, при-дбання нового обладнання та приміщень при розширенні діяльності банку тощо;
- вихідні ресурси. До вихідних ресурсів необхідно віднести всі грошові платежі, які здійснюються з кореспондентських рахунків банку: платежі за дорученням клієнтів, операції з розміщення залучених в тимчасове користування фінансових ресурсів і власних коштів, вкладення в основні засоби. Залучені платні пасиви в момент повернення процентів за їх

використання також належать до вихідних грошових потоків.

Запропонований поділ дозволяє простежити причин-но-наслідкові зв'язки у процесі формування ресурсної бази та здійснити відповідні кроки щодо збільшення її обсягів у розпорядженні банку.

За часовою ознакою ресурси поділено на: відносно статичні, тобто ресурси, що постійно знаходяться у розпорядженні банку і можуть вилучатися тільки при його ліквідації або реорганізації (кошти статутного капіталу, придбані у власність будівлі, обладнання тощо), відносно динамічні, тобто ресурси, що знаходяться у розпорядженні банку упродовж визначеного строку (залучені і запозичені кошти, орендовані приміщення тощо), статично-динамічні, тобто ресурси, що знаходяться у розпорядженні банку, однак не прогнозовано можуть бути вилучені власниками (кошти в розрахунках, залишки тимчасово вільних коштів на рахунках суб'єктів господарювання, інші джерела).

Дана класифікація дозволяє визначити рівень сталості ресурсної бази банку в часовому вимірі та вжити заходів для підвищення його фінансової міцності.

За ступенем новизни відносно бізнес-процесів банку:

- первинні (нові) ресурси (що раніше не обертались на фінансовому ринку). Первинний характер має залучення ресурсів, що купуються банком на ринку безпосередньо в їх власників (залучаються ресурси держави, сімейних господарств, суб'єктів господарювання, які виникли внаслідок здійснення господарської діяльності, з інших джерел отримання доходів і належать їм на правах власності);
- вторинні ресурси (що раніше вже обертались на фінансовому ринку). Вторинний характер має залучення ресурсів, які не належать безпосередньо кредитору банку, а вже залучені ним в інших суб'єк-тів на грошовому ринку.

Використання цього критерію має практичне значення, тому що:

по-перше, стабілізація економіки України, зростання темпів її економічного розвитку та інтеграція у світовий економічний простір супроводжуються поліпшенням фінансових результатів діяльності підприємств і доходів громадян, тому використання цього критерію буде своєрідним індикатором рівня розвитку економіки держави;

по-друге, розвиток грошового ринку супроводжується збільшенням кількості фінансових посередників, тому підвищення частки коштів вторинного залучення буде відображати вдосконалення інституційної структури грошового ринку та трансформаційної функції банківської системи. Однак, якщо ця тенденція відбувається на тлі кризових явищ в економіці, це буде характеризувати нестабільність і високу вартість ресурсної бази банків;

по-третє, виділення цих груп ресурсів дозволяє оці-нити ступінь успішності грошової політики в країні та міру довіри до банківської системи в суспільстві. Пропорції співвідношення коштів первинного і вторинного залучення визначаються розміром перших, тому що обсяги коштів вторинного залучення у першу чергу залежать від обсягів коштів на рахунках, що формують первинний ресурсний ринок.

За способом і джерелами формування розрізняють ресурси: власні (власний капітал і нерозподілений прибуток, власні «ноу-хау», праця штатних працівників), залучені (придбані на фінансовому ринку кошти у результаті надання банком послуг контрагентам, придбані чи інвестовані технології або патенти, природні ресурси), позичені (перекуплені на фінансовому ринку у результаті надання банком послуг контрагентам), комбіновані (створення асоціацій чи об'єднань господарюючих суб'єктів для реалізації проекту, залучення додаткових ресурсів, що доповнюють власні).

Автори статті зазначають, що поряд з виділенням багатьма авторами за критерієм джерел формування лише двох видів ресурсів банку (власних і залучених коштів), все частіше застосовується розширена класифікація ресурсів за цим критерієм з виокремленням трьох їх видів: власні, залучені і позичені [2, 4, 12]. Однак і при цьому підході мають місце розбіжності в трактуванні окремих структурних елементів ресурсної бази. Так, на думку Т. П. Остапишиної, «позичені ресурси – це грошові кошти кредиторів та інвесторів, мобілізовані банками на певних умовах на міжбан-ківському та фондовому ринках» [9]. При

цьому під визначення процесу мобілізації коштів на фондовому ринку підходить і продаж акцій, за рахунок яких може формуватися статутний капітал банку, а це вже сфера формування власного капіталу. Л. О. Дробозіна вказує, що ресурсна база банку формується за рахунок власних, залучених і емітованих коштів [13]. Виділення емітованих коштів як джерела формування ресурсної бази, на думку авторів, є некоректним, оскільки може включати і кошти, створені самим банком в процесі грошово-кредитної мультиплікації.

За ступенем участі у фінансово-господарській діяльності банку ресурси групуються як:

- ресурси, які беруть безпосередню участь у операційних бізнес-процесах (прямі) та формують ядро ресурсної бази банку (грошові кошти, персонал, матеріально-технічна база);
- ресурси, які опосередковано беруть участь у операційних бізнес-процесах (непрямі), забезпечуючи функціонування банку загалом (рівень оснащення системами обробки інформації та комунікаціями, невиробничі основні засоби, правова та юридична підтримка здійснення банківської діяльності, лобіювання інтересів банку, становище банку на ринку та сприйняття його суспільством, наявність кваліфікованої та відданої банку команди менеджерів тощо).

Використання запропонованої структури на практиці стимулює банк приділяти увагу всебічному вдосконаленню своєї діяльності в умовах зростаючої конкуренції та виживання в умовах кризових ситуацій на грошовому ринку.

Також пропонуємо запровадити критерій класифікації ресурсів за їх функціональним призначенням. Згідно цим критерієм нами виділено три складових:

- ресурси, призначені для формування портфеля дохідних активів (кредити, надані клієнтам банку; міжбанківські кредити; вкладення в спекулятивні операції — валютні цінності, цінні папери; інвес-тиційні вкладення тощо);
- ресурси, призначені для створення матеріально-технічної і технологічної бази банку;
- ресурси, призначені для самострахування банку від банківських ризиків, до яких слід віднести:

а) обов’язковий резервний фонд, сформований в межах нормативу обов’язкового резервування згідно з вимогами чинного законодавства; б) спеціальний резервний фонд, сформований в межах, установлених загальними зборами учасників (засновників, акціонерів).

Водночас автори зазначають, що структура ресурсів окремих банків є індивідуальною і залежить як від їх спеціалізації, так і особливостей їх діяльності, стану розвитку фінансового ринку, макроекономічної стабільності в країні та інших чинників. Так, в універсальних банках основний видом залучених ресурсів виступають короткострокові-депозити, оскільки такі банки здійснюють переважно операції з короткострокового кредитування, а іпотечні банки залучають ресурси в основному шляхом випуску та розміщення довгострокових зобов’язань, переважно іпотечних облігацій, що зумовлено здійсненням ними довгострокового кредитування під заставу нерухомості.

Зазвичай операції банку із залучення та запозичення коштів забезпечують формування ресурсів банку, необхідних йому для здійснення діяльності зверх власного капіталу. Такі ресурси покликані також забезпечувати ліквідність та одержання доходу.

Висновки. Отже, розглянута класифікація дозволяє більш ефективно здійснювати стратегічне управління діяльністю банку загалом та його ресурсною базою зокрема, від формування та використання якої залежить ефективність діяльності банківської установи та розвиток банківського сектору загалом. Фінансові показники діяльності банку (ліквідність, прибутковість, платоспроможність тощо) суттєво залежать від ступеня використання ресурсів банку для формування портфеля дохідних активів та обсягів невикористаної (резервної) ресурсної бази. Це дозволяє усунути недоліки в процесі управління пасивами та активами.

Враховуючи вищенаведене, можна зробити висновок, що ресурсна база виступає

основою фінансового потенціалу банку, його функціонування. Тому важливим побудова систематизованої класифікації, що охоплює різні складові елементи банківських ресурсів, що дозволяє простежити причинно-наслідкові зв'язки у процесі формування ресурсної бази банків та здійснити відповідні заходи щодо стратегічного управління нею.

Список літератури

1. Алексеєнко М. Д. Капітал банку: питання теорії і практики: монографія / М. Д. Алексеєнко. К.: КНЕУ, 2002. 276 с.
2. Вовчак О. Д. Кредит і банківська справа: підручник / О. Д. Вовчак, Н. М. Рущишин, Т. Я. Андрейків. К.: Знання, 2008. 564 с.
3. Кириченко О. А. Банківський менеджмент: підручник / за ред. О. А. Кириченка, В. І. Міщенка. К.: Знання, 2005. 831 с.
4. Примостка Л. О. Фінансовий менеджмент у банку: підручник / Л. О. Примостка. 2-ге вид., доп. і перероб. К.: КНЕУ, 2004. 468 с.
5. Банківський капітал: історія, теорія, досвід / С. К. Реверчук, У. В. Владичин, М. Б. Паласевич та ін.; за ред. д. е. н., проф. С. К. Реверчука. Львів, ЛНУ ім. І. Франка, 2004. 276 с.
6. Швець Н. Р. Аналіз та оцінка ресурсів банку: монографія / Н. Р. Швець. Чернівці: Рута, 2006. 168 с.
7. Киселев В. В. Управление банковским капиталом (теория и практика) / В. В. Киселев. М.: Экономика, 1997. 256 с.
8. Парасій-Вергуненко І. М. Аналіз банківської діяльності: навч.-метод. посібник для самост. вивч. дисц. / І. М. Пара- сій-Вергуненко. К.: КНЕУ, 2003. 347 с.
9. Остапишин Т. П. Основи банківської справи: курс лекцій. К.: МАУП, 1999. 112 с.
10. Росс С. Основы корпоративных финансов / С. Росс, Р. Вестерфилд, Б. Джордан. М.: Лаборатория Базовых Знаний, 2000. 720 с.
11. Бланк И. А. Управление формированием капитала / И. А. Бланк. К.: Ника-центр, 2000. 512 с.
12. Савлук М. І. Гроші та кредит: підручник / М. І. Сав- лук, А. М. Мороз, М. Ф. Пуховкіна та ін.; за заг. ред. М. І. Савлука. К.: КНЕУ, 2006. 744 с.
13. Дробозіна Л. О. Фінанси. Грошовий обіг. Кредит: навч. посібник; перекл. з рос. / Л. О. Дробозіна, Л. П. Окунєва та ін.; під ред. Л. О. Дробозіна. Рівне: Вертекс, 2001. 352 с.

УДК 651.012.12

Я. Пономаренко, магістр гр. ІС-19М (1,4)
О. Коломієць, канд. пед. наук, доцент
Центральноукраїнський національний технічний університет

КВАЛІФІКАЦІЙНИЙ ЕЛЕКТРОННИЙ ПІДПИС ЯК ЗАСІБ РОЗВИТКУ ДОКУМЕНТУВАННЯ ДІЯЛЬНОСТІ ПРИВАТНОГО ПІДПРИЄМСТВА

У статті досліджено шляхи вдосконалення документування діяльності приватних підприємств. Йдеться, зокрема, про можливості отримання кваліфікаційного електронного підпису та його функціонування в електронній системі документаційного забезпечення приватних підприємств.
приватне підприємство, документаційне забезпечення, кваліфікаційний електронний підпис, сертифікат ключа

Актуальність статті. Актуальність проблеми використання кваліфікаційного електронного підпису обумовлюється необхідністю застосування сучасних високотехнологічних і прогресивних підходів до організації системи документаційного забезпечення діяльності приватних підприємств в умовах інформатизації суспільства, а також пошуком ефективних методів їх впровадження та застосування.

Нині зростає роль електронних документів в управлінні процесом діяльності приватного підприємства. Використання електронної документації дає змогу створити автоматизовану систему документаційного забезпечення управління приватним підприємством для багаторазового використання. Це забезпечує оперативність фіксації, збору, оброблення, зберігання, пошуку та передачі документальної інформації.

Мета статті. Проаналізувати особливості функціонування кваліфікаційного електронного підпису в діяльності приватних підприємств

Новітній етап розбудови української державності, зростання динамізму суспільних перетворень, посилення інтеграційних процесів у всіх сферах життя накладають відбиток і на систему бізнесу, поставивши нові вимоги до організації діяльності приватних підприємств. Виникає потреба в розробці та впровадженні у діяльність приватних підприємств сучасних форм їх організації та розвитку з метою підвищення рівня конкурентоспроможності.

Будь-яке приватне підприємство самостійно вирішує проблеми документаційного забезпечення своєї діяльності. Проте, збільшення потоків інформації потребує докорінної зміни характеру виконання організаційних операцій і процесів інформаційного забезпечення організаційних рішень, опрацювання управлінської документації, документації з актуальних проблем, рішень тощо.

На зміну традиційній паперовій звітності приходять нові електронні форми документів. Електронне документування діяльності приватних підприємств передбачає: підготовку документів на основі стандартних бланків; документування інформації про роботу підприємства шляхом внесення в базу даних усіх версій документів; гарантовану ідентичну відповідність між паперовим документом і його електронною копією; спрощення пошуку необхідних документів; оптимізацію їхнього використання та зберігання.

Впровадження електронних форм документування є необхідною умовою якісного документаційного забезпечення діяльності приватних підприємств. А важливим засобом розвитку документування діяльності цих підприємств нам уявляється активне застосування кваліфікаційного електронного підпису (КЕП).

Саме поняття кваліфікаційний електронний підпис трактується як підпис, отриманий в результаті криптографічного перетворення набору електронних даних. Його реалізація проходить не лише за допомогою графічних зображень, а й за математичними перетвореннями над змістом документу. Так звана математика гарантує безпеку, тому що підробити електронний цифровий підпис неможливо.

Відповідно до Закону України «Про електронні довірчі послуги», кваліфікаційний електронний підпис – це удосконалений електронний підпис, який створюється з використанням засобу кваліфікаційного електронного підпису і базується на кваліфікаційному сертифікаті відкритого ключа.

Електронний підпис – це електронні дані, які додаються користувачем до інших електронних даних або логічно з ними пов’язуються і використовуються ним як підпис.

Засіб кваліфікаційного електронного підпису – апаратно-програмний або апаратний пристрій чи програмне забезпечення, які реалізують криптографічні алгоритми генерації пар ключів та створення електронного підпису, перевірки електронного підпису, або зберігання особистого ключа кваліфікаційного електронного підпису, який відповідає вимогам закону [2].

Система кваліфікаційного цифрового підпису припускає, що кожен користувач будь-якої електронної мережі має свій особистий ключ. Цей ключ зберігається в таємниці і використовується для формування підпису. Існує також так званий відкритий ключ, відомий решті користувачів мережі і призначений для перевірки справжності документа. Цифровий підпис обчислюється на основі особистого ключа відправника інформації й власної системи інформаційних бітів (розмірів) документу.

Система кваліфікаційного підпису розроблена таким чином, що наявність відкритого ключа не надає можливості іншому користувачу зчитувати алгоритм підпису задля подальшої його підробки.

Підтвердження фізичної особи, яка звернулася за отриманням послуги формування кваліфікаційного сертифіката відкритого ключа, здійснюється за умови її особистої присутності, за паспортом громадянина України або за іншими документами, які заперечують будь-які сумніви щодо особи, відповідно до законодавства про Єдиний державний демографічний реєстр та про документи, що посвідчують особу, підтверджують громадянство України чи спеціальний статус особи.

Допускається розпізнання фізичної або юридичної особи електронних довірчих послуг за ідентифікацією даних, які містяться в започаткованому раніше кваліфікаційному сертифікаті відкритого ключа, за наявності терміну дії.

На офіційному сайті Центрального засвідчувального органу можливо перевірити цілісність та достовірність відповідного електронного документу. Після завантаження електронного документу, на який було накладено цифровий підпис, на адресу центру технічної підтримки засвідчувального органу, мають надійти результати щодо справжності, цілісності та терміну дії сертифікату електронного підпису.

Під час перевірки цивільної правоздатності та дієздатності юридичної особи надавач електронних довірчих послуг зобов'язаний ознайомитися з інформацією про юридичну особу, що міститься в Єдиному державному реєстрі юридичних осіб, фізичних осіб – підприємців та громадських формувань, а також пересвідчитися, що обсяг її цивільної правоздатності та дієздатності є достатнім для формування та видачі кваліфікованого сертифіката відкритого ключа[2].

Законодавство передбачає, що установа чи кваліфікована особа, яка надає електронні довірчі послуги шляхом видачі сертифікату відкритого ключа, має проаналізувати обсяг повноважень замовника за особистими документами та даними з Єдиного державного реєстру юридичних осіб, фізичних осіб – підприємців та громадських формувань, що визначають повноваження представника.

У тому випадку, коли приватне підприємство колегіального характеру (двоє або більше власників) вирішило здобути кваліфікаційний електронний підпис, звернувшись до установи чи особи, яка надає електронні довірчі послуги, має подати документи, в яких було б зазначено повноваження колегіального підприємства та розподіл обов'язків кожного з наявних власників.

Зразок застосування електронного підпису в електронному документаційному забезпеченні зображено на рис1.

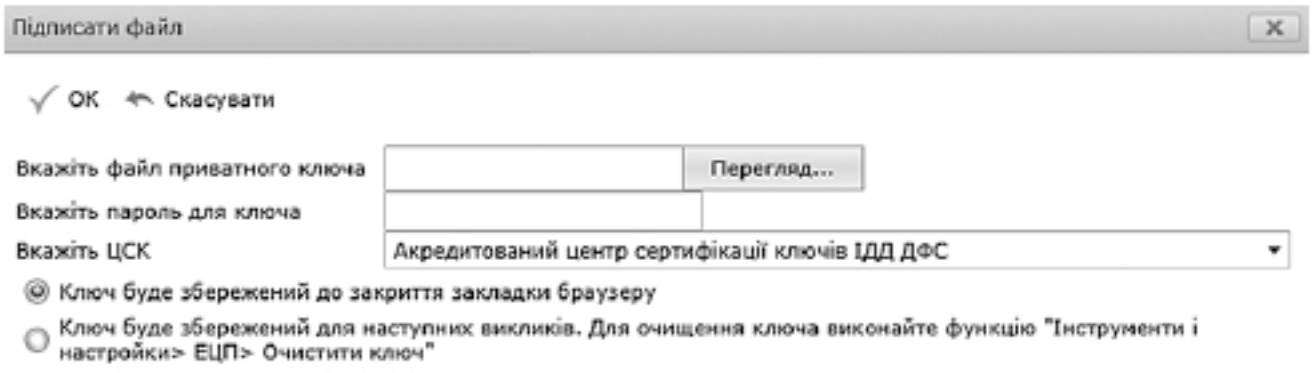


Рис.1.Застосування кваліфікаційного електронного підпису

Кваліфікаційний електронний підпис не лише надає інформацію про людину, яка підписала документ, але й дозволяє переконатись в тому, що сам документ не підроблений чи не піддавався стороннім змінам.

Завдяки КЕП можна вказати реальний час підписання документа. Дата зазначена у самому документі.

Крім того, КЕП забезпечує конфіденційність інформації, що міститься в документі, сприяє здійсненню шифрування документів.

Слід пояснити також значення терміну «сертифікат ключа».

Сертифікат ключа – це електронний документ. Він пов'язує дані для перевірки електронних підписів з певною особою. За допомогою цього документа підтверджується ідентичність тієї чи іншої особи. Завіряється сертифікат ключа електронним цифровим підписом надавача послуг – центром сертифікації ключів.

Відповідний "автограф" можна отримати в Акредитованому центрі сертифікації ключів (АЦСК) при фіскальній службі, або ж у будь-якій іншій організації, що видає ключі ЕЦП фізичним і юридичним особам. Однак у цьому випадку вже за гроші.

Юридичні особи можуть отримати ключ електронного цифрового підпису лише в АЦСК у межах області, тобто там, де були зареєстровані. Таке обмеження не стосується підприємців. Вони можуть отримати ключ цифрового підпису в АЦСК у будь-якому відділенні фіскальної служби

Отримати такий ключ може будь-хто. Для цього потрібно подати пакет документів до організації, яка видає ключі. Проте варто знати, що в кожному центрі сертифікації є свій список необхідних документів.

Наприклад, для отримання послуг КЕП фізичною особою у Акредитованому центрі сертифікації ключів необхідні такі документи:

1. заповнена та підписана Реєстраційна картка (для фізичної особи/фізичної особи-підприємця) встановленого зразка зі згодою на обробку персональних даних користувача. Потрібні 2 примірники;
2. копія паспорта користувача (1-2 сторінок, 3-6 – за наявності відміток. А також сторінка з відміткою про реєстрацію місця проживання);
3. копія картки платника податків, засвідчена підписом власника.

Загалом процедура отримання електронного підпису фізичною особою має займати не більше 15 хвилин.

Сфера застосування КЕП надзвичайно різноманітна. Електронний підпис може застосовуватись, зокрема, для подачі звітності онлайн до Пенсійного фонду України, Державної податкової адміністрації України, Державного комітету фінансового моніторингу, Державної митної служби, Національного депозитарію України тощо. До того ж, його використовують і під час заповнення електронних декларацій [1].

Разом з тим, сертифікати ключа можна використовувати для організації електронного документообігу, реєстрації та ідентифікації користувачів на різноманітних інформаційних ресурсах, а також для шифрування інформації, підписання будь-яких електронних документів тощо. При цьому необхідно провести ідентифікацію користувача, підтвердити цілісність даних, зафіксувати час підписання документа.

АЦСК не надає клієнтам носії ключової інформації, тому генерація особистих ключів виконується на клієнтські носії. Це, як правило – з'ємні флеш-носії, оптичні носії CD/DVD, захищені носії ключової інформації тощо.

Ідентифікацію особи здійснюють за паспортом. Посилені сертифікати відкритих ключів є чинними до 2 років від дати формування. До завершення цього терміну необхідно повторно отримати послуги ЕП, але це вже можна зробити дистанційно. Дізнатись про термін дії вже виданого посиленого сертифіката ЕП можна на офіційному інформаційному ресурсі АЦСК.

При зміні реквізитів(наприклад, податкової адреси), потрібно отримати нові ключі електронного підпису (ЕП) до моменту подання звітності. Разом з тим, слід переукласти Договір про визнання електронних документів з органом державної фіскальної служби області[3].

Отже, перехід від традиційного до електронного документообігу в системі документаційного забезпечення діяльності приватних підприємств має посилити вплив інформаційних процесів на різноманітні аспекти життєдіяльності приватного підприємства та

підвищити його конкурентоспроможність, створити умови наскрізного автоматизованого контролю на всіх етапах роботи з документами, що кардинально поліпшить якість роботи виконавців. В реалізації управлінської діяльності застосування кваліфікаційного електронного підпису (КЕП) має стати важливим засобом цієї роботи.

Список літератури

1. Кісельов А.П. Основи бізнесу: підручник для економ, спец. вузів. К.: Вища школа, 1998.191 с.
2. Про електронні довірчі послуги..Закон України від 14.01.2020 .№ 440 IX.URL:https://zakon.rada.gov.ua/laws/show/2155-19#Text(дата звернення: 18.12.2020).
3. Цигилик І.І. Основи підприємництва. К.: Центр учбової літератури, 2007. 224 с.

УДК 332.1:311.3

І. Свинаренко, магістр гр. ПА-19МЗ(ДС)
Центральноукраїнський національний технічний університет

ОСОБЛИВОСТІ УПРАВЛІННЯ ЕКОНОМІЧНИМ РОЗВИТКОМ КІРОВОГРАДСЬКОЇ ОБЛАСТІ В СУЧАСНИХ УМОВАХ

Стаття присвячена дослідженню особливостей управління економічним розвитком Кіровоградської області в сучасних умовах. Розглянуто основні проблеми економічного розвитку регіонів України, які є основною складовою економічної системи держави. Визначено основні підходи до використання економічного та природно-ресурсного потенціалу регіонів, які мають забезпечити досягнення якісно нового рівня ефективності і конкурентоспроможності економіки та життя населення. Наведено напрями удосконалення управління економічним розвитком Кіровоградської області.
управління, економічний розвиток, регулювання, регіон

Постановка проблеми. Актуальність теми полягає в тому, що в сучасних умовах розвитку механізмів державного управління економічним розвитком регіону є проведення моніторингу економічного розвитку регіону. Достовірність аналітичних висновків і якість аналізу залежить від якості інформаційних ресурсів моніторингу, що відкриває широкі можливості для забезпечення збалансованого соціально-економічного розвитку регіонів України.

На сьогоднішній день проблема соціально-економічного розвитку регіонів надзвичайно важлива, адже Україна перебуває у стадії пошуку власного підходу до вдосконалення існуючих підходів розвитку. Останнім часом проводиться активна робота щодо розробки програм соціально-економічного розвитку на регіональному рівні. Така спрямованість розвитку потребує нових підходів до використання економічного, людського та природно-ресурсного потенціалу регіонів, що забезпечить досягнення якісно нового рівня ефективності і конкурентоспроможності економіки та життя населення.

Аналіз останніх досліджень і публікацій. Різноманітні теоретичні засади та практичні механізми стратегічного управління регіональним розвитком України досліджували у своїх працях Балдич Н.І., Благодарний О.І., Будзяк В.М., Вакуленко В.М., Витвицька О.Д., Воротін В.Є., Данилишин Б.М., Дністрянський М.С., Долішній М.І., Клиновий Д.В., Константинов О.О., Коршикова І.О., Куйбіда В.С. та ін.

Мета й завдання дослідження. Метою дослідження є вдосконалення методики оцінки ефективності функціонування механізму регулювання процесів економічного розвитку регіону, створення організаційних механізмів, які б забезпечували постійну

підтримку ефективності функціонування регіональних органів влади, підвищення ефективності управління належного механізму регулювання економічного розвитку на регіональному рівні.

Завдання дослідження: вивчити теоретичний базис та основні елементи економічного розвитку регіону; проаналізувати рівень регіонального розвитку регіону; удосконалити механізми регулювання процесів економічного розвитку регіону; створити механізми регулювання економічного розвитку регіону; провести аналіз формування комплексних програм економічного розвитку регіону; запропонувати шляхи удосконалення інструментів економічного розвитку регіону.

Об'єктом дослідження є процес формування ефективних програм економічного розвитку регіону та виваженого управління економічним розвитком регіону, враховуючи існуючу спроможність регіону до економічного розвитку.

Предметом дослідження є теоретико-методичні засади прискорення розвитку Кіровоградської області на основі статистичного спостереження, дослідження закономірностей розвитку економічних процесів, які відбуваються в регіоні.

Методи дослідження: сукупність принципів, прийомів наукового пізнання, порівняння, систематизації та аналізу табличним та графічним методами.

Виклад основного матеріалу дослідження.

Ринкові умови вимагають переходу до стратегічного управління розвитком регіонів, яке виникло як відповідь на виклик і загрозу зовнішнього середовища: посилення його нестабільності, зростання глобалізації, загострення конкурентної боротьби. У загальному вигляді, стратегічне управління являє собою діяльність по розробці місії, найважливіших цілей України та способів їх досягнення, що забезпечують його розвиток у нестабільному зовнішньому середовищі шляхом зміни самого регіону і його зовнішнього середовища. По відношенню до регіонів України стратегічне управління створює базу для чіткого визначення позицій регіону та по відношенню до конкурентів і вимог споживачів дозволяє намітити заходи щодо поліпшення цих позицій [5].

У сучасних умовах проблема соціально-економічного розвитку України надзвичайно важлива в наш час, адже Україна перебуває у стадії пошуку власного підходу до вдосконалення існуючих підходів розвитку регіонів. Економічний розвиток регіону вимагає різнопланових структурних змін. До них відносяться модифікація факторів виробництва та більш ефективне використання всіх наявних ресурсів. Економічні процеси в регіоні, регулюються на місцевому та на загальнонаціональному рівнях. Економічний розвиток регіону забезпечується зростанням економічного добробуту населення регіону з найефективнішим використанням всіх наявних регіональних ресурсів. Економічний розвиток заключається в змінах технологічного прогресу, удосконалені якості продукції. Добробут населення є метою розвитку регіону. Розвиток регіону характеризується зміною і зростанням [6].

Аналіз сучасного стану механізмів державного управління економічним розвитком регіону необхідно здійснювати за допомогою реалізації моніторингу розвитку економічного стану регіонів України. Для побудови схеми моніторингу необхідно визначити всі елементи, які є основними і без яких неможливо її ефективне функціонування.

В системі моніторингу можна виділити перелік найважливіших базових показників і характеристик. Системою моніторингу передбачається формування системи інформаційної, яка необхідна для проведення аналізу економічного розвитку регіонів для забезпечення оцінки поточного стану і ходу реалізації державної регіональної політики з метою проведення економічних реформ в регіонах.

На сучасному етапі комплексний розвиток територій та реалізація стратегічних цілей і завдань їх розвитку досягається шляхом суспільної злагоди між органами влади і населенням. Моніторинг економічних процесів узгоджується в процесі реалізації стратегії регіонального розвитку і базується на основі консолідації регіонального співтовариства.

При проведенні моніторингу, діагностуються всі аспекти економічного розвитку регіону з метою виявлення основних тенденцій розвитку деяких видів діяльності, при цьому основною метою владних інститутів буде подолання диференціації територій за рівнем економічного розвитку. Моніторинг економічного розвитку регіону проводиться в основному для отримання необхідної інформації для коригування державної регіональної політики, а також подальшої розробки комплексних програм розвитку основних галузей і територій [2].

Моніторинг економічного розвитку регіонів використовується для кращого процесу прийняття управлінських рішень, тому він засновується на основі використання сучасних та ефективних методів аналізу, оперативних методів обробки інформації, використовуючи удосконалені нововведення програмного забезпечення. Фахівці, зайняті у сфері дослідження і обробки моніторингу повинні володіти усіма методами аналізу і прогнозу показників моніторингу та бути висококваліфікованими спеціалістами.

Основними завданнями моніторингу економічного розвитку регіонів є система методів економічного аналізу, що забезпечує реалізацію наступних етапів (рис. 1).

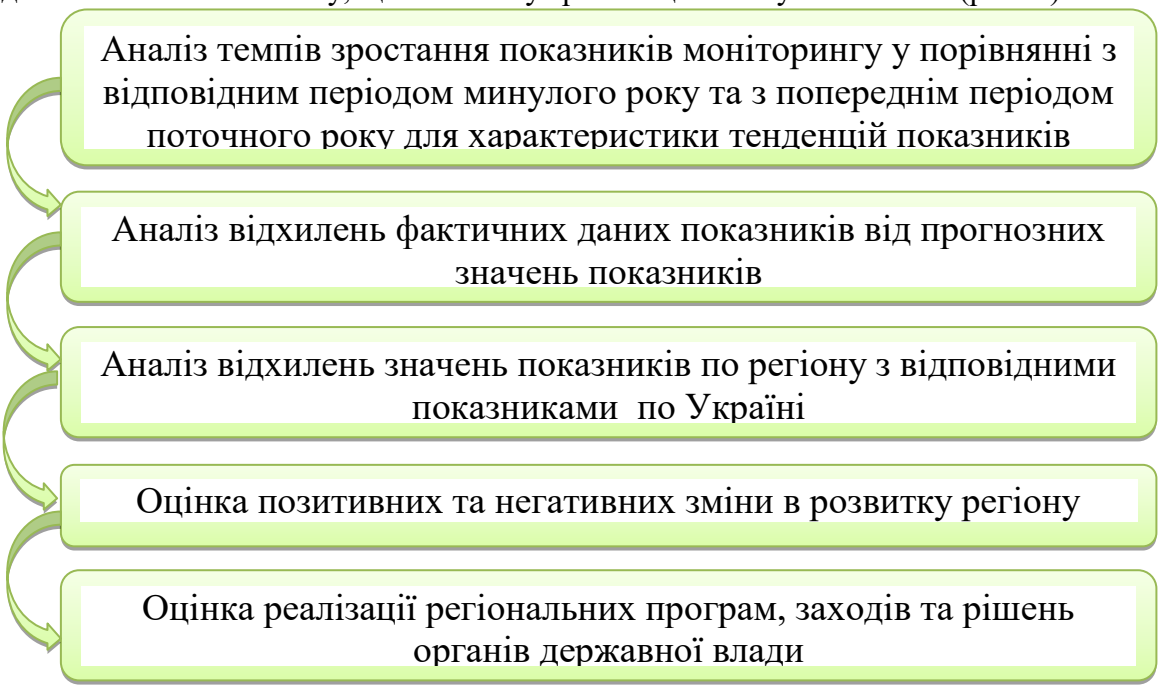


Рисунок 1 – Основні етапи моніторингу економічного розвитку регіонів

Джерело: побудовано автором

При побудові основної структури системи моніторингу необхідно орієнтуватися на використання функціонального підходу, з ієрархічною структурою, який забезпечить необхідне оперативне управління розвитком регіону з гнучкою системою та скоординованою взаємодію суб'єктів моніторингу. Завдяки такому моніторингу досягається ефективне управління регіональним розвитком на всіх рівнях. При нормативно-правовому регулюванні забезпечується поділ повноважень та визначення прав, обов'язків і відповідальності за надання інформації у встановлені терміни, та подання достовірної інформації з дотриманням методичних рекомендацій, установленого порядку та регламент проведення моніторингу.

Система моніторингу економічного розвитку регіонів, яка ґрунтується на основі системного підходу є надійним джерелом отримання достовірної інформації про економічні процеси, що відбуваються в регіонах, передбачає прийняття виважених рішень щодо усунення негативних явищ, які виявляються в процесі обробки інформації. Таким чином, на основі сформованих статистичних даних органи влади проводять моніторинг економічного розвитку.

Процедуру проведення моніторингу та оцінки його результативності визначено Кабінетом Міністрів України для реалізації державної регіональної політики. Оцінка моніторингу на основі наявних офіційних статистичних даних передбачає періодичне відстеження відповідних показників, інформації центральних органів виконавчої влади, органів місцевого самоврядування. Це відбувається шляхом порівняння запланованих цільових значень даних з офіційно отриманими у ході моніторингу оцінки результативності виконання результатів програми.

На теперішній час для розвитку економіки в області є дві особливо важливі галузі промисловості у розвитку промислового потенціалу. Це машинобудування та харчова промисловість. Цими галузями забезпечується вагома частка валової доданої вартості. Продукція цих галузей промисловості займає вагому частку товарного експорту області.

Введення глобальних технологічні змін у харчовій промисловості повинно сприяти розвитку виробництва екологічно чистих харчових продуктів з високої якості шляхом забезпечення маркетингової підтримки у ході реалізації цієї продукції. Необхідно забезпечити фінансування участі провідних виробників продукції найвищої якості у міжнародних виставках та ярмарках.

Забезпечити формування екологічно та економічно збалансованого сільськогосподарського комплексу шляхом ефективного використання існуючого в області природно-ресурсного потенціалу. Необхідно забезпечити підтримку постійного розвитку сіл і селищ області, створити комфортні умови для життєдіяльності людства, які б підвищували добробут населення області. На постійній основі забезпечувати нарощення виробництва високоякісної продукції, формувати замкнені цикли виробництва сільськогосподарської продукції шляхом вирощування екологічно чистої продукції та сприяти розвитку органічного виробництва.

В аграрному секторі Кіровоградська область займає значний ресурсний потенціал при формуванні високотехнологічного аграрного виробництва, який може здійснювати досить вагомий внесок у забезпечення продовольчої безпеки як регіону так і країни в цілому. Це в свою чергу розширить сировинну базу для харчової промисловості та посилить експортних позицій України [7].

В першу чергу основним завданням необхідно підвищити ефективність використання земельних площ, раціонально використовуючи сільськогосподарські угіддя. Це буде сприяти збільшенню виробництва сільськогосподарської продукції, забезпечить населення своєю якісною продукцією та розширить спроможність для нарощування експортного потенціалу галузі [4].

З метою поліпшення доступу сільськогосподарської продукції на ринок, зменшення втрат при її зберіганні та транспортуванні забезпечити розвиток інфраструктури аграрного ринку, сформувати ринкові ціни на продукти харчування [1].

Впроваджувати у практику господарювання інноваційних технологій на основі формування і розвитку аграрних технологічних парків та бізнес-інкубаторів. Необхідна підтримка розвитку сільського «зеленого туризму» як виду підприємницької діяльності, що буде сприяти утриманню на селі активного населення, поліпшенню благоустрою сільських садиб, вулиць та сіл в цілому.

Розробка комплексних програм розвитку окремих територій необхідна, щоб створювати умови для продуктивного використання існуючих переваг регіонів, беручи за основу забезпечення та покращення їх конкурентоспроможності.

Основним фактором програми розвитку Кіровоградської області є розташування по відношенню до інших, природні умови та особливості у економічній сфері. За їх розробку беруться при необхідності прискорення економічного розвитку області, підвищення ефективності ресурсів, які вже освоєні, так і нових. Кожний регіон України має в розробці конкретні програми, які містить вирішення конкретних питань галузевого або регіонального характеру. Отже, найважливіше завдання – втілення в життя програм міжрегіонального рівня, в яких вирішуватимуться питання освоєння й використання ресурсів згуртованих

спільними інтересами, цілеспрямованого розвитку науково-виробничих і виробничо-технологічних комплексів, створення виробничої та транспортної інфраструктури, розвитку регіональних ринків та інформаційних структур, підвищення рівня життя тощо.

Основні завдання, які необхідно виконати в процесі реалізації програми: підвищення життєвого рівня населення; забезпечення ефективного розвитку галузей спеціалізації регіону – сільського господарства, харчової і легкої промисловості, сільськогосподарського машинобудування, видобутку і переробки мінералів; технологічне оснащення і модернізація виробництва; приведення промислового виробництва у відповідність до ресурсної бази з її потребами; удосконалення ланок сільського господарства, створення і розширення в галузі м'ясного скотарства; створення нових підприємств, розширення і переоснащення діючих підприємств в галузі сільського господарського, формування господарського комплексу з узгодженістю економічних зв'язків; збільшення підприємств, що випускали б електронну техніку, електропобутові товарів тощо [3].

Практична значущість проведених досліджень ґрунтується на організаційно-економічній забезпеченості конкурентоспроможності та економічної безпеки регіону, що дозволило виявити найбільш проблемні питання, на основі вдосконалення програмного управління економічного розвитку регіону, що можуть бути впроваджені на прикладі Кіровоградської області.

Висновки. Отже, визначення напрямів стратегії розвитку регіону є актуальними аспектами вирішення проблеми. Стратегії розвитку регіону виокремлює нові положення щодо організації стратегічного управління регіону, регулює і розвиває економіку на регіональному рівні. Здійснюючи управління регіоном місцева влада, в межах своїх повноважень, керує територіальним регулюванням економічних процесів, який є головним інструментом. Стратегія розвитку регіону розглядає можливі шляхи та пріоритети в досягненні стратегічної мети, що відображає головний напрям господарської діяльності. Комплексні програми на регіональному рівні виступають основним інструментом, що сприяє здійснює конкретні оперативні дії у напрямку перспективи, узгоджуючи із загальною довгостроковою стратегією.

За результатами проведеного аналізу можна зробити висновок, що основними секторами економіки Кіровоградської області є виробництво сільськогосподарської продукції, розвиток промисловості, будівництво та зовнішньоекономічна діяльність. Цими галузями забезпечується найбільша частка валової доданої вартості. В аграрному секторі Кіровоградська область має суттєвий ресурсний потенціал для формування вагомого внеску у забезпечення продовольчої безпеки країни та підкріплює експортні позицій України.

Список літератури

1. Державне управління регіональним розвитком України : монографія / Воротін В. Є. та ін. ; за заг. ред.: В. Є. Воротіна, Я. А. Жаліла. Київ : НІСД, 2010. 288 с.
2. Константинов О.О. Основні підходи до реалізації сучасних механізмів державного управління соціально-економічним розвитком регіону в Україні. Державне управління: удосконалення та розвиток. 2014. № 12. URL: http://www.dy.nayka.com.ua/?op=1&z=1011 (дата звернення: 16.10.2020)
3. Небава М. І., Ткачук Л. М. Управління регіональним розвитком Електронний навчальний посібник Система основних загальноекономічних показників розвитку регіону та аналіз його економічного потенціалу: веб-сайт. URL: https://web.posibnyky.vntu.edu.ua/fmib/25nebava_ upravlinnya_ regionalnym_ rozvytkom/5_3.html (дата звернення: 08.11.2020)
4. Про державне прогнозування та розроблення програм економічного і соціального розвитку України: Закон України від 16 жов. 2012 р. №5463-VI. URL: https://zakon.rada.gov.ua/ laws/show/1602-14#Text
5. Соціально-економічний потенціал сталого розвитку України та її регіонів: національна доповідь. Лібанова Е.М. та ін. ; заред. акад. НАН України Е.М. Лібанової, акад. НААН України М.А. Хвесика. Київ: ДУІЕПСР НАН України, 2014. 776 с.
6. Стоянець Н.В. Методологічні аспекти соціально-економічного розвитку регіону. Науковий вісник Мукачівського державного університету. Сер. Економіка. 2015. № 2(4). Ч. 2
7. Управління комплексним розвитком агропромислового виробництва і сільських територій : монографія. Саблук П. Т. та ін. ; за ред. П. Т. Саблука, М. Ф. Кропивка. Київ : ННЦ ІАЕ, 2011. 454 с.

УДК 651.011.42.

В. Бондаренко, магістр гр. ІС-19М
Центральноукраїнський національний технічний університет

ОРГАНІЗАЦІЯ АРХІВНОГО ЗБЕРІГАННЯ ДОКУМЕНТАЦІЇ НА ПІДПРИЄМСТВІ

У статті розглянуто особливості організації архівного зберігання документації на підприємстві. Звернута увагу на порядок складання номенклатури справ підприємства. Встановлено, що процес підготовки передання документа на архівне зберігання має пройти декілька обов'язкових етапів: експертизу (оцінку) наукової та практичної цінності документів; описи справ; оформлення справ; опис документів постійного і довготривалого зберігання; забезпечення їх збереження; передачу справ до архіву підприємства або до обласного архіву.
інформаційна діяльність, документ, документообіг, документаційне забезпечення, архів, номенклатура справ, опис справ

Постановка проблеми. У сучасному інформаційному суспільстві відбувається постійне збільшення інформаційних потоків, у тому числі і у вигляді документів. Посилені інформаційні документальні потоки спостерігаються у сфері підприємницької діяльності котрі все більше потребують прискорення під час їхнього створення, обробки, передачі та подальшого зберігання. Саме етап архівного зберігання документації є важливим і відповідальним оскільки є завершальним етапом процесу діловодства.

Аналіз останніх досліджень і публікацій. Дослідженню проблем організації архівного зберігання документації на підприємствах, установах і організаціях у своїх працях приділяли увагу ряд українських науковців: Н.Анодіна[1], Р.Друзін[2], С.Кулешов[4;5], Ю.Палеха[6;7], І.Сокирник[9], спільній праці О.Кірічок, В.Корбутяк, В.Процюк та К.Дубич[3] та ін.

Метою статті є розгляд організації архівного зберігання документації на підприємстві.

Виклад основного матеріалу. Завершальним етапом процесу діловодства є підготовка виконаних документів до архівного зберігання на підприємстві та передача деяких з них до обласного архіву. Документи організації, що утворилися в процесі діловодства, надалі або залишаються на тривалому архівному зберіганні або зберігаються деяких час (короткі терміни) на підприємстві, а потім знищуються. Процес підготовки передання документа до архіву має пройти декілька обов'язкових етапів:

- експертизу (оцінку) наукової та практичної цінності документів;
- описи справ;
- оформлення справ;
- опис документів постійного і довготривалого зберігання;
- забезпечення їх збереження;
- передачу справ до архіву установи, тобто у відомчий архів.

Враховуючи, що на кожній справі вказують її індекс відповідно до затвердженої на підприємстві номенклатурою. Той й передача документів (опис) з усіх структурних підрозділів підприємства має здійснюватися відповідно до номенклатури. Для справ, що містять особливо цінні документи (протоколи, накази) складається та систематично ведеться внутрішній опис на початку справи. Номенклатура справ (далі НС) – це систематизований перелік справ який в обов'язковому порядку заводиться на підприємствах із зазначенням термінів їх зберігання справ. Номенклатура справ складається з метою обґрунтованого розподілу документів і формування справ, забезпечення пошуку документів і обліку справ. НС є класифікаційним довідником і використовується при побудові інформаційно-пошукової

системи.

НС бувають наступних видів: примірна, типова, номенклатура справ структурного підрозділу, зведена номенклатура справ підприємства. Примірна НС встановлює примірний склад справ для однорідних за характером діяльності, але різних за структурою організацій із зазначенням їх індексу і носить рекомендаційний характер. Типова номенклатура справ складається для однорідних за характером діяльності і структурі організацій. Вона встановлює типовий склад справ з єдиною системою індексації в галузі і є нормативним документом.

Номенклатуру справ структурного підрозділу розробляє його керівник разом з діловодною службою. НС відділу роздруковується в 3-х прим., підписується керівником відділу, узгоджується з архівом підприємства та передається для зберігання та використання в роботі: 1-й екз. - канцелярії; 2-й екз. - відділу; 3-й екз. - в архів підприємства.

Зведена номенклатура для підприємства складається службою документаційного забезпечення на основі номенклатури справ структурних підрозділів. Першим розділом НС завжди ставиться діловодний підрозділ або канцелярія, а далі за номером присвоєного індексу відділу (Наприклад 05- бухгалтерія, 06 – кадри і т.п.). Згідно діючого законодавства, НС підприємства (зведена) та її структурних підрозділів оформлюють наступним чином: «У графі 1 проставляється індекс кожної справи. Індекс справи структурного підрозділу складається з індексу структурного підрозділу установи (за штатним розписом або класифікатором структурних підрозділів) та порядкового номера справи в межах підрозділу. Наприклад: 05-10, де 05 - індекс самостійного відділу, 10 - порядковий номер справи, або 04.1-08, де 04.1 - індекс відділу у складі управління, 08 - порядковий номер справи.

У графу 2 включаються заголовки справ (томів, частин), які мають чітко, у стислій узагальненій формі відображати склад і зміст документів справи. <….>

Графа 3 номенклатури заповнюється наприкінці календарного року, коли відома кількість сформованих томів, частин справи.

У графі 4 номенклатури зазначаються строки зберігання справ, номери статей за типовими (галузевими) переліками документів із зазначенням строків їх зберігання, типовими і примірними номенклатурами справ.

У графі 5 «Примітка» робляться позначки про перехідні справи; про справи, що ведуться в електронній формі; про посадових осіб, відповідальних за формування справ; про передачу справ до архіву установи чи інших установ для їх продовження тощо»[8].

Окрім того, НС підприємства узгоджується з експертно-перевірочною комісією (далі - ЕПК) обласного державного архіву, куди документи направляються на державне зберігання, і затверджуються керівником організації. Експертиза цінності документів постійного і тимчасового термінів зберігання має проводитися щорічно. На експертні комісії, щорічного відбору документів на зберігання покладається: розгляд річних розділів справи постійного, довготривалого зберігання, в тому числі по особовому складу, актів про виділення до знищення документів і справ, не підлягають подальшому зберігання, про невиправному пошкодженні документів постійного зберігання і про не виявленні справ, що підлягають передачі на державне зберігання; питань про прийом на відомче зберігання документів особового походження; підготовка і внесення на розгляд ЕПК пропозицій щодо встановлення і зміни термінів зберігання документів і т.п. У результаті роботи експертної комісії утворюються чотири групи документів з різними термінами зберігання:

- постійного зберігання в державних архівах;
- тимчасового зберігання у архіві підприємства (понад 10 років);
- тимчасового зберігання (до 10 років);
- підлягають знищенню в зв'язку з закінченням терміну зберігання[8].

За результатами експертизи цінності документів складаються описи справ постійного, тимчасового (понад 10 років) термінів збереження і документів по особовому складу, а також акти про виділення до знищення справ з вичерпаним терміном зберігання (до 10 років включно). Описи справ постійного, тимчасового терміну зберігання (понад 10 років та

документів з особового складу, а також акти про виділення справ до знищення розглядаються на засіданні експертної комісії організації та узгоджуються з відомчим архівом. Справи тимчасового (до 10 років включно) строку зберігання можуть бути знищені тільки після того, як описи справ постійного, тимчасового (понад 10 років) строку зберігання та по особовому складу за відповідний період затверджені і передані у відомчий архів організації. Опис є обліковим документом і основною частиною науково-довідкового апарату архіву, забезпечує оперативний пошук документів. Опис складається у трьох примірниках: один передається разом із справами у відомчий архів, другий - додається в якості підстави до протоколу засідання експертної комісії, третій - залишається в якості контрольного екземпляра на підприємстві. На справи постійного, тимчасового (понад 10 років) термінів збереження і по особовому складу складаються окремі описи. Не підлягають здачі на державне зберігання справи з тимчасовим (до 10 років включно) терміном зберігання після закінчення встановленого терміну зберігання включаються в акт про виділення документів до знищення. Не допускається знищення документів до повного закінчення термінів їх зберігання. Для виключення передчасного знищення документів необхідно дотримувати наступне правило: справи включаються в акт про знищення, якщо передбачений у них термін зберігання закінчився до 1 січня того року, в якому складено акт. Закінчені діловодством справи постійного, тимчасового (понад 10 років) строку зберігання та з особового складу після закінчення календарного року, в якому вони заведені, повинні бути підготовлені до передачі у відомчий архів. Архівна підготовка справ включає дві процедури: опис та оформлення справ.

Оформлення справи – це роботи з його переобліку, нумерації аркушів, внутрішнього опису документів. Починається воно з моменту запевнення справи в діловодстві і завершується в процесі підготовки його до передачі у архів. Оформлення справ проводиться працівниками служби діловодства. У залежності від термінів зберігання проводиться повне або часткове оформлення справ. Повному оформленню підлягають справи постійного, довгострокового зберігання (понад 10 років) і з особового складу. Справи тимчасового (до 10 років включно) зберігання підлягають частковому оформленню, їх допускається зберігати у швидкозшивачах, без внутрішньої пересистематизації документів, без нумерації аркушів. «Справи постійного і тривалого зберігання підлягають повному оформленню, яке передбачає: підшивання в обкладинку з твердого картону; нумерацію аркушів у справі; складання підсумкового напису; складання внутрішнього опису документів; оформлення обкладинки справи.

Обкладинка справ постійного і тривалого зберігання оформляється за встановленою формою. Після закінчення діловодного року до написів на обкладинках справ постійного і тривалого зберігання вносять необхідні уточнення, перевіряють відповідність заголовків справ на обкладинці змісту підшитих документів, у разі необхідності до заголовку справи вносяться додаткові відомості (проставляють номери наказів, протоколів, вказують види і форми звітності тощо).

Дата на обкладинці має відповідати року заведення і закінчення справи; у справі, що містить документи років, що передували рокові утворення справи, під датою робиться запис : є документи за ___роки)»[9].

Після завершення справ у діловодстві структурні підрозділи підприємства зобов’язані описувати документи постійного та тривалого (понад 10 років) зберігання та справи з кадрових питань (особового складу) – через рік. Описи справ структурного підрозділу установи складаються щороку за встановленою формою[8].

«Під час формування справ слід дотримуватися таких загальних правил:

- вміщувати у справи тільки виконані документи відповідно до заголовків справ у номенклатурі;
- групувати у справи документи, виконані протягом одного календарного року, за винятком перехідних справ та судових справ (ведуться протягом кількох років до їх завершення), особових справ (формуються протягом періоду роботи особи в цій установі),

документів виборчих органів та їх постійних комісій, депутатських груп (формуються за період їх скликання), документів навчальних закладів, що характеризують навчально-виховний процес (формуються за навчальний рік), документів театрів, що характеризують сценічну діяльність (формуються за театральний сезон), справ фільмів, рукописів, історій хвороб;

- вміщувати у справи лише оригінали або у разі їх відсутності засвідчені в установленому порядку копії документів;
- не допускати включення до справ чорнових, особистих документів, розмножених копій та документів, що підлягають поверненню;
- до справи включати документи тільки з одного питання або групи споріднених питань, що становлять єдиний тематичний комплекс;
- окремо групувати у справи документи постійного, тривалого (понад 10 років), тимчасового зберігання;
- за обсягом справа постійного та тривалого (понад 10 років) зберігання не повинна перевищувати 250 аркушів (не більше 40 мм завтовшки)»[8].

Порядок передачі справ до архіву має свої особливості. У відомчий архів передаються справи постійного, тимчасового (понад 10 років) зберігання та з особового складу. Передача справ здійснюється лише з описів та відповідно до складеного завідувачем архівом графіком, погодженим з керівником структурних підрозділів і затвердженим керівником організації. Разом зі справами до архіву передаються реєстраційно-контрольні картотеки діловодної служби установи. Приймаючи справи, співробітник архіву ретельно звіряє кожну справу з описом, перевіряє правильність формування та оформлення справи. Завідувач архівом розписується у прийнятті справ на всіх примірниках річних розділах опису, вказує дату прийому та кількість прийнятих справ. Один примірник річних розділів описів повертається здавачеві, решта залишається в архіві. Взаємодія державних архівів із сучасними комерційними підприємствами здійснюється на договірній основі. У договорі закріплюються зобов'язання сторін, склад переданих документів, порядок і терміни передачі документів на постійне або депозитне зберігання.

Організація може скоротити термін збереження документів у своєму відомчому архіві до передачі їх на державне зберігання у випадках: припинення діяльності, нестабільності діяльності, відсутності умов для зберігання документів, бажання самої організації. При здачі справ на державне зберігання підприємства надає в державний архів:

- довідку на ім'я керівництва державного архіву з зазначенням назви підприємства, загальної кількості справ і крайніх дат документів;
- описи у трьох примірниках, затверджені архівним відділом або уповноваженою особою;
- історичну довідку організації, якщо справи здаються на державне зберігання вперше;
- довідку про неповну збереження документів (якщо будь-які справи втрачені).

Потім справи шифруються. Шифровка включає в себе вказівку на обкладинці справи номера фонду, номери опису, номера справи. Звірені з описом і зашифровані справи пов'язують в архівні зв'язки. Здача справ оформлюється актом. Підприємство яке здає документи і державний архів розписуються на всіх примірниках описів та акту здачі документів. Два примірники опису та один примірник акта залишаються в державному архіві, третій примірник опису та другий примірник акта повертаються організації і зберігаються постійно в діловодній службі.

Висновки.Таким чином, розглядаючи особливості організації архівного зберігання документації на підприємстві ми дійшли висновку, що підготовка виконаних документів до архівного зберігання є завершальним етапом процесу діловодства. Документи організації, що утворилися в процесі діловодства, надалі або залишаються на тривале архівне зберігання, або зберігаються на короткі терміни, а потім підлягають знищенню в установленому порядку.

Процес підготовки передання документа до архіву має пройти декілька обов'язкових етапів: експертизу (оцінку) наукової та практичної цінності документів; описи справ; оформлення справ; опис документів постійного і довготривалого зберігання; забезпечення їх збереження; передачу справ до архіву підприємства або до обласного архіву.

Список літератури

1. Анодіна Н. Н. Документооборот в организации. Изд-во: Омега-Л, 2007. 172с.
2. Друзін Р.В. Діловодство в банківських установах. URL: http://b-ko.com/book_376.html (дата звернення: 1.10.2020).
3. Кірічок О.Г.,Корбутяк В.І.,. Процюк В.І, Дубич К.В. Документування у менеджменті: підручник. К. : Центр навчальної літератури, 2003. 216 с.
4. Кулешов С.Г. Загальне документознавство. 2012. 124 с
5. Кулешов С.Г. Управлінське документознавство: навч. посібник. К.: ДЛККК лМ, 2003. 57с.
6. Палеха Ю. І. Організація сучасного діловодства. К.:Кондор, 2007. 194 с.;
7. Палеха Ю.І. Документування в підприємницькій сфері (зі зразками сучасних документів) : навч. посіб. К. : Ліра-К, 2010. 509 с.
8. Про затвердження Правил організації діловодства та архівного зберігання документів у державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях: Наказ Міністерства юстиції України від 18.06.2015р. №1000/5. Дата оновлення:07.17.11.2018. URL: https://zakon.rada.gov.ua/laws/show/z0736-15#Text (дата звернення: 1.10.2020).
9. Сокирник І.В. Діловодство конспект лекцій. URL :https://buklib.net/books/21961/ (дата звернення: 1.10.2020).

УДК 012:025.5

С. Геворкян, магістр гр. ІС-19М (1,4)
Л. Глєбова, канд. філ. наук, доцент
Центральноукраїнський національний технічний університет

ВТОРИННІ ІНФОРМАЦІЙНІ РЕСУРСИ БІБЛІОТЕКИ УНІВЕРСИТЕТУ

У статті розглянуто поняття вторинних документів та вторинної інформації, наведено один із можливих підходів до класифікування вторинних інформаційних продуктів, названо складові інформаційного ресурсу бібліотеки Центральноукраїнського національного технічного університету.
інформація, документ, вторинний документ, вторинна інформація, бібліотека, вторинні інформаційні ресурси

Постановка проблеми. Не потребує жодних доказів факт глобальної трансформації діяльності інформаційних установ на нинішньому етапі. Це стосується змін у роботі установ та організацій як у нашій країні, так і у країнах Заходу та Європи, хоча, звісно ж, ідеться тут про процеси, які мають у різних країнах відмінні риси, різну інтенсивність протікання, що зумовлено почасти низкою об'єктивних причин. Бібліотеки ж, одна з найдавніших інформаційних установ, у нашій країні знаходяться у авангарді цих змін, і, за влучним висловом Л.Й.Костенка, «мета та сутність трансформаційних процесів у бібліотеках в умовах переходу від індустріального суспільства до суспільства знань: вони мають забезпечити розробку, створення та впровадження наукоємних (насамперед, інтелектуальних) інформаційних технологій» [7].

Аналіз останніх досліджень та публікацій.

Генерація власних вторинних інформаційних ресурсів та надання доступу до придбаних чи передплачених баз вторинних документів наразі належить до пріоритетних напрямків у роботі бібліотечної установи. На цьому справедливо наголошує дослідник

Л.Костенко, переконуючи: «Інтегрований технологічний цикл, що передбачає бібліографування, реферування, підготовку інформаційно-аналітичних і прогностичних матеріалів, проведення бібліо-, інформо- та наукометричних досліджень є передумовою, необхідною для досягнення головного кінцевого результату – екстракції зі сховищ даних нових знань, що в явному вигляді в них не містяться» [7].

Вивченню окремих аспектів створення та функціонування вторинних інформаційних ресурсів присвячено окремі розділи у фундаментальних дослідженнях Н.Кушнаренко та В.Удалової [9], Г. Швецової-Водки [11; 12] та ін.

Вивченням інформаційного ресурсу бібліотеки ЦНТУ займаються викладачі кафедри історії, археології, інформаційної та архівної справи нашого університету (В.Барабаш та ін.) у межах розробки теми науково-дослідної роботи «Функціонування інформаційних установ та їх ресурси». Результати їх наукових пошуків представлено, зокрема, й у наукових публікаціях за темою [2; 3; 4]. Важливу інформацію про діяльність бібліотеки університету знаходимо в історичному нарисі про технічну освіту [10].

Підґрунтям даного дослідження, окрім названих наукових розвідок, є насамперед базовий Закон України «Про інформацію» [1].

Проте окреме дослідження вторинних інформаційних ресурсів бібліотеки Центральноукраїнського національного технічного університету ще не проводилося, що і зумовлює актуальність подальших пошуків в означеній царині.

Мета й завдання дослідження. Метою роботи є дослідження особливостей вторинних інформаційних ресурсів установи, їх складу та структури.

Для досягнення поставленої мети визначено такі завдання:

- Визначити особливості вторинних документів та документів із вторинною інформацією.
- Розглянути видову різноманітність вторинних документів та підходи до їх класифікації.
- Дослідити компоненти вторинного інформаційного ресурсу бібліотеки ЦНТУ.

Об'єктом дослідження є вторинні інформаційні ресурси бібліотеки.

Предметом дослідження є вивчення особливостей складу та структури вторинного інформаційного ресурсу бібліотеки Центральноукраїнського національного технічного університету.

Виклад основного матеріалу.

Базовими поняттями комунікаційно-інформаційної сфери є поняття *інформація* та *документ*. Вагомими та вихідними вважаємо їх і в контексті і даного дослідження. Єдиного загального визначення даних понять не існує. Базовий Закон України «Про інформацію» трактує ці поняття так: «Під інформацією розуміються документовані або публічно оголошувані відомості про події та явища, що відбуваються у суспільстві, державі та навколишньому природному середовищі» [1]. «Документ – це передбачена законом матеріальна форма одержання, зберігання, використання і поширення інформації шляхом фіксації її на папері, магнітній, кіно-, відео-, фотоплівці або іншому носієві» [1].

Визначення поняття *документ* було детально розглянуто у працях провідних фахівців у сфері інформаційної, бібліотечної та архівної справи, як-от: Н.Кушнаренко, С.Кулешова, Г.Швецова-Водки та ін.

У контексті вивчення інформаційних ресурсів будь-якої бібліотечної установи вагомим є окреслення ще одного важливого блоку понять – *вторинний документ* та *вторинна інформація*. Фахівці справедливо стверджують, що між цими поняттями є відмінності, відтак вторинний документ та документ із вторинною інформацією – не одне і те ж саме. «Сказати, що деякі документи відображають інформацію, яка не була раніше представлена в інших документах, можна лише умовно, щодо певних видів документів. Насправді створення документа людиною спирається на певні знання, отримані раніше з інших документів. Тому будь-який документ ґрунтується на інших документах» [12]. У якості прикладу дослідниця називає такі «класично» первинні документи з первиною

інформацією, як дисертація та наукова монографія, наголошуючи на тому, що вони, безумовно, спираються на праці інших науковців у досліджуваній царині. «Таким чином, новий (первинний) документ теж є результатом переробки інших документів», – справедливо вважає Г.Швецова-Водка [12]. Науковиця доходить висновку, що поділяти документи на первинні та вторинні можна лише досить умовно. «Документи, які потрапляють в інформаційну сиситему «на вході» і піддаються аналітико-синтетичній переробці інформації називаються первинними, а ті, що створюються системою в результаті обробки первинних документів і передаються споживачам інформації «на виході із системи», – вторинними. Поділ документів на первинні та вторинні є у даному випадку умовним, тому що він залежить від того місця у певній системі, яке займає той чи інший документ…Щоб ліквідувати таку невизначеність у бібліотечно-бібліографічній справі прийнято вважати первинним тільки такі документи, які не дають інформацію про інші документи, а точніше, не призначаються для їх заміни. При цьому вторинними вважаються документи, у яких представлена інформація про інші документи» [12].

Дослідниці Н.Кушнаренко та В.Удалова у підручнику «Наукова обробка документів» розглядають такі види вторинних документів (інформаційних продуктів, інформаційної продукції): бібліографічні документи: каталоги, бібліографічні посібники (покажчики, списки, огляди) тощо; реферативні: реферативні збірники, реферативні журнали, інформаційний листок та ін.; оглядово-аналітичні: огляди (аналітичні, інформаційні тощо), тематичні підбірки, дайджести та ін. [9].

Натомість же Г. Швецова-Водка на позначення вторинних документів та вторинних інформаційних ресурсів використовує поняття «інформаційні документи, інформаційні видання», «інформаційна література». «Отож, під назвою «інформаційна література» або «інформаційні документи», «інформаційні видання» розуміють такі джерела, які містять інформацію про первинні документи. Серед них розрізняють «бібліографічні» – які дають відомості про документи у вигляді бібліографічного опису і анотацій, «реферативні», що дають характеристику первинного документа у вигляді реферату, і «оглядові» – дають огляд декількох первинних документів. Такий підхід став загальноприйнятим… Однак він не відповідає теоретичним поглядам спеціалістів відносно бібліографії та бібліографічної інформації, відповідно до яких бібліографічна інформація не обмежується способами бібліографічного опису і анотації. Для бібліографознавців усі документи, що передають інформацію про інші документи будь-яким способом, є бібліографічними. Тому не можна називати «бібліографічними» тільки документи з бібліографічним описом і анотацією. Швидше за усе, усі вторинні документи слід було б вважати бібліографічними» [12]. Як випливає із вищезазначеного, існує думка, що усі вторинні інформаційні документи, а відтак, вважаємо, і ресурси варто іменувати бібліографічними.

Існування будь-якої бібліотечної системи неможливе без створення бібліографічного (вторинного) інформаційного ресурсу. «Особливістю КБР є переважання серед них бібліотечно-каталожних БП. Практично кожна бібліотека починає автоматизацію бібліотечно-бібліографічної діяльності зі створення власного електронного каталогу, що є головним різновидом бібліотечно-каталожних БП. Крім того, до бібліотечно-каталожних БП належать електронні каталоги інших бібліотек, доступні для користування через Інтернет; зведені каталоги, створені зусиллями декількох установ, та інші бібліографічні посібники, які відображають склад певного фонду (наприклад, електронний аналог традиційного «бюлетеня нових надходжень»)» [11]. Електронний каталог бібліотеки ЦНТУ наразі поки що є оф-лайновим інформаційним продуктом.

Отже, вторинний інформаційний ресурс бібліотеки ЦНТУ складають:

1) Власний (створений) вторинний інформаційний ресурс:
- Електронний каталог;
- Карткові каталоги;
- Бібліографічні документи (списки, покажчики);
- Оглядово-аналітичні документи (огляди нових надходжень, періодичних

видань; віртуальні книжкові виставки);

2) Придбані чи передплачені вторинні інформаційні ресурси (доступ до баз даних) [13].

У зв'язку з проблемою створення вторинних інформаційних ресурсів у бібліотечних установах та екстракцією знань дослідник Л.Костенко виокремлює п'ять етапів наукової обробки документів (наукоємних технологій екстракції нових знань): 1. Аналітико-синтетична обробка первинної інформації в бібліографічну; 2. Підготовка реферативної інформації; 3. Створення прогностичних та оглядово-аналітичних документів; 4. Бібліо-, інформо- та наукометричні дослідження, у тому числі класифікація, кластеризація документів; 5. Витягнення, здобуття нових знань на основі наявних інформаційних ресурсів. Він справедливо наголошує, що «п'ятий етап наукової обробки документів сьогодні не реалізовано, проводяться дослідження та експерименти. Однак, саме він забезпечить входження бібліотек у суспільство знань у якості системоутворюючої ланки інформаційної сфери суспільства, сприятиме їх трансформації з відносно автономних елементів інфраструктури, що сьогодні вважається допоміжною, в інформаційні серцевини виробничих, наукових, освітянських і культурологічних структур» [7].

Висновки. Отож, бібліотекою Центральноукраїнського національного технічного університету проводиться значна робота у напрямку підготовки вторинних інформаційних продуктів, що свідчить про високу кваліфікацію та професіоналізм бібліотечних працівників даного структурного підрозділу ЗВО та репрезентує чітке усвідомлення перспектив подальшого розвитку інформаційних установ даного типу.

Список літератури

1. Інформаційне законодавство: Збірник законодавчих актів. У 6 т. / За заг. ред. Ю.С. Шемчученка, І.С. Чижа. Т.1. Інформаційне законодавство. К.: Юридична думка, 2005. 116 с.
2. Барабаш В. А., Глєбова Л. В. Інформаційний ресурс бібліотеки університету як фактор формування ціннісних орієнтацій майбутніх фахівців // Соціум. Документ. Комунікація: збірник наукових статей. Серія «Історичні науки». Вип.4. Переяслав-Хмельницький, 2017. С.159 –175.
3. Барабаш В. А., Глєбова Л. В. Інформаційні ресурси бібліотеки закладу вищої освіти як джерело розвитку інтелектуального та духовного потенціалу студентів // Соціум. Документ. Комунікація: збірник наукових праць. Серія «Історичні науки». Переяслав-Хмельницький: ФОП Домбровська Я.М., 2019. Вип.6/2 (Спецвипуск). С.11 – 28.
4. Барабаш В. А., Глєбова Л. В., Тупчієнко М.П. Формування бібліографічної інформації – один із напрямків взаємодії кафедри та бібліотеки технічного університету // Соціум. Документ. Комунікація: зб. наук. праць. Серія: Історичні науки. Переяслав-Хмельницький: ФОП Домбровська Я.М., 2019. Вип. 8. С.14 – 31.
5. Бібліотека Центральноукраїнського національного технічного університету. URL. http://library.kntu.kr.ua (дата звернення 27.11.2020).
6. Горбаченко Т.Г. Аналітико-синтетична переробка документної інформації [Текст] : навч. посіб. для дистанційного навчання / Т. Г. Горбаченко. 2-ге вид., перероб. і доп. К. : Університет „Україна", 2008. 312 с.
7. Костенко Л.Й. Інформаційні технології в бібліотеці суспільства знань. URL. http://www.nbuv.gov.ua/sites/default/files/msd/0510kos.pdf (дата звернення 27.11.2020).
8. Кулешов С. Про значення поняття «документ» / С. Кулешов // Бібл. вісн. 2014. № 1. С. 1 – 4.
9. Кушнаренко Н.М. Удалова В.К. Наукова обробка документів: Підручник. 4-те вид., перероб. і доп. К.: Знання, 2006. 334 с.
10. Технічна освіта на Кіровоградщині: історичний нарис. Кіровоград: «Імекс-ЛТД», 2009. 240 с.
11. Швецова-Водка Г.М. Вступ до бібліографознавства. К., 2004
12. Швецова-Водка Г.Н. Общая теория документа и книги : учеб. пособие / Г. Н. Швецова-Водка. М.: Рыбари ; К. : Знання, 2009. 487 с.
13. URL. https://www.docsity.com/ru/diyalnist-zi-stvorennya-i-rozpovsyudzhennya-vtorinnoji-informaciji-bibliotekami-ukrajini/1769876/ (дата звернення 27.11.2020).

УДК 657

Я. Луцевят, магістр гр. ООУД – 19МЗ – 1,4
М. Петленко, магістр гр. ООУД – 19МЗ – 1,4
В. Селіщев, магістр гр. ООУД – 19М - 1,4
Центральноукраїнський національний технічний університет

НОРМАТИВНА РЕГЛАМЕНТАЦІЯ ОБЛІКУ ОБОРОТНИХ АКТИВІВ СІЛЬСЬКОГОСПОДАРСЬКИХ ПІДПРИЄМСТВ

У статті розглядаються методологічні аспекти обліку оборотних активів сільськогосподарських підприємств та їх нормативна регламентація. Виокремлено етапи нормативного регулювання обліку оборотних активів сільськогосподарських підприємств
оборотні активи, запаси, біологічні активи, грошові кошти, нормативна регламентація, сільськогосподарські підприємства

Постановка проблеми та її актуальність. В умовах розвитку ринкових відносин аграрне виробництво залишається однією із стратегічно найважливіших галузей національної економіки і запорукою збереження продовольчої безпеки країни, що зумовлює пошук принципово нових підходів до вирішення питань ефективності господарської діяльності сільськогосподарських підприємств. Значну увагу при цьому приділяють раціональному формуванню та ефективному використанню ресурсного потенціалу суб`єктів господарювання, чільне місце у складі якого займають оборотні активи. Оборотні активи, разом із необоротними, є чинником забезпечення безперебійності виробничого та збутового процесів, тому їх структура, розміщення на різних стадіях кругообігу капіталу, джерела формування та рівень забезпеченості ними прямо впливають на ділову активність і фінансовий стан підприємств.

Раціональне використання оборотних активів є одним з ключових факторів підвищення темпів розвитку сільськогосподарського підприємства, зниження собівартості продукції, підвищення ефективності виробництва й конкурентоспроможності. А для забезпечення безперервного процесу виробництва та реалізації продукції, кожне підприємство повинно мати чітко сформований механізм управління оборотними активами, який не можливий без відповідного облікового та контрольного забезпечення.

Аналіз останніх досліджень і публікацій. Теоретичні та практичні особливості нормативної регламентації та відображення в обліку оборотних активів сільськогосподарських підприємств висвітлені в працях таких українських та зарубіжних науковців та дослідників, як Атамас О.П. [1], Брик М. [2, 3], Гаценко-Колумбет О. П. [4], Гай О.М. [5], Єрмолаєва М. В. [6], Давидов Г.М. [7], Іщенко Я. П. [8], Донін Є.О. [9], Калюга Є. В. [10], Канцедал Н.А. [11], Полторак А.С. [12], Савченко В.М. [13], Стаднік Л.І. [14], Фатенок-Ткачук А. О. [15] та інші.

Однак, незважаючи на наявність численних науково-методичних розробок, окремі проблеми дослідження сутності, складу та відображення в обліку оборотних активів залишаються не дослідженими та потребують подальшого наукового обґрунтування. Водночас через постійні зміни, що відбуваються у законодавстві України та в системі управління, постійно виникають проблемні питання, організації та методики обліку оборотних активів на сільськогосподарських підприємствах, які потребують подальшого розгляду і опрацювання.

Метою статті є дослідження нормативної регламентації та відображення в обліку оборотних активів сільськогосподарських підприємств та надання пропозицій щодо його вдосконалення.

Виклад основного матеріалу. Як відомо, метою ведення бухгалтерського обліку і складання фінансової звітності є надання користувачам повної, правдивої та неупередженої інформації про рух активів, відносини з покупцями, замовниками, постачальниками, працівниками, власниками, іншими дебіторами та кредиторами, про результати діяльності й у цілому фінансовий стан підприємства. Для її досягнення здійснюється державне регулювання бухгалтерського обліку і фінансової звітності.

Методичні основи щодо формування в обліковому процесі інформації про оборотні активи, а також розкриття такої інформації у фінансовій звітності підприємства регламентуються комплексом нормативних актів, що в сукупності формують відповідну нормативно-правову базу, які доцільно систематизувати у вигляді п'яти основних рівнів (рис. 1):

Рисунок 1 – Класифікація нормативних документів щодо обліку оборотних активів за рівнями нормативної регламентації

Основою нормативно-правової бази, яка здійснює регламентування порядку організації обліку оборотних активів є Закон України «Про бухгалтерський облік та фінансову звітність в Україні» [16] та відповідний комплекс Національних положень (стандартів) бухгалтерського обліку. На рис. 2 наведено класифікацію нормативного-законодавчої бази, що регулює облік оборотних активів сільськогосподарських підприємств.

Як видно з наведеного рисунку нормативні документи, що регламентують організацію обліку та контролю оборотних активів сільськогосподарських підприємств доцільно розділити на три групи: нормативні документи щодо загальних питань обліку та контролю оборотних активів; нормативні документи щодо обліку та контролю оборотних матеріальних активів; нормативні документи щодо обліку та контролю оборотних фінансових активів.

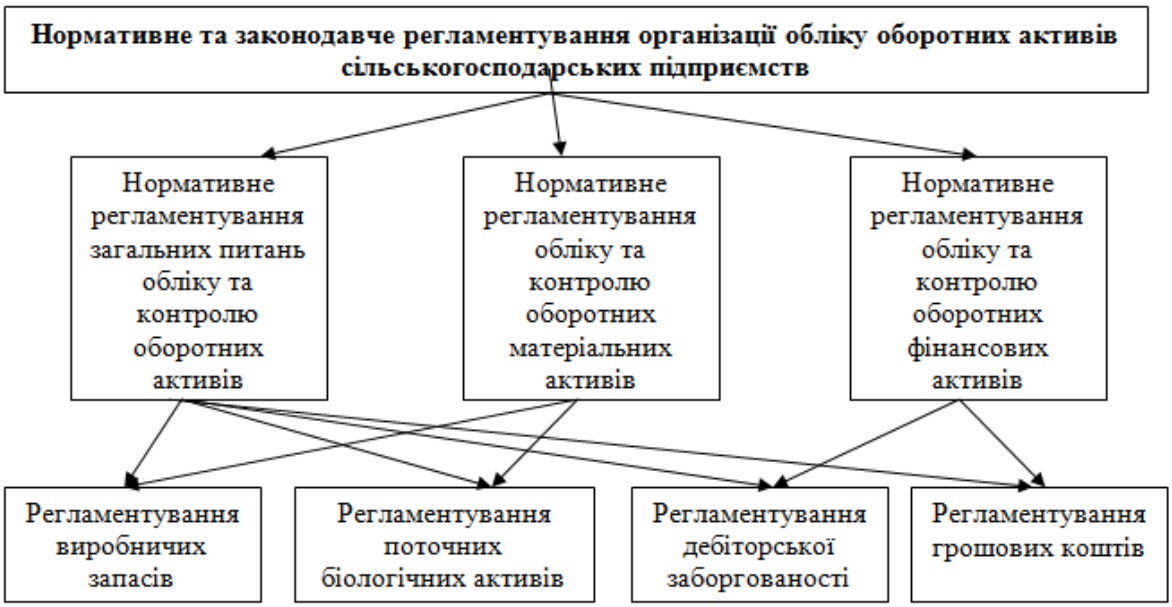


Рисунок 2 – Класифікація нормативно-законодавчої бази щодо обліку та контролю оборотних активів сільськогосподарських підприємств

В таблиці 1 наведено характеристику нормативних документів щодо загальних питань обліку та контролю оборотних активів підприємств.

Таблиця 1 – Характеристика нормативно-правових документів щодо загальних питань обліку оборотних матеріальних активів

Назва нормативно-правового документа	Сутність нормативно-правового документу щодо регулювання обліку оборотних активів
1	2
НП(С)БО 1 «Загальні вимоги до фінансової звітності [17]	Визначається зміст і форма Балансу та загальні вимоги до розкриття його статей. У відповідних рядках Балансу відображається наявність оборотних активів на підприємстві на звітну
Інструкція про застосування плану рахунків бухгалтерського обліку [18]	Встановлює призначення і порядок ведення рахунків бухгалтерського обліку для узагальнення методом подвійного запису інформації про наявність і рух оборотних активів
Положення № 88 [19]	Встановлює порядок створення, прийняття і відображення у бухгалтерському обліку, а також зберігання первинних документів, облікових регістрів, бухгалтерської звітності підприємствами та госпрозрахунковими організаціями (крім банків) незалежно від форм власності, установ та організацій, основна діяльність яких фінансується за рахунок коштів бюджету
Методичні рекомендації № 356 [20]	Відповідно до методичних рекомендацій № 356 для відображення в обліку оборотних активів використовуються Журнал № 1, № 3 та № 5 та 5А
План рахунків бухгалтерського обліку [21]	Цей документ являє собою перелік рахунків та схем реєстрації та угрупування на них фактів фінансово-господарської діяльності (кореспонденції рахунків) в бухгалтерському обліку. Для обліку оборотних активів Планом рахунків передбачено рахунок 20 «Виробничі запаси», рахунок 21 «Поточні біологічні активи», рахунок 22 «МШП», рахунок 24

	«Брак у виробництві», рахунок 25 «Напівфабрикати», рахунок 26 «Готова продукція», рахунок 27 «Продукція сільськогосподарського виробництва», рахунок 28 «Товари», рахунок 30 «Готівка», рахунок 31 «Рахунки в банках», рахунок 36 «Розрахунки з покупцями та замовниками», рахунок 37 «Розрахунки з різними дебіторами»
Положення про інвентаризацію активів і зобов'язань № 879 [22]	Визначає порядок проведення інвентаризації оборотних активів, основні завдання інвентаризації та випадки, в яких проведення інвентаризації є обов'язковим, зокрема щодо проведення інвентаризації оборотних матеріальних активів

Друга група запропонованої класифікації нормативного регламентування обліку оборотних активів це нормативні документи, що регулюють облік і контроль оборотних матеріальних активів. До складу оборотних матеріальних активів сільськогосподарських підприємств входять запаси та поточні біологічні активи.

Нормативно-правове регулювання обліку запасів сільськогосподарських підприємств, на нашу думку, слід розглядати на глобальному, національному та локальному рівнях (рис. 3).

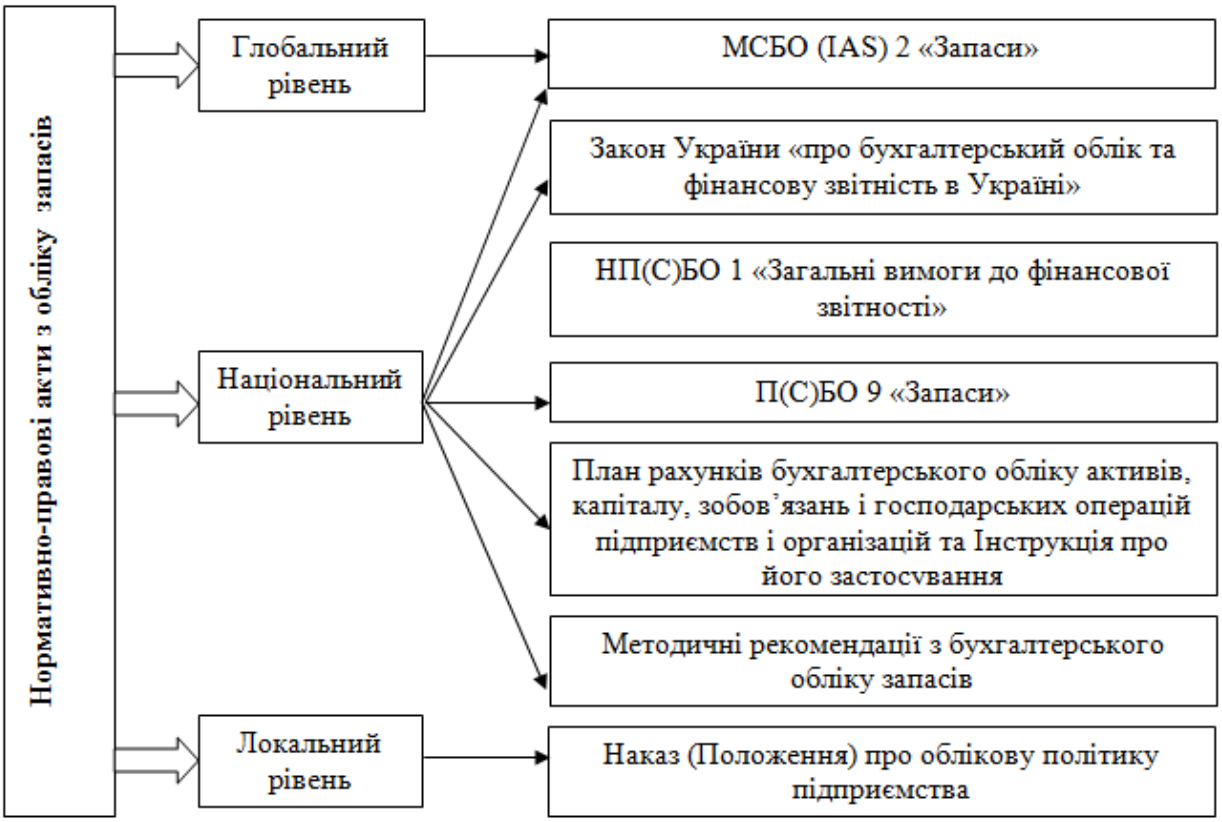


Рисунок 3 – Рівні нормативно-правового регулювання обліку запасів сільськогосподарських підприємств [16, 17, 21, 22, 23]

Відповідно до Положення (стандарту) бухгалтерського обліку 9 «Запаси» «запасами визнаються активи, які: утримуються для подальшого продажу за умов звичайної господарської діяльності; перебувають у процесі виробництва з метою подальшого продажу продукції виробництва; утримуються для споживання під час виробництва продукції, виконання робіт та надання послуг, а також управління підприємством» [24].

Здійснюючи облік операцій із запасами, підприємство повинно дотримувати тися вимог П(С)БО 9 «Запаси» [24]. Цим нормативним документом визначаються методологічні засади формування у бухгалтерському обліку інформації про запаси і розкриття її у фінансовій звітності. У П(С)БО 9 наведено визначення та методи оцінки запасів, перелік витрат, які

формують первісну вартість запасів.

Інструкція про застосування Плану рахунків бухгалтерського обліку активів, капіталу, зобов'язань і господарських операцій підприємств та організацій 291, містить коротку характеристику рахунків і субрахунків, установлює порядок ведення аналітичного обліку та кореспонденцію рахунків з обліку запасів [18].

Одним із специфічних видів запасів для сільськогосподарських підприємств є поточні біологічні активи, облік яких регулюється відповідними нормативними документами. Основними нормативними документами в Україні, що визначають порядок здійснення господарських операцій з біологічними активами на підприємствах сільського господарства, є: П(С)БО 30 «Біологічні активи» [26] та Методичні рекомендації з бухгалтерського обліку біологічних активів [25]. Згідно з П(С)БО 30 «Біологічні активи», «тварини або рослини, які в процесі біологічних перетворень спроможні давати сільськогосподарську продукцію та/або додаткові біологічні активи, а також приносити в інший спосіб економічні вигоди, визначені як біологічні активи» [26]. Тобто біологічним активом може бути будь-яка тварина чи рослина, яку утримують або вирощують на підприємстві.

В Методичних рекомендаціях з бухгалтерського обліку біологічних активів деталізовано норми П(С)БО 30. Крім того, в додатку 1 до цих Методичних рекомендацій детальніше, ніж в додатку до П(С)БО 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.

Основним нормативним документом щодо обліку дебіторської заборгованості є П(С)БО 10 «Дебіторська заборгованість» від 08.10.1999 р. № 237 [27], яке визначає методологічні засади формування у бухгалтерському обліку інформації про дебіторську заборгованість та її розкриття у фінансовій звітності. Відповідно до П(С)БО 10 здійснюється визнання та оцінка дебіторської заборгованості та розкриття інформації про дебіторську заборгованість у примітках до фінансової звітності.

Для сільгосподарських 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» від 16.07.1999 р. № 996-XIV [16] та Положенні про документальне забезпечення записів у бухгалтерському обліку, затвердженому наказом Мінфіну України від 24.05.1995 р. № 88 [19]. Проте для сільгосподарської 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 [28].

Більшість операцій, що відбуваються на підприємстві, пов'язані з придбанням, виробництвом і продажем товарів та послуг і отже, оплатою та одержанням грошових коштів та їх еквівалентів. Оскільки вони мають здатність обертатись, ступінь ризику помилок в обліку та контролю на цій ділянці обліку є досить великий.

Законність здійснення операцій з грошовими потоками регламентується чинним законодавством України і визначається на основі нормативно-правових документів. На наш погляд, нормативне регулювання бухгалтерського обліку грошових коштів можна представити чотирма рівнями регламентування (рис.4).

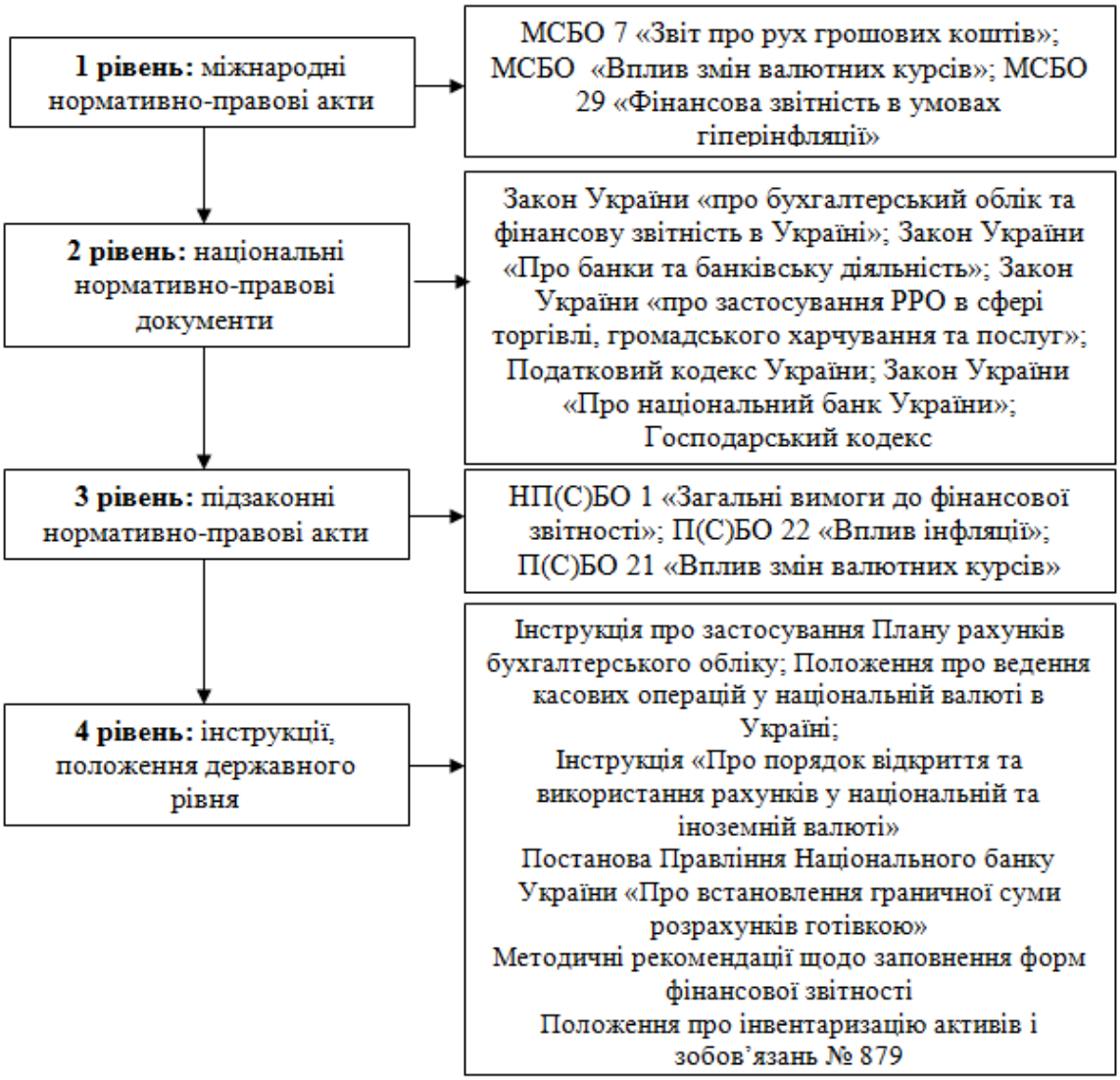


Рисунок 4 – Рівні нормативно-правового регулювання бухгалтерського обліку грошових коштів та їх еквівалентів

Операції з готівкою здійснює майже кожне підприємство, коли отримує її за продані товари (надані послуги), виплачує заробітну плату працівникам, видає готівку під звіт або на відрядження.

На сьогодні основним нормативним документом, що регулює ведення касових операцій у національній валюті, є Положення про ведення касових операцій у національній валюті в Україні, затверджене постановою № 148.

Вимоги до організації готівкових розрахунків викладено у розділі ІІ Положення № 148, яким, зокрема, передбачено, що «суб'єкти господарювання мають здійснювати розрахунки за своїми грошовими зобов'язаннями, що виникають у господарських відносинах, пріоритетно у безготівковій формі, а також у готівковій формі з дотриманням обмежень та в порядку, встановленому законодавством України».

Обмеження, яких мають дотримуватися суб'єкти господарювання та фізичні особи при здійсненні готівкових розрахунків, визначено пунктами 6 – 8 розділу ІІ Положення № 148. При цьому суб'єкти господарювання здійснюють розрахунки готівкою між собою і з фізичними особами через касу як коштами, одержаними як готівкова виручка, так і коштами, одержаними із банків. Зазначені розрахунки проводяться також шляхом переказу готівки для сплати відповідних платежів (п. 5 розділу ІІ Положення № 148).

Пунктом 17 цього розділу передбачено, що «суб'єкти господарювання використовують готівкову виручку (готівку), у тому числі готівку, одержану з банку, для

забезпечення потреб, що виникають у процесі їх функціонування, а також для проведення розрахунків з бюджетами та державними цільовими фондами за податками і зборами (обов'язковими платежами)». Крім того, вони не мають права накопичувати готівкову виручку (готівку) у своїх касах понад установлений ліміт каси для здійснення витрат до настання строків цих витрат.

Відповідно до ст.341 ГК України при безготівкових розрахунках всі платежі провадяться через установи банків шляхом перерахування належних сум з рахунку платника на рахунок отримувача або шляхом заліку взаємних зобов'язань та грошових претензій [30].

Розрахунки підприємств через банківські установи в безготівковій формі регулюються Інструкцією про безготівков розрахунки в Україні в національній валюті від 21.01.2004 р. № 22 зі змінами, внесеними Постановою НБУ правління від 24.04.2020 р. № 56, згідно якої «безготівкові розрахунки являють собою перерахування певної суми коштів з рахунків платників на рахунки отримувачів коштів, а також перерахування банками за дорученням підприємств і фізичних осіб коштів, унесених ними готівкою в касу банку, на рахунки отримувачів коштів». Ці розрахунки проводяться банком на підставі розрахункових документів на паперових носіях чи в електронному вигляді.

Вважаємо за доцільне наголосити на суттєвому значенні регулюючої документації, що розробляється безпосередньо на рівні підприємства, оскільки вона регламентує специфіку обліково-аналітичного процесу відповідно до особливостей діяльності кожного окремого господарюючого суб'єкта. Така документація є досить важливою у формуванні обліково-аналітичного процесу оборотних матеріальних активів підприємства, оскільки її розробка потребує врахування вимог законодавчих актів вищого рівня та виявлення і правильного відображення специфічних аспектів обліково-аналітичної діяльності на рівні даного суб'єкта господарювання.

Практичне втілення прийнятих управлінських рішень залежить від достовірності сформованого інформаційного середовища щодо бухгалтерського обліку та внутрішнього контролю оборотних активів на підприємствах. Контроль витрачання оборотних активів необхідно організовувати на всіх рівнях управління, у результаті чого він отримує певну ієрархію: нижній рівень - безпосередньо контроль за виробничими запасами, незавершеним виробництвом, готовою продукцією, який на великих підприємствах здійснюється бригадами, дільницями, групами; середній - до вище перерахованих об'єктів контролю належать грошові кошти, розрахунки з дебіторами та ін. (цехи, служби, відділи); вищий рівень - здійснюється контроль за всіма видами оборотних активів (керівники та заступники керівників).

Підсумовуючи, зауважимо, що кожне вітчизняне підприємство повинно самостійно, ґрунтуючись на чинному законодавчому полі та власному досвіді роботи, а також галузевих особливостях діяльності, відображати в обліку та проводити контроль операції щодо оборотних активів із врахуванням специфіки здійснення господарської діяльності відповідно до умов ринкової кон'юнктури та інших внутрішніх і зовнішніх факторів функціонування. У зв'язку із цим забезпечення коректного відображення в обліку цієї вагомої складової активів підприємства повинно базуватись виключно на діючій нормативно-правовій базі, визначеній законодавством України та враховувати внутрішню нормативну документацію підприємства, яка б надавала можливість повною мірою відображати специфіку його функціонування.

На нашу думку, таке коректне відображення облікових даних у внутрішніх нормативних документах, діючих у межах кожного окремого підприємства, надасть можливість та створить передумови для врахування специфіки діяльності кожного суб'єкта господарювання, забезпечить достатню інформативність та аналітичність при виконанні функцій контролю, планування та формування управлінських рішень тактичного та стратегічного значення.

Висновки та перспективи подальших досліджень. В результаті проведеного дослідження визначено, що в процесі регламентування обліку та контролю оборотних активів сільськогосподарських підприємств використовується надзвичайно велика кількість

нормативних документів різної спрямованості, рівня регламентування та юридичної сили. Для ефективного використання нормативних документів в процесі обліку та контролю оборотних активів, вважаємо за доцільне класифікувати їх за такими критеріями: за рівнем регулювання, галузевою приналежністю, об'єктами обліку та контролю. При цьому слід відмітити, що основними проблемами формування якісної облікової інформації в бухгалтерському обліку оборотних активів є недосконаліть нормативного регулювання бухгалтерського обліку складових оборотних активів. На сьогодні в Україні існує досить багато нормативно-правових актів, що регламентують облік оборотних активів.

Список літератури

1. Атамас О.П., Січева Д.В. Питання організації бухгалтерського (фінансового) обліку на сільськогосподарських підприємствах. Науковий огляд. 2019. № 6 (59). С. 110 – 118. URL: http://naukajournal.org/index.php/naukajournal/article/view/1868 (дата звернення: 11.11.2020).
2. Брик М. Своєрідність обліку та контролю поточних біологічних активів в тваринництві. Регіональні аспекти розвитку продуктивних сил України. 2018. Вип. 23. С. 61-65. URL: http://nbuv.gov.ua/UJRN/rarpsu_2018_23_14 (дата звернення: 17.11.2020).
3. Брик М. М. Проблематика обліку і відображення у звітності довгострокових біологічних активів. Розвиток соціально-економічних систем в сучасних умовах: матеріали II Міжнар. наук.-практ. конф. (Одеса, 2–3 лют. 2018 р.). Херсон : Вид-во Молодий вчений, 2018. С. 52–54.
4. Гаценко-Колумбет О. П. Оборотні активи підприємства: проблеми теорії обліку. Вісник Житомирського державного технологічного університету. Серія: Економічні науки. 2013. № 1. С. 42-47. URL: http://nbuv.gov.ua/UJRN/ Vzhdtu_econ_2013_1_10 (дата звернення: 16.11.2020).
5. Гай О.М., Кононенко Л.В., Шинкаренко А.В., Костенко В.Г. Організація внутрішнього контролю виробництва продукції тваринництва та його документальне оформлення. Вісник Чернівецького торговельно-економічного інституту. Економічні науки. Чернів. торг.-екон. ін-т КНТЕУ. Чернівці: ЧТЕІ КНТЕУ, 2020. Вип. III (79). Економічні науки. (дата звернення: 17.11.2020).
6. Єрмолаєва М. В. Облік сільськогосподарської діяльності та біологічних активів: актуальні питання теорії та практики. Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія: Економіка і управління. 2019. . Т. 30(69), № 4(1). . С. 128-133. URL: http://nbuv.gov.ua/UJRN/UZTNU_econ_2019_30(69)_4(1)__24 (дата звернення: 17.11.2020).
7. Облікова політика: навч. посіб. Г.М. Давидов, В.М. Савченко, О.В. Пальчук, та ін.; за заг. ред. Г.М. Давидова. 2-ге вид., перероб. і доп. Кропивницький: ПП «Ексклюзив-Систем», 2017. 362 с. URL: http://dspace.kntu.kr.ua/jspui/handle/123456789/7357 (дата звернення: 09.11.2020).
8. Іщенко Я. П. Правове забезпечення обліку витрат на виробництво сільськогосподарської продукції в Україні. Економіка. Фінанси. Менеджмент: актуальні питання науки і практики. 2019. № 8. - С. 120-130. URL: http://nbuv.gov.ua/UJRN/efmapnp_2019_8_15 (дата звернення: 19.11.2020).
9. Донін Є.О., Особливості сучасних підходів щодо специфіки класифікації оборотних активів підприємства. Економіка і організація управління. 2018. Випуск № 1 (29). С. 75 – 85. URL: http://jeou.donnu.edu.ua/article/view/5738 (дата звернення: 27.11.2020).
10. Калюга Є. В. Оцінка біологічних активів як елемент методу бухгалтерського обліку. Облік і фінанси. 2017. № 4. С. 33-39. URL: http://nbuv.gov.ua/UJRN/Oif_apk_2017_4_7 (дата звернення: 12.11.2020).
11. Канцедал Н.А. Інституціальний підхід до формування в обліку інформації про біологічні активи та сільськогосподарську діяльність. Економіка. Фінанси. Менеджмент: актуальні питання науки і практики. 2018. № 1. С. 44-55. URL: http://dspace.pdaa.edu.ua:8080/xmlui/handle/123456789/228 (дата звернення: 11.11.2020).
12. Полторак А.С. Класифікація оборотних активів підприємств АПК: сучасні науково-методологічні підходи. Інвестиції: практика та досвід. 2013. № 15. С. 68-71. URL: http://nbuv.gov.ua/UJRN/ipd_2013_15_17 (дата звернення: 12.11.2020).
13. Савченко В. М. Інформаційне забезпечення податкового менеджменту Центральноукраїнський науковий вісник . Економічні науки. 2018. Вип. 1. С. 214-220. URL: http://nbuv.gov.ua/UJRN/Npkntu_e_2018_1_25 (дата звернення: 11.11.2020).
14. Стаднік Л.І. Облік запасів сільськогосподарських підприємств. Економіка та управління АПК. 2016. № 1-2. С. 79-83
15. Фатенок-Ткачук А. О. Теоретичні аспекти фінансового обліку біологічних активів. Економічний вісник Запорізької державної інженерної академії. 2016. Вип. 5(2). С. 120-123. URL: http://nbuv.gov.ua/ UJRN/evzdia_ 2016_5(2)__26 (дата звернення: 25.11.2020).
16. Закон України «Про бухгалтерський облік та фінансову звітність в Україні» № 996-XIV від 16 лип. 1999 р. URL: http://www.rada.gov.ua. (дата звернення: 21.11.2020).
17. НП(С)БО 1 «Загальні вимоги до фінансової звітності» : затв. наказом Міністерствава фінансів України від 07.02.2013 р. № 73. База даних «Законодавство України» / ВР України. URL: http://www.minfin.gov.ua/

control/uk/publish/article?art_id=367055&cat_id=293533 (дата звернення: 17.11.2020).
18. 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. URL: http://zakon3.rada.gov.ua (дата звернення: 23.11.2020).
19. Положення про документальне забезпечення записів в бухгалтерському обліку, затверджене наказом Мінфіну України від 24.05.95 р. № 88. URL: http://search.ligazakon.ua/l_doc2.nsf/link1/T990996.html (дата звернення: 21.11.2020).
20. Методичні рекомендації по застосуванню регістрів бухгалтерського обліку від 29 грудня 2000 р. № 356 // Міністерство Фінансів України. URL: http://www.uazakon.com/ big/text574/ pg1.htm.
21. План рахунків бухгалтерського обліку активів, капіталу, зобов'язань і господарських операцій підприємств і організацій: Наказ Міністерства фінансів України від 30.11.99 р. URL: http://search.ligazakon.ua/ l_doc2.nsf/ link1/T990996.html (дата звернення: 18.11.2020).
22. Наказ Міністерства фінансів України «Про затвердження Положення про інвентаризацію активів та зобов'язань» від 02.09.2014 р. № 879. URL: http//www.zakon1.rada.gov.ua (дата звернення: 21.11.2020).
23. Міжнародні стандарти бухгалтерського обліку та фінансової звітності. URL: http://www.minfin.gov.ua.
24. П(С)БО 9 «Запаси»: наказ Міністерства фінансів України від 20. 10. 99 р. № 246. URL: http://dtkt.com.ua/show/2bid17066.html (дата звернення: 17.11.2020).
25. Методичні рекомендації з бухгалтерського обліку біологічних активів, затверджені наказом МФУ від 29.12.2006 р. № 1315. URL: http://www.rada.gov.ua. (дата звернення: 22.11.2020).
26. П(С)БО 30 «Біологічні активи»: затверджене наказом Міністерства фінансів України від 18 листопада 2005 р. № 790. URL: http://www.rada.gov.ua. (дата звернення: 23.11.2020).
27. П(С)БО 10 «Дебіторська заборгованість»: наказ Міністерства фінансів України від 08. 10. 99 р. № 237. URL: http://dtkt.com.ua/show/2bid17066.html (дата звернення: 17.11.2020).
28. 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 URL: http://www.rada.gov.ua. (дата звернення: 12.11.2020).
29. П(С)БО 16 «Витрати», затверджене наказом МФУ від 31.12.99 р. № 318. URL: http://dtkt.com.ua/show/2bid17066.html (дата звернення: 17.11.2020).
30. Господарський кодекс України № 436ıIV від 16.01.2003 р. Сайт «Законодавство України» URL: www.zakon.rada.gov.ua (дата звернення: 17.11.2020).

УДК 657

А. Суріна, магістр гр. ООУД – 19МЗ – 1,4
В. Шикіта, магістр гр. ООУД – 19М - 1,4
Центральноукраїнський національний технічний університет

ОСОБЛИВОСТІ ОЦІНКИ МАТЕРІАЛЬНИХ АКТИВІВ В ДЕРЖАВНОМУ СЕКТОРІ

У статті розкрито особливості оцінки матеріальних активів на підприємствах державного сектору. Досліджено види вартості та порядок визначення первісної вартості матеріальних активів за національними стандартами бухгалтерського обліку в державному секторі.
бюджетна установа, суб'єкт державного сектору, оцінка, матеріальні активи бюджетних установ, первісна вартість, метод оцінки матеріальних активів

Постановка проблеми та її актуальність. Задля виконання своїх функцій бюджетні установи, організації і підприємства державного сектору закуповують або отримують безоплатно матеріальні актьиви. Різноманітна структура матеріальних активів в установах зумовлена широким спектром діяльності бюджетних установ: охорона здоров'я, культура, мистецтво, освіта, дошкільне виховання, позашкільне і фізичне виховання молоді, адміністративно-управлінська робота та інша діяльність.

В системі бухгалтерського обліку бюджетних установ саме облік матеріальних активів є однією з найскладніших і найвідповідальніших ділянок, яка вимагає

скрупульозності, відповідальності та значних затрат робочого часу через значну кількість об'єктів обліку.

Модернізація бухгалтерського обліку в державному секторі, зокрема щодо обліку матеріальних активів бюджетних установ та їх оцінки, сприяє наближенню вітчизняної облікової практики до міжнародних стандартів.

Аналіз останніх досліджень і публікацій. Питанням оцінки матеріальних активів та їх обліку у державному секторі присвячено багато праць таких вітчизняних вчених як: Атамас П.Й. [1], Давидов Г.М. [2], Джога Р.Т., Сінельник Л. М., Дунаєва М. В. [3], Зеленко С. В. [4], Капустяк У. І. [5], Артюх О., Максімова В., Черкашина Т. [6], Плаксієнко В. Я. [7], Романченко Ю. О. [8], Савченко В.М. [9], Фесун І. Ю. [10] та інші. У вітчизняній науковій літературі, присвяченій питанням обліку матеріальних активів в бюджетних установах, науковці намагаються дослідити особливості методів оцінки вибуття матеріальних активів та показати їх переваги та недоліки. Проте, на сьогодні, в умовах законодавчих змін, існує необхідність подальших наукових досліджень в цьому напрямку.

Метою статті є з'ясування й обґрунтування особливостей оцінки матеріальних активів в установах державного сектору за національними стандартами бухгалтерського обліку в державному секторі.

Виклад основного матеріалу. Важливим аспектом бухгалтерського обліку є надання подіям господарської діяльності грошової оцінки. Концепція оцінки суттєво впливає на систему аналітичних показників, визначаючи вартість елементів фінансової звітності, дає змогу отримати узагальнене уявлення про майновий стан та результати діяльності, є необхідною умовою визнання активів і пасивів, здійснюється з допустимою точністю та обачністю.

Оскільки матеріальні активи установ державного сектору включають різні за складом та сутністю об'єкти, для їх оцінки в обліковій практиці використовуються різноманітні підходи та види оцінки.

Кожен об'єкт бухгалтерського обліку, а саме матеріальні активи суб'єктів державного сектору має специфічні особливості при формуванні первісної вартості, які напряму залежать від каналів їх надходження в установу (рис. 1).

Необоротні матеріальні активи суб'єктів державного сектору займають значну питому вагу у структурі її майна. При цьому первісна вартість необоротних матеріальних активів залежить від способу їх надходження до установи, а саме: вартість придбання за плату; собівартість виробництва у разі самостійного виготовлення (створення); справедлива вартість у разі отримання без оплати від фізичних та юридичних осіб (крім суб'єктів державного сектору); первісна (переоцінена) вартість основних засобів у разі отримання без оплати від суб'єктів державного сектору; залишкова вартість переданого об'єкта основних засобів у разі отримання у результаті обміну на інший актив; умовна вартість у разі відсутності активного ринку.

Первісна вартість об'єкта необоротних активів може формуватися як за рахунок капітальних витрат, так і за рахунок поточних витрат (витрати на транспортування, установку, монтаж, налагодження основних засобів тощо) згідно з економічною класифікацією видатків бюджету.

В процесі експлуатації необоротні матеріальні активи підлягають амортизації. Амортизація це систематичний розподіл вартості необоротних активів, яка амортизується, протягом строку їх корисного використання (експлуатації). При цьому об'єктом амортизації є вартість, яка амортизується. Вартість, яка амортизується, у свою чергу, це первісна або переоцінена вартість необоротних активів, за вирахуванням їх ліквідаційної вартості.

Ліквідаційна вартість - сума коштів або вартість інших активів, яку суб'єкт державного сектору очікує отримати від реалізації (ліквідації) необоротних активів після закінчення строку їх корисного використання (експлуатації), за вирахуванням витрат, пов'язаних з продажем (ліквідацією)

Амортизація інших необоротних матеріальних активів (крім необоротних

матеріальних активів спеціального призначення та інших необоротних матеріальних активів, створених у результаті поліпшення об’єкта операційної оренди), нараховується в першому місяці передачі у використання об'єкта необоротних активів у розмірі 50 відсотків його первісної вартості та решта 50 відсотків первісної вартості - у місяці їх вилучення з активів (списання з балансу).

Запаси є найбільш значною частиною оборотних матеріальних активів суб’єктів державного сектору. В свою чергу їх оцінка впливає на результати діяльності установи та на розкриття інформації про її фінансовий стан. Окрім того, що це значні суми у загальній валюті балансу, це ще і власність держави. За рахунок вартості запасів формується вартість послуг, що отримує населення від імені держави. На відміну від комерційних підприємств, вартість запасів, що увійшли у надані послуги, не повертається у бюджетних установах у вигляді доходу. Ці витрати формують фактичні видатки установи (рис. 2).

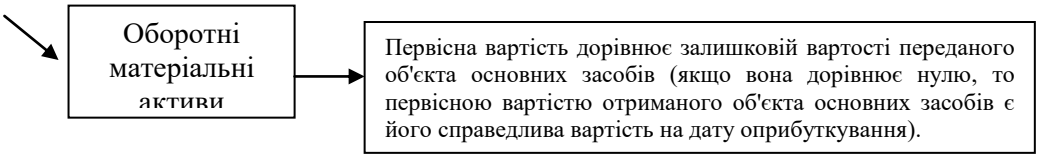


Рисунок 1 – Складові первісної вартості матеріальних активів в державному секторі (складено на підставі [11; 12])

У бухгалтерському обліку установ державного сектору придбані (отримані) або вироблені запаси зараховуються на баланс за первісною вартістю. Для правильного визначення первісної вартості бухгалтеру необхідно звернути увагу на спосіб їх надходження до установи, що наведено на рис. 1.

Особливістю формування первісної вартості в державних установах є те, що витрати, пов'язані з наймом транспорту для перевезення запасів, відносяться до видатків організації за відповідними кодами економічної класифікації, за якими вони передбачені в кошторисі доходів та видатків, а також не включаються до первісної вартості придбаних запасів. Також до збільшення первісної вартості запасів не відносяться суми ПДВ, сплаченого під час придбання запасів, що списується на видатки бюджетних організацій.

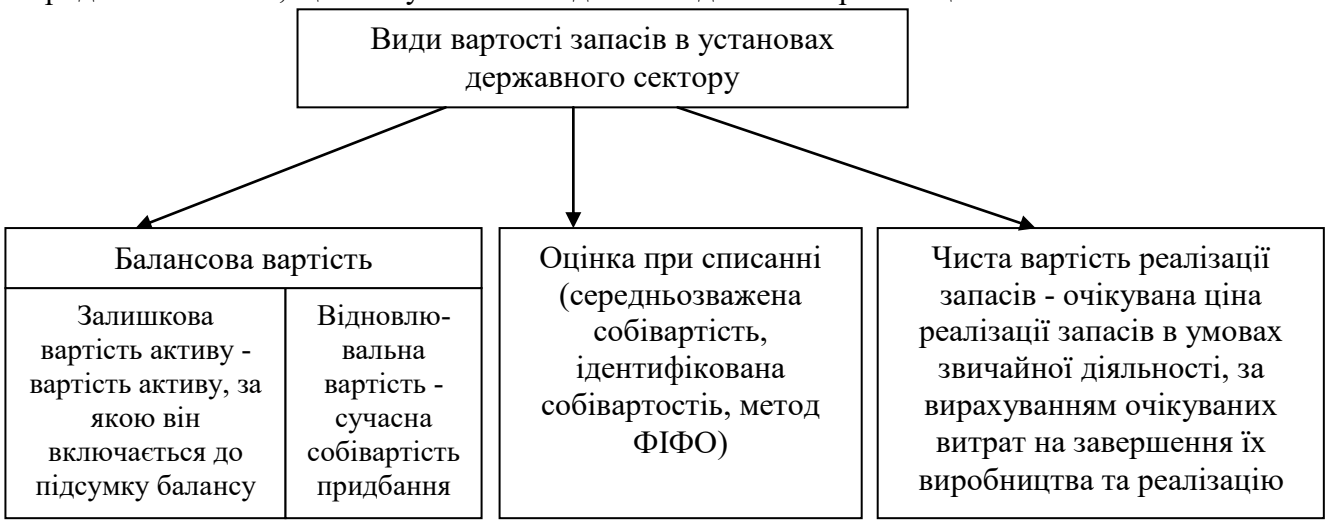


Рисунок 2 – Види оцінки запасів за НП(С)БОДС 123 «Запаси»

Особливого контролю потребують транспортно-заготівельні витрати (ТЗВ), що входять до первісної вартості запасів. Суб'єкт державного сектору самостійно визначає порядок обліку і розподілу ТЗВ. По-перше, сума ТЗВ може узагальнюватися на окремому субрахунку або аналітичному рахунку за окремими групами запасів, якщо вони пов'язані з доставкою кількох найменувань, груп, видів запасів. По-друге, сума ТЗВ, що узагальнюється на окремому субрахунку або аналітичному рахунку обліку запасів, щомісяця розподіляється між сумою залишку запасів на кінець звітного місяця і сумою запасів, що вибули (використані, реалізовані, безоплатно передані тощо) за звітний місяць.

Щодо оцінки запасів, то, згідно з НП(С)БО 123 «Запаси», «оцінка запасів на дату балансу відображається за найменшою з двох оцінок, а саме первісною вартістю або чистою вартістю реалізації» [13].

Під час зниження ціни запасів, псування або втрати вигоди оцінка проводиться за чистою вартістю реалізації. Під час перевищення суми купівельної вартості над чистою вартістю реалізації різниця списується на витрати звітного періоду. Дохід визначається, якщо вартість реалізації запасів, які були уцінені, збільшується на суму, не більшу суми за попереднім замовленням.

Вибуття запасів (списання з балансу) в бухгалтерському обліку установ державного сектору відображається як збільшення витрат та зменшення запасів звітного періоду. У разі якщо запаси безоплатно передано в межах уповноваженого органу, то балансова вартість

таких запасів до їх використання відображається у бухгалтерському обліку як збільшення дебіторської заборгованості (зобов'язань) за розрахунками з внутрішнього переміщення запасів.

Списання використаних запасів, отриманих безоплатно в межах уповноваженого органу, відображається в бухгалтерському обліку як зменшення балансової вартості цих запасів та зобов'язань за розрахунками з їх внутрішнього переміщення. У бухгалтерському обліку суб'єкта державного сектору, що передав ці запаси, таке списання відображається як збільшення витрат та зменшення дебіторської заборгованості за розрахунками з внутрішнього переміщення (внутрівідомчої безоплатної передачі) запасів на підставі акта списання, отриманого від суб'єкта державного сектору, що їх використав.

Вибуття запасів в установах державного сектору оцінюється за такими методами: ідентифікованої собівартості відповідної одиниці запасів; середньозваженої собівартості; собівартості перших за часом надходження запасів (ФІФО). Характеристику методів вибуття запасів в установах державного сектору наведено на рис. 3.

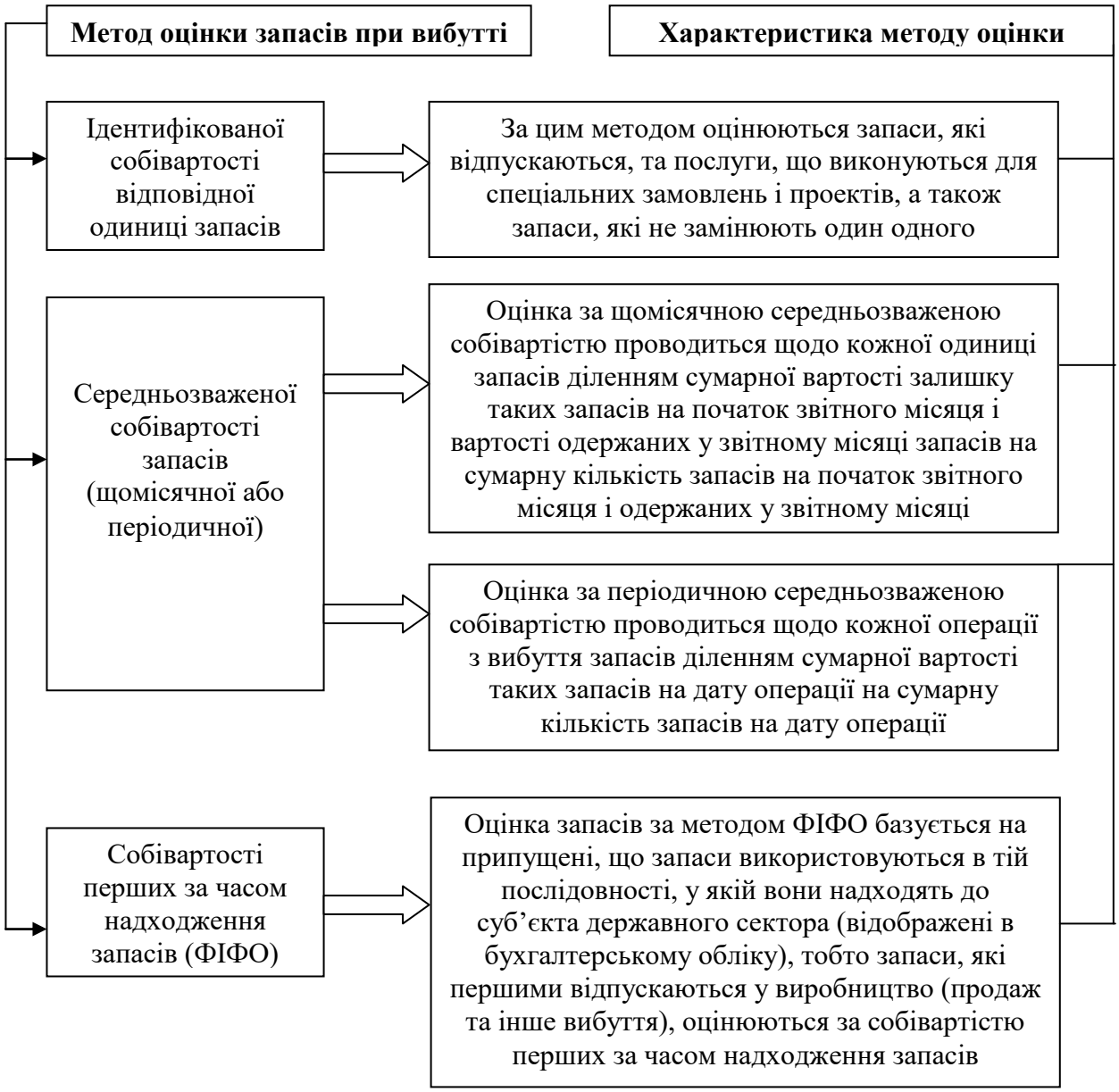


Рисунок 3 – Методи оцінки запасів при вибутті та їх характеристика

В установах державного сектору для всіх одиниць обліку запасів, що мають однакове призначення та однакові умови використання, застосовується лише один із наведених

методів. При цьому вибраний метод оцінки вибуття запасів визначається в розпорядчому документі про облікову політику, яка має бути єдиною у відповідній галузі. Найбільш поширеною оцінкою вибуття запасів у бюджетній сфері є оцінка запасів за методом ФІФО, застосування якого є доцільним для оцінки запасів під час їх відпуску у виробництво.

За НП(С)БОДС 123 «Запаси» «запаси відображаються в бухгалтерському обліку і звітності на дату балансу, в тому числі у разі зміни мети утримання запасів за найменшою з двох оцінок: первісною вартістю або чистою вартістю реалізації. Запаси відображаються за чистою вартістю реалізації, якщо на дату балансу їх ціна знизилась або вони зіпсовані, застаріли або іншим чином втратили первісно очікувану економічну вигоду» [13]. Це важливий момент, який підвищує якість представленої фінансової звітності установ державного сектору.

НП(С)БОДС 123 «Запаси» зобов'язує до розкриття інформації про запаси в примітках до фінансової звітності щодо: «балансової (облікової) вартості запасів у розрізі окремих класифікаційних груп; балансової (облікової) вартості запасів, які відображені за чистою вартістю реалізації; балансової вартості запасів, відображених за відновлювальною вартістю; балансової вартості запасів, переданих у переробку, на комісію, в заставу» [13]. У примітках до фінансової звітності також наводиться інформація про: методи оцінки запасів і суму збільшення чистої вартості реалізації, за якою проведена оцінка запасів.

Необхідно зазначити, що інформація про балансову вартість різних видів запасів та про ступінь змін у цих активах є важливою для користувачів фінансових звітів і вимагає повного її розкриття у примітках до фінансових звітів.

Особливим видом матеріальних активів суб'єктів державного сектору, починаючи з 2018 року, є біологічні активи. Тому вважаємо за доцільне розглянути порядок оцінки біологічних активів та сільськогосподарської продукції в установах державного сектору.

НП(С)БО 136 «Біологічні активи» запровадило щодо біологічних активів сільськогосподарського призначення та сільськогосподарської продукції модель оцінки за справедливою вартістю. У системі МСФЗ оцінка за справедливою вартістю є однією з пріоритетних. У світовій практиці можливі три підходи до оцінки справедливої вартості: ринковий, доходний та витратний.

В.М. Жук вважає, що «методологія оцінки біологічних активів та сільськогосподарської продукції за справедливою вартістю має узагальнені підходи. Бухгалтерський облік біологічних активів за міжнародними стандартами передбачає ринкову оцінку активів (за справедливою вартістю). Оцінка активів за справедливою вартістю хоча і викликає труднощі на практиці, проте має величезне значення для інвестиційної привабливості сільського господарства України. Взагалі оцінка активів за ринковою вартістю стає пріоритетним напрямом розвитку бухгалтерського обліку у світі» [15].

В українській практиці переважно використовують ринковий підхід. На вітчизняних підприємствах особливості оцінки біологічних активів сформувалися з урахуванням шляхів надходження біологічних активів, їх класифікації та дати оцінки відповідно до певних господарських операцій у процесі руху вказаних об'єктів обліку. На сьогодні більшість установ державного сектору не застосовують нововведення і відображають в обліку оприбуткування готової продукції за старою методикою, тобто за плановою собівартістю, а це призводить до викривлення інформації в фінансовій звітності.

Довгострокові, поточні та додаткові біологічні активи при первісному визнанні оцінюються на кожну звітну дату. Сільськогосподарська продукція оцінюється лише при первісному визнанні. При цьому оцінка за справедливою вартістю передбачає вирахування витрат на продаж.

Лень В.С. вказує на те, що «у міжнародному стандарті фінансової звітності 41 «Сільське господарство» встановлено, що справедливу вартість сільськогосподарської продукції в момент її збору можна завжди визначити з достатнім ступенем вірогідності, а тому у всіх випадках в момент збору сільськогосподарської продукції вона повинна оприбутковуватись за справедливою вартістю за винятком передбачуваних збутових витрат»

[16].

На думку Л. С. Голотюк, «використання справедливої вартості для оцінки активів підприємства сприяє реальнішому відображенню їхньої вартості в балансі, що дає можливість об'єктивніше проводити аналіз структури майна підприємств. При цьому єдині підходи відображення вартості активів дають можливість порівнювати показники фінансової звітності різних підприємств» [17].

На рис. 4 узагальнено інформацію щодо оцінки різних видів біологічних активів згідно з НП(С)БОДС 136 «Біологічні активи».

Рисунок 4 – Оцінка біологічних активів у бюджетних установах (складено на основі [18])

Варто звернути увагу на той факт, що первісне визнання додаткових біологічних активів відображається в тому звітному періоді, в якому вони відокремлені від біологічного активу. Пункт 10 розділу ІІ НП(С)БОДС 136 дає роз'яснення щодо алгоритму дій у випадку неможливості оцінки біологічних активів за справедливою вартістю за вирахуванням витрат на продаж. Отже, довгострокові біологічні активи, справедливу вартість яких на дату балансу достовірно визначити неможливо, можуть визнаватися та відображатися за первісною вартістю з урахуванням суми їх зносу і втрат від зменшення корисності.

Оцінка й амортизація таких довгострокових біологічних активів здійснюється відповідно до Національного положення (стандарту) 121 «Основні засоби» та Національного положення (стандарту) бухгалтерського обліку в державному секторі 127 «Зменшення корисності активів» [19; 20].

Л.В. Гуцаленко звертає увагу, що «можуть бути випадки, коли неможливо здійснити надійну оцінку справедливої вартості біологічного активу. Справедливу вартість біологічного активу можна оцінити з певною ступінню надійності. Такий підхід можливо заперечити тільки в момент первинного визнання біологічного активу, відносно якого відсутня інформація про ринкові ціни, а альтернативні розрахунки справедливої вартості не є надійними. У такій ситуації біологічний актив необхідно оцінювати за собівартістю за мінусом накопиченої амортизації і збитків від його знецінення» [21].

На думку Жука В.М. «поточні та додаткові біологічні активи, справедливу вартість

яких на дату балансу достовірно визначити неможливо, можуть визнаватися та відображатися за виробничою собівартістю, крім поточних біологічних активів рослинництва, які визнаються і відображаються як незавершене виробництво» [15].

Щодо первісного визнання сільськогосподарської продукції (зерна, молока, меду, приплоду тощо), то її бажано відображати у тому звітному періоді, в якому вона була відокремлена від біологічного активу. Після первісного визнання її оцінюють та відображають відповідно до НП(С)БОДС 123 «Запаси» [13].

Найпоширенішим способом оцінки біологічних активів є справедлива вартість, тобто сума, за якою установа може продати біологічний актив за звичайних умов на певну дату. Однак не за всіма видами біологічних активів і не завжди справедливу вартість можна визначити. У таких випадках законодавством передбачено використання інших облікових оцінок, тож вивчайте їх і застосовуйте.

Важливим аспектом бухгалтерського обліку є надання подіям господарської діяльності грошової оцінки. На сьогодні, в установах державного сектору, мають місце методичні та організаційні проблеми щодо оцінки матеріальних активів, а саме: формування первісної вартості; проблеми складності застосування різних оцінок; визначення справедливої вартості; облік знецінення активів; формування залишкової вартості. Успішне розв'язання названих проблем дозволить забезпечити адекватне грошове вираження відносної корисності активів і конструктивність оцінювання соціально-економічної ефективності діяльності суб'єкта державного сектору.

Висновки та перспективи подальших досліджень. В процесі дослідження особливостей оцінки матеріальних активів в державному секторі встановлено, що обґрунтований вибір базової оцінки сприятиме формуванню єдиних підходів до подання достовірної облікової та звітної інформації установ державного сектору. При цьому подальшого розгляду потребують питання застосування оцінки активів за справедливою вартістю (уточнення сутності, порядок визначення, законодавче регулювання).

Список літератури

1. Атамас П.Й., Атамас О.П. Облік у бюджетних установах. 5-те вид., перероб. та доп. Навч. посіб. / П.Й. Атамас, О.П. Атамас. – Київ: «Центр учбової літератури», 2018. – 392 с.
2. Облікова політика: навч. посіб. Г.М. Давидов, В.М. Савченко, О.В. Пальчук, та ін.; за заг. ред. Г.М. Давидова. 2-ге вид., перероб. і доп. Кропивницький: ПП «Ексклюзив-Систем», 2017. 362 с. URL: http://dspace.kntu.kr.ua/jspui/handle/123456789/7357 (дата звернення: 09.11.2020).
3. Облік у бюджетних установах: підручник / Джога Р.Т., Сінельник Л. М., Дунаєва М. В.; за заг. ред. проф. Р. Т. Джоги. К.: КНЕУ 2006. 483с.
4. Зеленко С. В. Оцінка нормативно-правового забезпечення обліку господарської діяльності бюджетних установ. Економічний форум. 2020. № 3. С. 130-137. URL: http://nbuv.gov.ua/UJRN/ecfor_2020_3_22 (дата звернення: 12.11.2020).
5. Капустяк У. І. Особливості обліку з надходження та оприбуткування основних засобів у бюджетних установах. Економіка. Фінанси. Право. 2018. № 3(2). С. 13-17. URL: http://nbuv.gov.ua/UJRN/ecfipr_2018_3(2)__5 (дата звернення: 29.11.2020).
6. Артюх О., Максімова В., Черкашина Т. Облік у бюджетних установах: навчальний посібник Одеса: ОНЕУ: Ротапринт, 2013. 264 с.
7. Плаксієнко В. Я. Надходження та оприбуткування основних засобів у світлі імплементації міжнародних стандартів обліку у державному секторі. Актуальні проблеми інноваційної економіки. 2017. № 2. С. 78-82. URL: http://nbuv.gov.ua/UJRN/apie_2017_2_13 (дата звернення: 01.11.2020).
8. Романченко Ю. О. Облікова політика як елемент системи обліку та контролю в державному секторі. Науковий погляд: економіка та управління. 2017. № 2. С. 147–153. URL: http://nbuv.gov.ua/UJRN/vamsue_2017_2_15 (дата звернення: 12.11.2020).
9. Савченко В.М., Кононенко Л.В. Розвиток оцінки в обліку сільськогосподарської діяльності. Розвиток національної економіки: теорія і практика: Матеріали міжнародної науково-практичної конференції 3-4 квітня 2015 року, проведеної на базі ДВНЗ "Прикарпатський національний університет імені Василя Стефаника", м. Івано-Франківськ. Тернопіль: Крок, 2015. Ч.3. С. 320 -322
10. Фесун І. Ю. Модернізація системи бухгалтерського обліку в державному секторі: виклики і перспективи. Вісник Хмельницького національного університету. Економічні науки. 2018. № 4. С. 119-124. URL: http://nbuv.gov.ua/UJRN/Vchnu_ekon_2018_4_22 (дата звернення: 19.11.2020).

11. Методичні рекомендації щодо облікової політики суб'єкта державного сектору, затверджено наказом Міністерства фінансів України від 23.01.2015 №11. Міністерство фінансів України. Офіц. Веб-сайт. URL:: http://minfin.kmu.gov.ua/control/uk/publish/ article?art_id=407392&cat_id=407391. (дата звернення: 15.11.2020).
12. Національні положення (стандарти) бухгалтерського обліку в державному секторі: наказ Міністерства фінансів України. URL: http://zakon3.rada.gov.ua/laws/show/z0090-11. (дата звернення: 21.11.2020).
13. НП(С)БОДС 123 «Запаси»: наказ Міністерства фінансів України від 12.10.2010 р. № 1202 станом на 01.04.2018. URL: http://zakon2.rada.gov.ua/laws/show/z1019-10. (дата звернення: 22.11.2020).
14. Глушко О.В. Методичні основи оцінки довгострокових біологічних активів: теорія та практика оцінки. Науковий вісник Національного університету біоресурсів і природокористування України. 2013. Вип. 181, ч. 3. 268 с.
15. Жук В. М. Концепція розвитку бухгалтерського облік у в аграрному секторі економіки : монографія. Київ : ННЦ ІАЕ, 2009. 648 с.
16. Лень В.С., Стародуб І.Л. Оцінка та облік поточних біологічних активів рослинництва. Вісник Чернігівського державного технічного університету, 2008. № 33. С. 172–178.
17. Голотюк Л. С. Проблеми оцінки біологічних активів тваринництва за справедливою вартістю в сільськогосподарських підприємствах. Ефективна економіка. 2014. № 12. URL: http://www.economy.nayka.com.ua/?op=1 z=3699. (дата звернення: 21.11.2020).
18. Національне положення (стандарт) бухгалтерського обліку в державному секторі 136 «Біологічні активи»: Наказ Міністерства фінансів України від 15.11.2017 р. № 943. URL: https://zakon.rada.gov.ua/laws/show/z1478-17(дата звернення: 01.11.2020).
19. Національне положення (стандарт) бухгалтерського обліку в державному секторі 121 «Основні засоби» : затверджене наказом Міністерства фінансів України від 12.10.2010 № 1202. URL: http://zakon3.rada.gov.ua/laws/show/z1017-10. (дата звернення: 13.11.2020).
20. Національне положення (стандарт) бухгалтерського обліку в державному секторі 127 «Зменшення корисності активів»: затв. наказом Міністерства фінансів України від 24.12.2010 № 1629. URL: http://zakon0.rada.gov.ua/laws/show/z0092-11 (дата звернення: 17.11.2020).
21. Гуцаленко Л.В. Можливості застосування справедливої вартості у вітчизняній обліковій системі. Збірник наукових праць Вінницького національного аграрного університету. 2012. Випуск 3. Том 2. С.40–46.

УДК 316.774

О. Терещенко, магістр гр. ІС-19М
Центральноукраїнський національний технічний університет

ОСНОВНІ ЕТАПИ КОМУНІКУВАННЯ ТЕЛЕКАНАЛУ З ГЛЯДАЧЕМ

У статті розглянуто особливості етапів комунікування телеканалу з глядачем. Звернуто увагу на порядок збору та аналізу інформації. Було з'ясовано шлях від вхідної інформації до випуску теленовин. Шлях трансформації інформації при роботі телеканалу «Прямий» - це її пошук та перевірка на правдивість, аналіз, переробка та створення новинного сюжету. Було розглянуто роботу телеведучих та особливості подачі інформації глядачам.
інформаційна діяльність, документ, документообіг, документаційне забезпечення, архів, номенклатура справ, опис справ

Постановка проблеми. У сучасному інформаційному суспільстві відбувається постійне збільшення потрібності комуні кування засобів масової інформації з глядачем.

Аналіз останніх досліджень і публікацій. Дослідженню проблем організації комуні кування за глядацькою аудіторією:Л.Ажнюк[1], Ван Дейк[2], А.Суходолов[3], , спільній праці О. Клишин, И. Максимальный [4] та ін.

Метою статті є розгляд основних етапів організації комуні кування телеканалу з глядачем.

Виклад основного матеріалу. На базі роботи журналістів телеканалу «Прямий» мною було вивчено методи ефективного пошуку та відбору інформації, яка в подальшому підлягає

аналітичній обробці. В першу чергу журналіст телеканалу при пошуку будь-якої інформації звертає увагу:

- яка організація займається питаннями, що цікавлять журналіста для отримання тієї чи іншої інформації,
- як вона організована,
- хто є ключовими фігурами (керівниками),
- хто може дати інформацію, яка відповідатиме дійсності.

Коли матеріал з'являється в полосі чи ефірі, необхідно перевірити його достовірність – проаналізувати посилання на джерело. В деяких випадках, інформація надається без вказівки на її походження, що часто зустрічається в передвиборчій боротьбі, чи це робиться для забезпечення конфіденційності джерела. Кращий варіант, коли інформатори не заперечують проти обнародування їх імен. Дуже часто журналіста попереджають: "Це не для друку". Що робити в таких випадках? Кореспондент умовляє співрозмовника залишити в матеріалі інформацію, яку інтерв'юер не бажає залишати. Якщо співрозмовник не піддається умовам – журналіст керується законодавством України.

Інколи плітки стають привидом для журналістського розслідування і наприкінці припиняють бути такими. На телеканалі «Прямий» такі випадки були у команди розслідувачів «Watchdogs. Розслідування»

До анонімних джерел інформації журналісти телеканалу ставляться дуже прискіпливо, або не використовують взагалі такі джерела, або ретельно перевіряють.

Один з самих розповсюджених методів для збору інформації це – співпраця з представниками органів влади. За даними центра Разумкова близько 80% журналістів українських ЗМІ звертаються в органи виконавчої влади. Деякі служби виконавчої влади постійно співпрацюють зі ЗМІ.

Під час збирання інформації у журналіста телеканалу «Прямий» існує декілька правил та способів перевірки інформації:

- коли матеріал готовий, необхідно передзвонити джерелу та, опираючись на текст, переперевірити цифри, факти, дані, імена тощо, та вголос прочитати все, а потім переспитати: "Чи правильно я все виклав?";
- по можливості отримані дані співставляють з існуючими відео-аудіо записами, текстовими документами;
- проводиться опитування допоміжних свідків;
- при необхідності текст дають на перевірку експертам;
- проводиться зачитування матеріалів досвідченим спеціалістам в редакції;
- якщо є така потреба текст дають на перевірку редакційному юристу.

Також мною були розглянуті способи отримання інформації журналістами телеканалу «Прямий». Під час збирання інформації журналіст зіштовхується з трьома проблемами: вибору самого надійного способу, фіксування отриманих даних, забезпечення техніки безпеки в роботі.

Зазвичай сучасні мас-медіа використовують три найрозповсюджених метода отримання інформації: інтерв'ю, спостереження, вивчення документів. Однак, самі надійні – інтерв'ю та спостереження.

В подальшому інформація потрапляє в руки редакторів телеканалу «Прямий», вони займаються аналізом і формуванням новин. Редактор керується соціологічними способами аналізу інформації. Алгоритм дій при використанні таких способів є наступним :

- спочатку редактор ознайомлюється з інформацією;
- співставляє список імен та організацій, які слід навідати;
- в цей список включає людей, що керуються різними точками зору, які цікавлять редактора;
- редактори діють за методом "відкритого забрала" (В. Аграновський), який забезпечує право "супротивника" на захист та народжує відчуття справедливості;
- намагаються звільнитися від гіду, яким постачають журналіста;

- ведуть розмови з джерелами інформації;
- наносять "визит вежливости" начальству;
- запасаються необхідною кількістю документів чи копій, стосовно тих чи інших питань чи подій.

Таким чином до формування новин потрапляє уже перевірена інформація, та зводиться до мінімуму трансляція недостовірної інформації глядачам.

Формування новин є найважливішою складовою випуску новин. У більшості випадків випуск новин на телеканалі «Прямий» укладається в формат 10-20 хвилин. У типовому випадку найбільш важливі новини потрапляють в початок випуску, сюжети нарисового плану, довші, більшого обсягу сюжети потрапляють в середню частину; культурні новини відходять на кінець випуску. Далі йде спортивний репортаж і прогноз погоди.

На телеканалі «Прямий» існують різні типи подачі події: репортаж, дикторська начитка та відеоряд, дикторська начитка на відеоряд та одне інтерв'ю, усна інформація, дикторська начитка та графіка.

Сюжети в новинах на телеканалі бувають різних видів. Випереджаючий сюжет роблять до настання події, він анонсує цю подію. Такий сюжет створює настрій очікування, дозволяє людям дізнатися про те, до чого їм слід готуватися. Існують також сюжети реального часу, тобто про те, що відбувається сьогодні. І третій тип – це сюжет за результатами якоїсь події.

Щоб наповнити передачу різноманітними сюжетами, телеканал має численні джерела інформації. Це приватні джерела, прес-відділи різних організацій, інформаційні служби, інформаційні агентства, інші ЗМІ, свідчення очевидців, телефонні опитування. Велику допомогу надають глядачі, які часто дають хороші ідеї.

Якщо є необхідність помістити рекламну паузу всередині випуску, глядачам повідомляється що вони побачать після реклами.

Прогноз погоди потрібен передачі новин тому, що цільовій аудиторії телеканалу (40+) ця інформація потрібна. Після прогнозу можна повідомити глядачеві додаткову інформацію, яка буде цікава власникам дач і городів.

Спортивна інформація розміщується наприкінці випуску новин, щоб глядач, який чекає саме її подивився всі інші сюжети. Винятки можуть становити лише події дуже великого масштабу, велика спортивна перемога яка важлива для країни.

До створення «кривавих» сюжетів редактори підходять дуже відповідально та тактично. Коректно показувати тільки тіла покриті пластиковими мішками, висвітлювати лише найважливіші деталі. Можна використовувати фотографії жертв в той момент коли вони були живі, архівні кадри.

Також на телеканалі «Прямий» дуже рідко показують неповнолітніх злочинців. Навіть якщо молода людина скоїв тяжкий злочин, не можна ставити на ньому клеймо.

Самогубство новини не висвітлюють, за винятком випадків, коли це відбувається з якоюсь важливою фігурою, наприклад, якщо мер міста наклав на себе руки.

Хочу зазначити що будь-який випуск новин неможливо уявити без телевізійного репортажу. Це унікальний жанр, що дозволяє показати подію, створити ефект присутності, який створює відчуття повної об'єктивності наданої інформації. Якісний телевізійний репортаж зрозумілий і логічний і несуперечливий від початку до кінця. Термін "репортаж" походить від французького "reportage" і англійського "report", що означає повідомляти. Загальний корінь цих слів - латинський ("reporto" - передавати).

Репортаж – найоперативніший жанр донесення інформації на телеканалі «Прямий». Його популярність пояснюється насамперед максимальною наближеністю до життя, здатністю передавати явища реальної дійсності. Телерепортаж об'єктивний за своєю природою, тому що відеокамера фіксує тільки те, що відбувається насправді. Однак в закадровому тексті репортера завжди відчувається суб'єктивне сприйняття автором того, що відбувається, і воно нерідко виходить на перший план. Тому можна говорити про те, що репортаж - це все-таки жанр суб'єктивний.

Як і інші жанри журналістики, репортаж повідомляє про новини. Але істотним його відмінністю є факт обов'язкової присутності на місці дії автора - репортера, тобто людини зі своєю точкою зору.

Телерепортаж здатний показати так подію яка набито відбувається в реальному часі що глядач ніби стає очевидцем події. Тому журналісту немає необхідності описувати подію - цю функцію виконує відеоряд. Репортер в закадровому тексті розповідає про подробиці події - причини і наслідки, проводить аналогії, шукає зв'язок з іншими подіями. Словом говорить про неочевидне, але важливе.

Варто відзначити і той факт, що телевізійний сюжет створює ціла команда. Якщо газетяр може один побувати на місці події і підготувати матеріал, то створення телерепортажу вимагає залучення значних сил служби новин: оператора, режисера, монтажерів.

За способом трансляції розрізняють прямий і фіксований репортажі. Прямий репортаж транслюється в ефір в момент вчинення дії. Неможливість показати подію в момент її вчинення або в її реальному часовому обсязі (простіше кажучи, якщо дія затягується, а його інформаційна цінність поступається цінністю ефірного часу) вимагає його фіксації.

За способом подачі репортажі діляться на коментовані або без коментарів. Репортаж без коментарів, або трансляція - це найпростіша різновид репортажу. Він повністю позбавлений закадрового авторського тексту і використовується в прямому ефірі при показі найважливіших суспільно-політичних і культурних подій де глядачам все зрозуміло і без коментарів. Але коли подія незрозуміло без пояснень репортера, застосовується коментований репортаж, де репортер пояснює те, що відбувається на екрані за допомогою закадрового тексту.

Таким чином формується випуск новин на телеканалі «Прямий»

Ведучий це обличчя голос і стиль програми новин. Основні характеристики роботи ведучого новин на телеканалі «Прямий» - це престижність і відповідальність. Ведучий новин має вселяти симпатію і вільно триматися в кадрі. Його поведінка повинна бути демократичною, але не вульгарною. Завдання ведучого - вміло, з розумінням і тактовно подати новини, підготовлені його колегами. Дуже важливими є чітка дикція і виразна інтонація. Професійний ведучий інтелігентний і ерудований, вміє «зберегти обличчя» в будь-якій ситуації, дає глядачам впевненість в тому, що вони отримують найбільш достовірну, найоб'єктивнішу інформацію.

На відміну від радіомовлення, яке не створює видовищної наочності поведінки диктора в студії, на телеекрані ми маємо справу з «розкритим», видимим в реальному часі провідним, оживляючих повідомлення картиною практичних дій. Інформація немов приходить у міру того, як останній дає їй життя, роблячи це на наших очах. В результаті інформаційний випуск стає зримою демонстрацією активної безпосередності поведінки, в якому щохвилини породжується та чи інша новина.

При всьому характер поведінки ведучого новин в кадрі має місце елемент творчості, оскільки в нових умовах від самого ведучого залежить, що саме він «зробить» в кадрі. Оцінка рольової поведінки залежить від спостережливості телеглядачів та від уміння ведучого триматися, виробляти вигідне враження, приховуючи видимі елементи гри.

Ведучий на телеканалі вміє подати новину так, немов це сталося на його очах. Можна навчитися вести поглядом по рядках телесуфлера, але не так просто виглядати берегинею інформаційного вогнища в студії, як це робить Христина Чернега. У веденні інформаційного випуску текст значною мірою сприяє виразності телеведучих.

Телеаудиторія - це невидима аудиторія. З цієї причини, звертаючись до неї в інформаційному випуску, супроводжуючи різні відеосюжети, телеведучий виходить за межі простору студії. Вміючи бачити просторове ціле телеефіру, він у самому собі набуває нової якості зримості, для якого невидимого в умовному сенсі вже не існує.

Якісна новинна програма має свій сценарний склад і стиль виробництва, послідовний і добре впізнаваний графічний стиль, яскравих ведучих у студії і репортерів на виїзді. У сюжетах необхідно використовується інтершум (термін, що вживається в журналістиці, шум із місця, де відбувалося знімання, «задній план» знімання. Наприклад, під час запису репортажу з футбольного матчу – звуки на стадіон), графічні елементи.

Музика в сюжеті може звучати насправді або на фоні. Крім того, обов'язково присутня музика для початку програми, музика всередині між програмами. Існує поняття "шапка новинного блоку", її використовують на виході з рекламної паузи, коли повертаються до змісту новин. Вона триває всього 3 секунди, але це слухова підказка для глядача про те що новини поновилися.

Після кожного випуску новин у глядачів телеканалу «Прямий» повинен залишатися гарний настрій та легке відчуття. Тому навіть якщо доводиться говорити про проблеми і складнощі, закінчувати випуск намагаються простим і приємним для сприйняття сюжетом. В кінці можна оголосити, про що розкажуть новини завтра. Крім анонсу сюжетів, які глядачі побачать в наступному випуску, багато нагадують глядачам про найважливіші події сьогоднішнього дня. Крім того, рекомендується починати і закінчувати випуск провідними в кадрі. Адже ведучі програми - це господарі, які повинні зустрічати і проводжати гостей, тобто бути на вході в програму і на виході.

Композиційна побудова інформаційної програми представляє «суцільну» сполучну тканину, властивої тому текстово-сюжетної передачі повідомлень, і вимагає від ведучого вміння перейти від зовнішньої виразності в реакціях і рухах до розуміння колізій різних подієвих контекстів, створюючи особливий ритм характерної уваги, діалогірованних форм звернень, підводок.

Таким чином, для створення якісної інформаційної програми необхідно знати особливості збору і аналізу інформації, якісно перероблювати її, створювати професійні сюжети, враховувати мовну специфіку та правильно підбирати провідних ведучих. Сукупність цих компонентів принесе успіх телевізійної компанії.

Список літератури

1. Ажнюк Л.В. Конфліктний медійний текст як об'єкт лінгвістичної експертизи / Л.В. Ажнюк // Актуальні проблеми української лінгвістики : теорія і практика. – 2013. – Вип. 27. – С. 18-32
2. Ван Дейк Т.А. Язык. Познание. Коммуникация / Т.А. Ван Дейк. – М., 2000.
3. Суходолов, А. П. Феномен «фейковых новостей» в современном медиапространстве / А. П. Суходолов // Евроазиатское сотрудничество: гуманитарные аспекты. — 2017. — С. 87–106.
4. Клишин, И. Максимальный ретвит: Фейк-пропаганда на новом уровне / И. Клишин // URL: https://www.vedomosti.ru/newspaper/articles/2014/02/12/fejk-propaganda-na-novom-urovne (дата обращения: 30.11.2018).

УДК 621.787

М. Мацаєнко, магістр гр. МЗ-19М (1,4)
Центральноукраїнський національний технічний університет

СПОСОБИ ВІДНОВЛЕННЯ ВНУТРІШНЬОЇ ПОВЕРХНІ ШАТУННИХ ВТУЛОК

Розглянуті існуючі методи відновлення внутрішньої поверхні шатунних втулок, які виготовлені з дефіцитних бронз. Визначено, що найбільш перспективним та таким, що не потребує складаного обладнання, є спосіб вібраційного розкочування. Для отримання точності розмірів і шорсткості поверхні доцільне використання комбінованої технології. Таким чином, для збільшення опорної площі поверхонь відновлених вібророзкочуванням зі збереженням підвищеної маслоемкості можливе використання в якості фінішної операції високопродуктивного способу - деформуючого протягування
бронзові втулки, вібраційне розкочування, деформуюче протягування, маслоємність

Шатунні втулки двигунів внутрішнього згорання виготовляють з дорогих, дефіцитних бронз (Бр ОЦС 5-5-5, Бр ОЦС 4-4-2,5) та відносяться до числа швидкозношуваних деталей. Ці фактори, а також з огляду на їх велику кількість (число втулок на один двигун становить 4 ... 8), вага (ремонтна втулка шатуна двигуна ЯМЗ-236 важить 0,214 кг) і те, що при ремонті двигунів на багатьох ремонтних заводах все втулки замінюються на нові, роблять проблему відновлення шатунних втулок актуальною.

Невеликі габаритні розміри відновлюваної поверхні втулки (діаметр близько 40 ... 50 мм, довжина 45 ... 55 мм), малі допустимі радіальні зноси (менше 0,1 мм) і важкі умови роботи (граничне тертя при високих питомих тисках і навантаженнях з наявністю абразиву) обмежують використання ряду відомих для відновлення внутрішніх поверхонь втулок способів [1].

З урахуванням вищевикладених особливостей розроблена класифікація існуючих способів, які можна застосувати для відновлення шатунних втулок (рис.1). Відповідно до цієї класифікації всі способи можна розділити на дві основні групи:

- відновлення втулок нанесенням покриттів на зношені внутрішні поверхні;
- відновлення розмірів отвору втулок пластичним деформуванням.

Більшість цих методів широко відомі і детально описані в літературі [2 - 4].

Стосовно до відновлення внутрішніх поверхонь спосіб вібраційного розкочування представляється найбільш перспективним, однак раніше він вивчався мало, а до відновлення отворів шатунних втулок взагалі не розглядався.

В основі способу вібраційного накочування покладено процес холодного пластичного деформування, що відрізняється від відомої схеми накочування тим, що інструменту - кулі або алмазному сферичному наконечнику, крім руху подачі, надається додатковий осцилюючий рух уздовж твірної оброблюваної заготовки. Цей метод поверхневого пластичного деформування (ППД) досить широко використовується в машинобудуванні [5].

Найбільше застосування спосіб вібронакочування отримав для обробки зовнішніх (обкатування) і внутрішніх (розкочування) циліндричних поверхонь деталей - тіл обертання. Обладнанням для цього способу ППД служить токарно-гвинторізний верстат і віброголовка. Основним призначенням віброголовки є надання осциляційного руху деформуючому елементу. За способом створення осциляційного руху вібраційні пристрої поділяють на електромеханічні, електромагнітні, поршневі (пневматичні, гідравлічні), фрикційно - електричні.

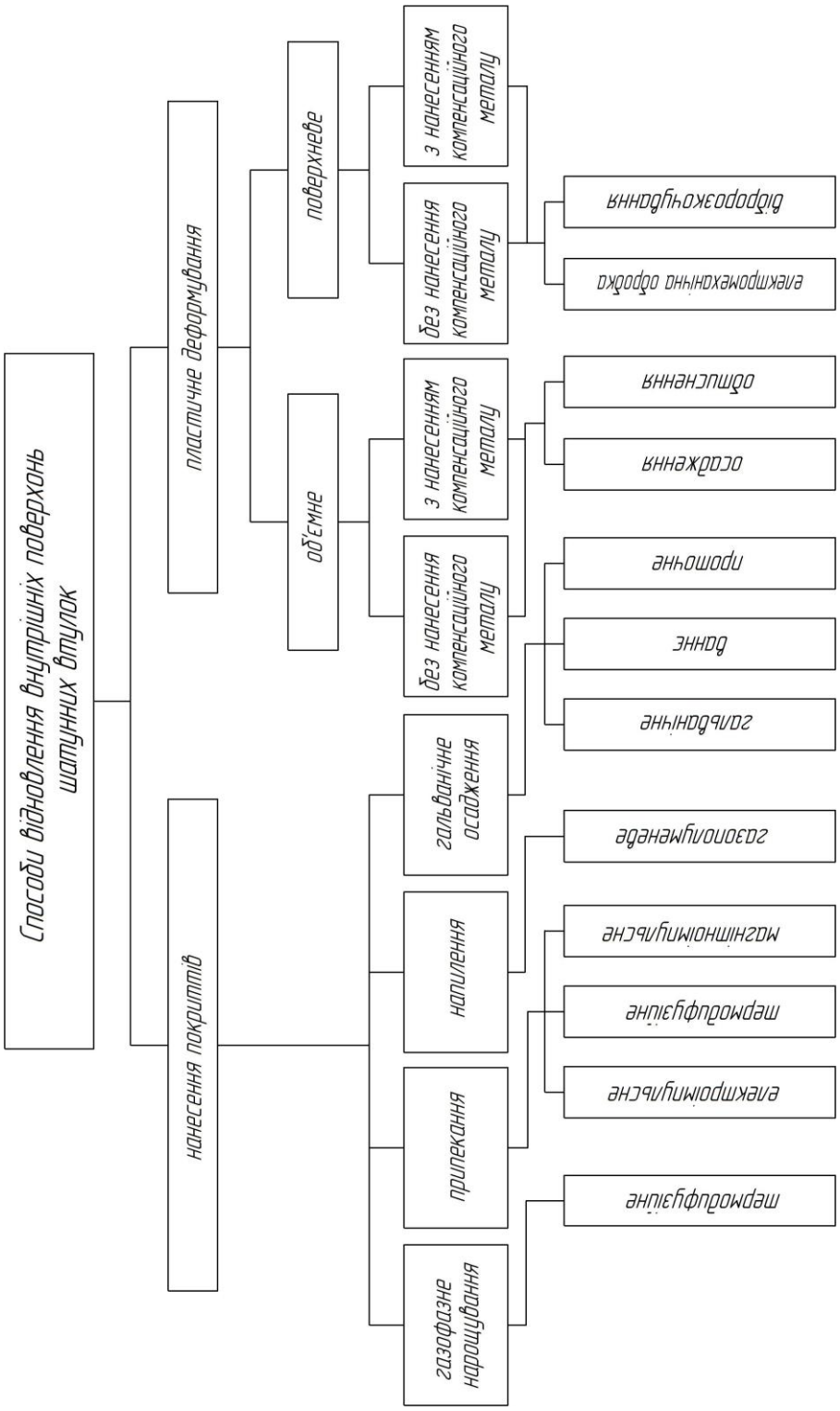


Рисунок 1 – Класифікація способів відновлення внутрішніх поверхонь шатунних втулок

Параметри, що визначають режим вібронакочування, призначають за заданими характеристиками мікрорельєфу: характеру малюнка, ширині *b* і глибині *h* канавок, відносної площі канавок [5, 6].

Таким чином, вібронакочування як зовнішніх, так і внутрішніх поверхонь в порівнянні з обкочуванням (розкачування) має такі переваги: отримання більшого деформаційного ефекту при одних і тих же зусиллях деформування; нанесення повністю нового, аналітично розрахованого регулярного мікрорельєфу зі збільшеними радіусами виступів і западин елементів регулярного мікрорельєфу; утворення шару з підвищеною маслоемністю і опорною поверхнею, що робить можливим його використання для відновлення деталей, виготовленими з пластичних металів з незначними зносами.

Разом з тим, слід зазначити, що спосіб вібраційного розкочування вимагає завершувальної операції механічної обробки (розточування, шліфування і т.д.) з метою отримання точності розмірів і шорсткості поверхні. Отже, для відновлення внутрішніх поверхонь бронзових втулок доцільне використання комбінованих способів обробки.

Для збільшення опорної площі поверхонь відновлених вібророзкочуванням зі збереженням підвищеної маслоемкость можливе використання в якості фінішної операції високопродуктивного способу ППД - деформуючого протягування, відомого завдяки роботам Розенберга О.М. та його учнів [7, 8].

Отже, доцільним представляються нанесення на внутрішню поверхню бронзових втулок регулярного мікрорельєфу з подальшим деформуючим протягуванням.

Список літератури

1. Пахомов Е.В., Антропов С.Ф. Восстановление бронзових втулок// Техника в сельском хозяйстве. – 1987, №1. – С.39 – 40.
2. Пиявский Р.С. Восстановление втулок верхней головки шатуна// Техника в сельском хозяйстве. – 1982, №3. – С.37 – 39.
3. Рыжов Э. В. Технологическое обеспечение качества деталей с покрытиями / Э. В. Рыжов, С. А. Клименко, О. Г. Гуцаленко. – К.: Наукова думка, 1994. – 181 с.
4. Харламов Ю.А. Основы технологии восстановления и упрочнения деталей машин / Ю. А. Харламов, Н. А. Будагьянц. – Луганск : Восточно – украинский Национальный университет, 2003. – 480 с.
5. Шнейдер Ю.Г. Эксплуатационные свойства деталей с регулярным микрорельефом. - Л.: Машиностроение, 1982. – 248 с.
6. Наливайко В.Н., Шепеленко И.В., Русских В.В. Прирабатываемость поверхностей с регулярным микрорельефом// Проблеми трибології. – Хмельницький: ТУП. - 2001, №1. – С.44 – 51.
7. Розенберг А.М. Механика пластического деформирования в процессах резания и деформирующего протягивания / А.М. Розенберг, О.А. Розенберг; отв. ред. П.Р. Родин. – К.: Наук. думка, 1990. – 320 с.
8. Посвятенко Е.К. Протягування та протяжний інструмент: монографія/ Е.К. Посвятенко, Я.Б. Немировський, І.В. Шепеленко. Кропивницький: Видавець Лисенко В.Ф., 2020. – 298 с.

УДК 621.891.539.375.6

В. Мошнягул, магістр гр. МЗ-19М (1,4)
Центральноукраїнський національний технічний університет

МЕТОДИ ВІДНОВЛЕННЯ ЦАПФ ШЕСТЕРЕНЬ ГІДРОНАСОСІВ

Розроблена класифікація існуючих методів, застосування яких можлива для фінішної обробки цапф шестерень. Значно підвищити експлуатаційні властивості деталей можна за рахунок використання комбінованих методів обробки, суть яких полягає в сумарному впливі фізичних і хімічних факторів та способів їх підведення в зону обробки, що дозволяє досягти більш високі експлуатаційні властивості деталей. Визначено, що найбільш перспективним є спосіб фінішної антифрикційної безабразивної обробки. Зазначено, що для підвищення продуктивності обробки та якості покриття слід ускладнити кінематику рух інструменту, а саме інструмент у процесі обробки повинен мати обертальний рух і осциляцію.
цапфа шестерні гідронасосів, фінішна антифрикційна безабразивна обробка, якість обробки, комбінована обробка

Прийнятий технологічний процес механічної обробки цапфи шестерні гидронасосів включає наступні операції:

- токарна;
- шліфувальна;
- суперфінішування;
- доведення.

Проведені дослідження показали, що при виготовленні та ремонті цапф шестерень на більшості підприємств в якості фінішної обробки використовують шліфувальну операцію з наступним доведенням до отримання шорсткості поверхні Ra=0,16 мкм.

Фінішна обробка використовується для отримання заданої шорсткості поверхні деталі та виконується, як правило, в межах допуску попередньої обробки, однак на точність обробки вплив майже не має. Фінішна обробка при різних методах і оброблюваних матеріалах повинна забезпечити шорсткість поверхні Ra=0,63 ... 0,16 мкм.

На підставі аналізу літературних джерел розроблена класифікація існуючих методів, застосування яких можлива для фінішної обробки цапф шестерень (рис.1). Відповідно до цієї класифікації, методи фінішної обробки цапф шестерень можна розділити на наступні основні групи:

- обробка лезовим інструментом;
- обробка абразивним інструментом;
- електрофізична обробка;
- електрохімічна обробка;
- обробка поверхневим пластичним деформуванням;
- комбінована обробка.

Більшість цих методів широко відомі та детально висвітлені в літературі [1-4 та інш.]. Значно підвищити експлуатаційні властивості деталей можна за рахунок використання комбінованих методів обробки [5], суть яких полягає в сумарному впливі фізичних та хімічних факторів та способів їх підведення в зону обробки, що дозволяє досягти більш високі експлуатаційні властивості деталей. До одних з таких методів слід віднести фінішну антифрикційну безабразивну обробку (ФАБО) [6]. Під ФАБО розуміють різні способи фінішної обробки, засновані на використання в процесі тертя явищ схоплювання поверхонь та вибіркового перенесення.

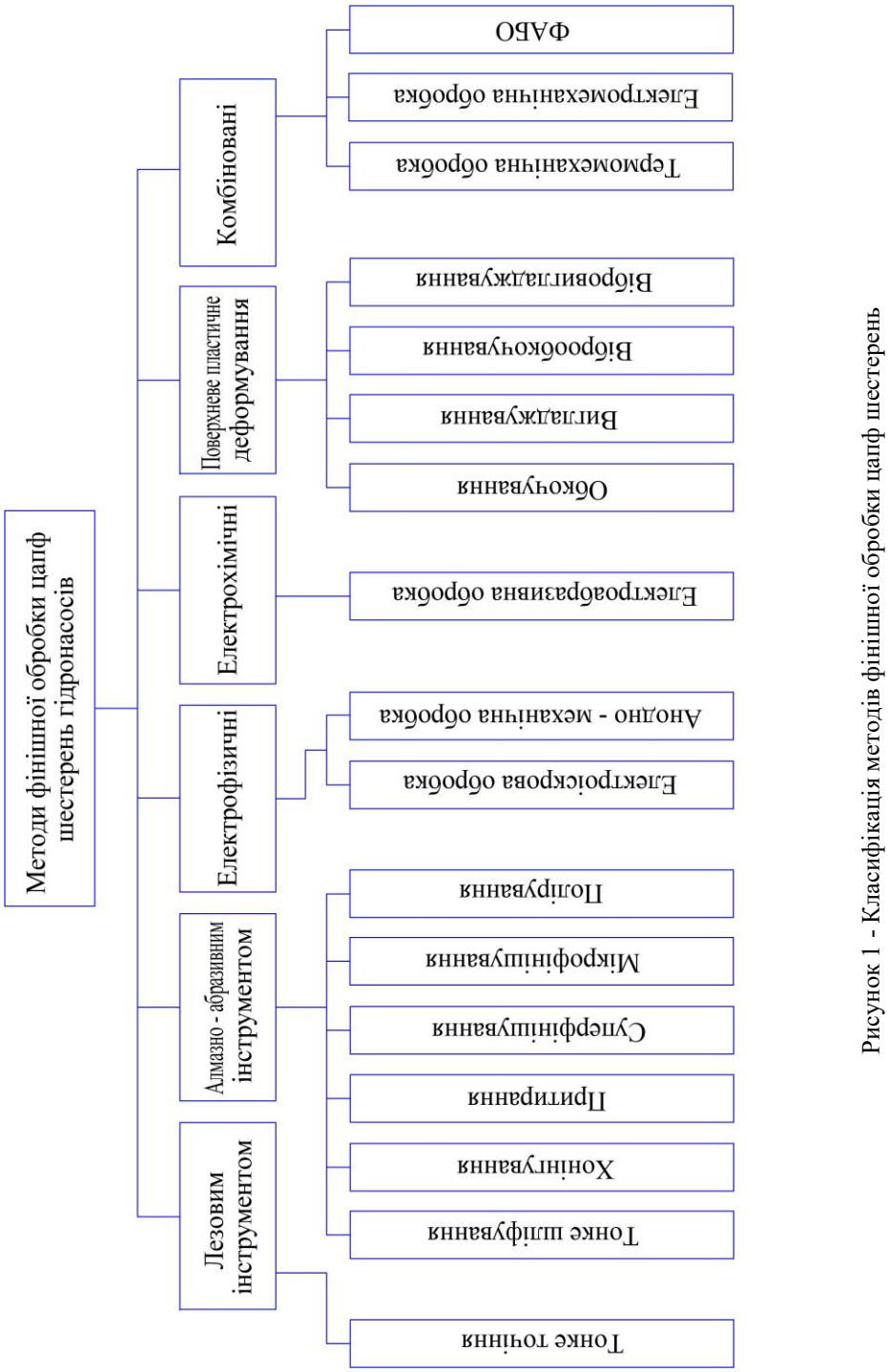


Рисунок 1 - Класифікація методів фінішної обробки цапф шестерень

В якості фінішної обробки ФАБО представляється найбільш перспективною, оскільки поряд з формуванням необхідної шорсткості на поверхні тертя утворюється тонкі припрацювальні покриття. Однак різні модифікації цього методу обробки вимагають подальших досліджень.

ФАБО застосовується з метою зниження інтенсивності зношування, підвищення задиростійкості поверхонь тертя та інтенсифікації процесів утворення захисних плівок у період припрацювання після виготовлення або ремонту виробу.

Простота і технологічність способу ФАБО визначила його застосування для поліпшення триботехнічних властивостей поверхонь, що піддаються зношуванню. У той же час більшість робіт, присвячених ФАБО, ґрунтуються на емпіричному матеріалі з вибору технології нанесення, складу технологічного середовища, матеріалу інструмента та режимів обробки. До недоліків існуючого технологічного процесу варто віднести низьку

продуктивність, часту заміну прутка через його нерівномірне зношування. Нерівномірне зношування інструмента можна ліквідувати тільки при провертанні інструмента в процесі ФАБО. Низька продуктивність процесу полягає в тому, що швидкість відносного переміщення інструмента і деталі забезпечується тільки обертанням деталі. Підвищити продуктивність ФАБО можна за рахунок збільшення швидкостей відносного переміщення інструмента - деталь і створенням поздовжньої осциляції інструмента в процесі ФАБО [7]. Це дозволить прискорити процеси ФАБО, не знижуючи якості самого процесу.

З огляду на ці недоліки, інструмент у процесі ФАБО повинен мати обертовий рух і осциляцію. Це ставить необхідністю вдосконаленні технології та інструменту для нанесення покриттів методом ФАБО.

Список літератури

1. Кремень З. И. Технология шлифования в машиностроении / З.И.Кремень, В. Г. Юрьев, А. Ф. Бабошкин. – М. : Политехника, 2007. – 424 с.
2. Афонькин М. Г. Производство заготовок в машиностроении / М.Г. Афонькин, В. Б. Звягин. – М. : Политехника, 2007. – 384 с.
3. Харламов Ю.А. Основы технологии восстановления и упрочнения деталей машин / Ю. А. Харламов, Н. А. Будагьянц. – Луганск : Восточно – украинский Национальный университет, 2003. – 480 с.
4. Горохов В. А. Обработка деталей пластическим деформированием / В. А. Горохов. – К. : Техніка, 1978. – 191 с.
5. Черновол М.И. Комбинированный метод обработки поверхностей трения/ М.И.Черновол, И.В.Шепеленко, Варума Арифа// Техніка в сільськогосподарському виробництві, галузеве машинобудування, автоматизація. – Кіровоград: КНТУ, 2011. – Вип.24, Ч.II. – С.13-16.
6. Гаркунов Д. Н. Триботехника (износ и безызносность): учебник/ Д.Н.Гаркунов. – М.: МСХА, 2001. – 616 с.
7. Черкун В.В. Підвищення зносостійкості цапф шестерень гідронасосів фінішною антифрикційною безабразивною обробкою: автореф. дис. на здобуття наук. ступеня канд. техн. наук: спец. 05.02.04 «Тертя та зношування в машинах»/ В.В. Черкун. – К., 2011. – 19 с.

УДК 621.43.06

О. Степанов, магістр гр. АТ 19М
Центральноукраїнський національний технічний університет

АНАЛІЗ УМОВ РОБОТИ ТА НЕСПРАВНОСТЕЙ ТУРБОКОМПРЕСОРІВ АВТОМОБІЛЬНИХ ДВИГУНІВ

Проведений аналіз основних несправностей турбокомпресорів та причин їх виникнення. Встановлено діагностичні ознаки несправностей турбокомпресорів. Основними найбільш вагомими несправностями слід вважати пошкодження крильчаток ротора, зношування вала ротора, зношування упорного підшипника, зношування байпасного клапана, витікання масла з турбіни. Розглянуто процеси дефекації зносів деталей турбокомпресора.
турбокомпресор, двигун, турбонаддув, система впуску

Постановка проблеми. Концепція розвитку автомобільного транспорту передбачає збільшення потужності двигунів автомобілів при зниженні витрат палива і викидів в атмосферу продуктів згоряння. Для досягнення поставлених цілей автомобільні двигуни оснащуються турбокомпресорами (ТКР), охолоджувачами надувного повітря (інтеркулерами), акумуляторними системами подачі палива, електронними елементами управління і вбудованими системами самодіагностики.

Система газотурбінного наддуву (ГТН) автомобільних дизелів в класичному її конструктивному виконанні складається з двигуна, турбіни і компресора. Між турбіною і компресором має місце механічний зв'язок, а між турбіною і двигуном - газовий. При відносно простій конструктивній схемі і нескладному принципі дії турбокомпресора, визначення його технічного стану в процесі експлуатації є непростим завданням. Несправності в будь-якому з елементів поступово розвиваються в процесі експлуатації і зовні помітно не виявляються, на певних режимах роботи можуть привести до відмови турбокомпресора, або двигуна в цілому.

Складність діагностування турбокомпресора визначається багатьма причинами. По-перше, показники ефективності функціонування ТКР в експлуатації залежать як від технічних і режимних характеристик двигуна, так і самого турбокомпресора. По-друге, до цих пір практично відсутні надійні інструментальні засоби контролю технічного стану турбокомпресора в експлуатації. Визначення найбільш інформативних функціональних параметрів турбокомпресора, встановлення їх граничних значень, розробка методів і засобів їх контролю є першорядним при технічному сервісі двигунів мобільної сільськогосподарської техніки.

Аналіз останніх досліджень та публікацій. Проблемою вдосконалення методів і засобів діагностування двигунів мобільної сільськогосподарської техніки займалися В. В. Альт, В. Й. Бєльських, С. Н. Боричів, Н. В. Бишів, І. І. Габбітов, І. П. Добролюбов, Н. С . Жданівський, Г. Д. Кокорєв, А. П. Іншаков [1-4], В. В. Лянденбурскій, В. М. Михлин, А. В. Ніколаєнко, А. В. неговори, С. Н. Ольшевський, К. Ю. Скібневскій, А. П. Савельєв, О. Ф. Савченко, І. П. Терських, І. А. Успенський та інші. Однак більшість методів діагностування технічного стану турбокомпресорів до сих пір не достатньо опрацьовані, не враховують повною мірою особливостей їх функціонування, відрізняються досить високою вартістю і складністю застосовуваного обладнання.

Мета і завдання досліджень. *Метою роботи є* розробка методів контролю технічного стану турбокомпресорів двигунів автомобілів.

Для досягнення поставленої мети вирішувалися наступні *завдання* досліджень:

1. Ідентифікувати несправності турбокомпресорів
2. Дослідити причини виникнення дефектів турбокомпресорів.

Провести комплексний аналіз взаємозв'язків оціночних показників правильного функціонування ТКР, існуючих методів і засобів їх діагностування..

Об'єкт дослідження – функціональні параметри турбокомпресорів автомобільних двигунів.

Предмет дослідження – закономірності зміни показників функціонування турбокомпресорів в експлуатаційних умовах.

Методи досліджень базуються на вивченні процесів зношування деталей автомобільних турбокомпресорів.

Потужність двигуна внутрішнього згоряння багато в чому визначається ступенем стиснення робочої суміші. У атмосферному ДВЗ (без турбонаддуву) поршень стискає суміш, початковий тиск якої дорівнює атмосферному. Якщо на початку такту стиснення в циліндр подати повітря і підвищити цей тиск, скажімо, на 2 бари, то ступінь стиснення збільшиться, а потужність звичайного серійного двигуна підвищиться до 30-50%.

Турбокомпресор (ТК) служить для подачі в камеру згоряння повітря під надлишковим тиском.

Повітря в турбіну забирається з повітряного фільтра через витратомір. У корпусі компресора воно розкручується і під впливом відцентрових сил, що забезпечують необхідний надлишковий тиск, потрапляє у впускний колектор двигуна.

Найбільш вразливий вузол турбокомпресора - це підшипник і ротор, тобто обидві крильчатки, з'єднані валом. Вони працюють в критичних режимах. Швидкість ковзання вала в підшипнику досягає 70 м/с. Окружна швидкість лопатей доходить до 600 м/с. На таких надзвукових режимах потрапляння найменшого стороннього предмета виводить

турбокомпресор з ладу. Тому для його нормальної роботи потрібне високе очищення, по-перше, повітря, а по-друге - мастила, що подається під розрахунковим тиском у підшипники. Самий незначний перебій з подачею масла виводить ротор з ладу: при таких оборотах без мащення будь-який підшипник миттєво згорить. Найменші частки сажі або масла з двигуна, тим більше - окалина або шматочки поршневих кілець, можуть пошкодити крильчатку. Тобто, для нормальної роботи турбокомпресора поршнева група двигуна повинна бути справна.

Крім того, дуже високі вимоги висуваються до матеріалу, з якого виготовляються крильчатки. Турбінна, наприклад, повинна витримувати температуру від 900° С і вище (в деяких турбінах робоча температура досягає 1100° С). Тому вона робиться з термостійкого кобальто-нікелевого сплаву.

Компресорна крильчатка кріпиться до валу гайкою через набір спеціальних шайб (одна з них працює в парі з опорним підшипником, а в другій є канавка під компресійне кільце, яке утримує масло з боку компресора). Вона виготовляється з високоякісного алюмінієвого сплаву, і повинна протистояти атмосферній корозії, витримувати дуже високі відцентрові навантаження, а також не деформуватися в процесі роботи, тобто її матеріал володіє дуже високою межею текучості.

Вал виготовляється зі сталі і зварюється з турбінною крильчаткою методом зварювання тертям. Відбувається це наступним чином: крильчатка обертається на верстаті, вал нерухомий. У зону контакту подається електричний струм (для такого зварювання нагрівання одним тільки тертям недостатньо), пара нагрівається, обертання різко припиняється, з'єднання зварюється і охолоджується. Потім заготовку обробляють на токарному верстаті, після чого вона проходить термічну обробку з наступним шліфуванням, накатуванням різьби, фінішним поліруванням і двоступеневим балансуванням. Дана технологія дуже точна, відповідальна, дорога і проводиться на спецобладнанні.

Несправності, що підлягають усуненню при ремонті турбокомпресора, виникають як в корпусі (підлягають відновленню посадочні місця під підшипники, компресійні кільця), так і у деталей ротора (знос опорного підшипника, втулок, компресійних кілець і канавок під них, опорного підшипника, ротора).

Пошкодження крильчаток ротора. Негерметичність систем впуску та випуску також викликає небезпечні перепади тиску. А банальна економія на заміні повітряного фільтра або несвоєчасне усунення підсосу повітря за його корпусом призводять до зносу компресорного колеса турбіни. Його лопатки сточуються потрапляють в середину частинками піску.

Поширена причина виходу ТКР з ладу - потрапляння сторонніх предметів в крильчатки. Часом це трапляється через недбалість механіка, який при обслуговуванні машини залишив ганчір'я або впустив всередину шайбу, або через непередбачене руйнування деталей двигуна, коли, наприклад, відвалюється електрод від свічки. Вал турбіни обертається з величезною швидкістю, і потрапляючи на крильчатки сторонні предмети значно їх деформують, через що турбіну може навіть заклинити. В результаті ротор ламається навпіл від скручування. В цьому випадку ремонтувати агрегат не має сенсу.

До характерних пошкоджень крильчаток і вала призводить так зване перекручування турбіни, тобто перевищення допустимих обертів. Перекручування може бути спровоковане і певним збігом обставин. Наприклад, через помилкові показання датчика витрати повітря з запізненням спрацьовує механізм регулювання тиску наддуву. ТК працює в дуже жорстких умовах (взяти хоча б термічне навантаження), і навіть незначне відхилення від допустимих режимів призводить до непоправних наслідків.

Зношування валу ротора. Описані вище причини відмов турбін зустрічаються не так часто, основна частка припадає на несправності в системі мастила ТК. У зазорах між валом турбіни і його підшипниками повинен бути присутній масляний клин, інакше відбувається перегрівання і знос валів, підшипників і ущільнень - внаслідок контактної роботи елементів. Найчастіше вихід з ладу турбіни настає через масляне голодування і наявність сторонніх часток в маслі.

ТКР дуже чутливий до чистоти і якості масла - більше, ніж двигун, в основному через те, що цей вузол працює в важких температурних режимах. Зокрема, на бензинових двигунах відпрацьовані гази розігріваються аж до 1000°С. Тому збільшені інтервали заміни масла і економія на фільтрі насамперед скорочують ресурс ТКР.

Масляне голодування турбіни має масу причин, про які мало хто замислюється. Одна з найпоширеніших - закоксовування підвідної трубки. Найчастіше вона забивається повністю - і ТКР працює на сухо. Не менш важлива справність масляного насоса двигуна, а також системи вентиляції картера. Часто саме через неї турбіна непомітно виходить з ладу. Масло в корпус підшипників ТКР надходить під тиском близько 4 бар, а зливається з нього в піддон двигуна самопливом. І, навіть незначне підвищення тиску картерних газів, сильно обмежить витрату мастила через турбіну, знижуючи несучу здатність його плівки, і призведе до його просочування через ущільнення. Нерідко це відбувається через несправний клапана вентиляції.

Зношування вала ротора, головним чином, відбувається через недостатню подачу масла в зону тертя. В результаті цього з’являються глибокі задири на валу в місцях посадки підшипників і навіть в зоні газодинамічного ущільнення.

При серйозних пошкодженнях корпусу відновлювати турбіну економічно недоцільно. Швидше за все, всередині все набагато гіршими.

Зношення упорного підшипника. Упорний підшипник вала турбіни страждає через критичний перепад тиску на сторонах впуску та випуску. Це призводить до збільшення осьового люфту ротора з усіма наслідками, що випливають.

Зношування байпасного клапана. У турбін бензинових двигунів на сідлах байпасного клапана часто з'являються тріщини.

Витікання масла з турбіни (маслогон). У турбіні замість сальників на кінцях вала використовують газодинамічні ущільнення. Їх завдання - ізолювати центральний корпус ТК від впускної і випускної систем двигуна, тобто від холодного та гарячого корпусу турбіни. Тиск відпрацьованих газів і впускного повітря в певних режимах роботи мотора дуже високий, і без ущільнень вони «наддувалися» в картер двигуна через зливну масляну трубку турбіни.

За принципом роботи і конструкцією газодинамічні ущільнення схожі з поршневими компресійними кільцями. Вони встановлені нерухомо в корпусі турбіни і ізолюють порожнини тільки при обертанні вала, але не стикаються з ним, маючи певний зазор. Ці кільця не герметичні повністю і пропускають частину газів.

На деяких режимах роботи будь-якої турбіни виникає поєднання високого тиску відпрацьованих газів і надмірне зріджування на впуску. Через такий перепад тиску можливе проривання частини газів з гарячого корпусу в холодний. Разом з собою на «вхідну» сторону вони переносять і масляний туман, який виходить з корпусу підшипників і йде на зливання. Це і викликає запотівання стиків патрубків турбіни. Обсяг «маслогона» не нормується - він залежить від конкретної моделі турбіни і режимів роботи двигуна.

Дефектація. Важливе значення при ремонті має процес дефектації деталей.

Спочатку турбокомпресор надходить на розбірний стіл, де розбирається і дефектів. Потім його деталі піддаються двоступеневому очищенню. Піскоструминній обробці піддаються деталі зі слідами іржі, пригорілого масла, окалини, корозії.

Далі дефектують деталі. До подальшої роботи буде придатний ротор, який не має слідів торкання крильчатки по корпусу турбіни. По-друге, якщо у нього канавка під компресійне кільце розбита більше певного допуску, такий ротор слід замінити. Якщо ротор зігнутий на більш ніж 0.02 мм, він теж вибраковується. Про його непридатність до подальшої роботи свідчать і сліди припалів через відсутність мастила, оскільки через перегрівання сталь могла відпуститися, тобто втратити твердість. Вибракування проводиться візуально і за допомогою мікрометричних вимірювань і перевірки допусків. У деяких випадках, наприклад, якщо вал має деформацію, його розглядають під мікроскопом на предмет виявлення тріщин.

Висновки. В результаті аналізу літературних джерел виділено найбільш значущі фактори, що впливають на зношування деталей турбокомпресорів автомобільних двигунів. В даній роботі встановлено причини виникнення дефектів деталей турбокомпресорів автомобільних двигунів та їх наслідки та вплив на роботу двигуна.

Список літератури

1. Иншаков А. П. Автоматизированный комплекс для диагностирования систем наддува воздуха в двигателях МЭС / А. П. Иншаков, А. Н. Кувшинов, И. И. Курбаков // Тракторы и сельхозмашины. - 2012. - № 10. - С. 16 - 18.
2. Иншаков А. П. Диагностика турбокомпрессоров на стенде КИ-5543/ А. П. Иншаков, А. Н. Кувшинов, И.И. Курбаков, О.Ф. Корнаухов // Сельский механизатор. - 2013. - №12. - С. 39.
3. Иншаков А. П. Программный комплекс «ДИЗЕЛЬ РК» / А. П. Иншаков, И.И. Курбаков // Сельский механизатор. - 2013. - №12. - С. 45.
4. Иншаков А. П. Способ диагностирования системы воздухопадачи тракторного дизеля / А. П. Иншаков, И.И. Курбаков, А. Н. Кувшинов // Известия Самарской государственной сельскохозяйственной академии. - 2014. - №3. - С. 67 - 71.
5. Иншаков А. П. Диагностирование турбокомпрессора автотракторного дизельного двигателя на обкаточно-тормозном стенде КИ 5543 ГОСНИТИ / А. П. Иншаков, А. Н. Кувшинов, И.И. Курбаков, О.Ф. Корнаухов // Тракторы и сельхозмашины. - 2014. - №1. - С. 39 - 41.
6. Иншаков А. П. Экспериментальные исследования системы диагностирования турбонаддува автотракторного двигателя Д-245-35 / А. П. Иншаков, А. Н. Кувшинов, И.И. Курбаков, О.Ф. Корнаухов // Тракторы и сельхозмашины. - 2014. - №5. - С. 45 - 47.

УДК 621.43.06

О. Степанов, магістр гр. АТ19М
Центральноукраїнський національний технічний університет

АНАЛІЗ УМОВ РОБОТИ ТА НЕСПРАВНОСТЕЙ ТУРБОКОМПРЕСОРІВ АВТОМОБІЛЬНИХ ДВИГУНІВ

Проведений аналіз основних несправностей турбокомпресорів та причин їх виникнення. Встановлено діагностичні ознаки несправностей турбокомпресорів. Основними найбільш вагомими несправностями слід вважати пошкодження крильчаток ротора, зношування вала ротора, зношування упорного підшипника, зношування байпасного клапана, витікання масла з турбіни. Розглянуто процеси дефекації зносів деталей турбокомпресора.

турбокомпресор, двигун, турбонаддув, система впуску

Постановка проблеми. Концепція розвитку автомобільного транспорту передбачає збільшення потужності двигунів автомобілів при зниженні витрат палива і викидів в атмосферу продуктів згоряння. Для досягнення поставлених цілей автомобільні двигуни оснащуються турбокомпресорами (ТКР), охолоджувачами надувного повітря (інтеркулерами), акумуляторними системами подачі палива, електронними елементами управління і вбудованими системами самодіагностики.

Система газотурбінного наддуву (ГТН) автомобільних дизелів в класичному її конструктивному виконанні складається з двигуна, турбіни і компресора. Між турбіною і компресором має місце механічний зв'язок, а між турбіною і двигуном - газовий. При відносно простій конструктивній схемі і нескладному принципі дії турбокомпресора, визначення його технічного стану в процесі експлуатації є непростим завданням. Несправності в будь-якому з елементів поступово розвиваються в процесі експлуатації і

зовні помітно не виявляються, на певних режимах роботи можуть привести до відмови турбокомпресора, або двигуна в цілому.

Складність діагностування турбокомпресора визначається багатьма причинами. По-перше, показники ефективності функціонування ТКР в експлуатації залежать як від технічних і режимних характеристик двигуна, так і самого турбокомпресора. По-друге, до цих пір практично відсутні надійні інструментальні засоби контролю технічного стану турбокомпресора в експлуатації. Визначення найбільш інформативних функціональних параметрів турбокомпресора, встановлення їх граничних значень, розробка методів і засобів їх контролю є першорядним при технічному сервісі двигунів мобільної сільськогосподарської техніки.

Аналіз останніх досліджень та публікацій. Проблемою вдосконалення методів і засобів діагностування двигунів мобільної сільськогосподарської техніки займалися В. В. Альт, В. Й. Бєльських, С. Н. Боричів, Н. В. Бишів, І. І. Габбітов, І. П. Добролюбов, Н. С . Жданівський, Г. Д. Кокорєв, А. П. Іншаков [1-4], В. В. Лянденбурскій, В. М. Михлин, А. В. Ніколаєнко, А. В. неговори, С. Н. Ольшевський, К. Ю. Скібневскій, А. П. Савельєв, О. Ф. Савченко, І. П. Терських, І. А. Успенський та інші. Однак більшість методів діагностування технічного стану турбокомпресорів до сих пір не достатньо опрацьовані, не враховують повною мірою особливостей їх функціонування, відрізняються досить високою вартістю і складністю застосовуваного обладнання.

Мета і завдання досліджень. Метою роботи є розробка методів контролю технічного стану турбокомпресорів двигунів автомобілів.

Для досягнення поставленої мети вирішувалися наступні завдання досліджень:

Ідентифікувати несправності турбокомпресорів

Дослідити причини виникнення дефектів турбокомпресорів.

Провести комплексний аналіз взаємозв'язків оціночних показників правильного функціонування ТКР, існуючих методів і засобів їх діагностування..

Об'єкт дослідження – функціональні параметри турбокомпресорів автомобільних двигунів.

Предмет дослідження – закономірності зміни показників функціонування турбокомпресорів в експлуатаційних умовах.

Методи досліджень базуються на вивченні процесів зношування деталей автомобільних турбокомпресорів.

Потужність двигуна внутрішнього згоряння багато в чому визначається ступенем стиснення робочої суміші. У атмосферному ДВЗ (без турбонаддуву) поршень стискає суміш, початковий тиск якої дорівнює атмосферному. Якщо на початку такту стиснення в циліндр подати повітря і підвищити цей тиск, скажімо, на 2 бари, то ступінь стиснення збільшиться, а потужність звичайного серійного двигуна підвищиться до 30-50%.

Турбокомпресор (ТК) служить для подачі в камеру згоряння повітря під надлишковим тиском.

Повітря в турбіну забирається з повітряного фільтра через витратомір. У корпусі компресора воно розкручується і під впливом відцентрових сил, що забезпечують необхідний надлишковий тиск, потрапляє у впускний колектор двигуна.

Найбільш вразливий вузол турбокомпресора - це підшипник і ротор, тобто обидві крильчатки, з'єднані валом. Вони працюють в критичних режимах. Швидкість ковзання вала в підшипнику досягає 70 м/с. Окружна швидкість лопатей доходить до 600 м/с. На таких надзвукових режимах потрапляння найменшого стороннього предмета виводить турбокомпресор з ладу. Тому для його нормальної роботи потрібне високе очищення, по-перше, повітря, а по-друге - мастила, що подається під розрахунковим тиском у підшипники. Самий незначний перебій з подачею масла виводить ротор з ладу: при таких оборотах без мащення будь-який підшипник миттєво згорить. Найменші частки сажі або масла з двигуна, тим більше - окалина або шматочки поршневих кілець, можуть пошкодити крильчатку.

Тобто, для нормальної роботи турбокомпресора поршнева група двигуна повинна бути справна.

Крім того, дуже високі вимоги висуваються до матеріалу, з якого виготовляються крильчатки. Турбінна, наприклад, повинна витримувати температуру від 900° С і вище (в деяких турбінах робоча температура досягає 1100° С). Тому вона робиться з термостійкого кобальто-нікелевого сплаву.

Компресорна крильчатка кріпиться до валу гайкою через набір спеціальних шайб (одна з них працює в парі з опорним підшипником, а в другій є канавка під компресійне кільце, яке утримує масло з боку компресора). Вона виготовляється з високоякісного алюмінієвого сплаву, і повинна протистояти атмосферній корозії, витримувати дуже високі відцентрові навантаження, а також не деформуватися в процесі роботи, тобто її матеріал володіє дуже високою межею текучості.

Вал виготовляється зі сталі і зварюється з турбінною крильчаткою методом зварювання тертям. Відбувається це наступним чином: крильчатка обертається на верстаті, вал нерухомий. У зону контакту подається електричний струм (для такого зварювання нагрівання одним тільки тертям недостатньо), пара нагрівається, обертання різко припиняється, з'єднання зварюється і охолоджується. Потім заготовку обробляють на токарному верстаті, після чого вона проходить термічну обробку з наступним шліфуванням, накатуванням різьби, фінішним поліруванням і двоступеневим балансуванням. Дана технологія дуже точна, відповідальна, дорога і проводиться на спецобладнанні.

Несправності, що підлягають усуненню при ремонті турбокомпресора, виникають як в корпусі (підлягають відновленню посадочні місця під підшипники, компресійні кільця), так і у деталей ротора (знос опорного підшипника, втулок, компресійних кілець і канавок під них, опорного підшипника, ротора).

Пошкодження крильчаток ротора. Негерметичність систем впуску та випуску також викликає небезпечні перепади тиску. А банальна економія на заміні повітряного фільтра або несвоєчасне усунення підсосу повітря за його корпусом призводять до зносу компресорного колеса турбіни. Його лопатки сточуються потрапляють в середину частинками піску.

Поширена причина виходу ТКР з ладу - потрапляння сторонніх предметів в крильчатки. Часом це трапляється через недбалість механіка, який при обслуговуванні машини залишив ганчір'я або впустив всередину шайбу, або через непередбачене руйнування деталей двигуна, коли, наприклад, відвалюється електрод від свічки. Вал турбіни обертається з величезною швидкістю, і потрапляючи на крильчатки сторонні предмети значно їх деформують, через що турбіну може навіть заклинити. В результаті ротор ламається навпіл від скручування. В цьому випадку ремонтувати агрегат не має сенсу.

До характерних пошкоджень крильчаток і вала призводить так зване перекручування турбіни, тобто перевищення допустимих обертів. Перекручування може бути спровоковане і певним збігом обставин. Наприклад, через помилкові показання датчика витрати повітря з запізненням спрацьовує механізм регулювання тиску наддуву. ТК працює в дуже жорстких умовах (взяти хоча б термічне навантаження), і навіть незначне відхилення від допустимих режимів призводить до непоправних наслідків.

Зношування валу ротора. Описані вище причини відмов турбін зустрічаються не так часто, основна частка припадає на несправності в системі мастила ТК. У зазорах між валом турбіни і його підшипниками повинен бути присутній масляний клин, інакше відбувається перегрівання і знос валів, підшипників і ущільнень - внаслідок контактної роботи елементів. Найчастіше вихід з ладу турбіни настає через масляне голодування і наявність сторонніх часток в маслі.

ТКР дуже чутливий до чистоти і якості масла - більше, ніж двигун, в основному через те, що цей вузол працює в важких температурних режимах. Зокрема, на бензинових двигунах відпрацьовані гази розігріваються аж до 1000°С. Тому збільшені інтервали заміни масла і економія на фільтрі насамперед скорочують ресурс ТКР.

Масляне голодування турбіни має масу причин, про які мало хто замислюється. Одна з найпоширеніших - закоксовування підвідної трубки. Найчастіше вона забивається повністю - і ТКР працює на сухо. Не менш важлива справність масляного насоса двигуна, а також системи вентиляції картера. Часто саме через неї турбіна непомітно виходить з ладу. Масло в корпус підшипників ТКР надходить під тиском близько 4 бар, а зливається з нього в піддон двигуна самопливом. І, навіть незначне підвищення тиску картерних газів, сильно обмежить витрату мастила через турбіну, знижуючи несучу здатність його плівки, і призведе до його просочування через ущільнення. Нерідко це відбувається через несправний клапана вентиляції.

Зношування вала ротора, головним чином, відбувається через недостатню подачу масла в зону тертя. В результаті цього з’являються глибокі задири на валу в місцях посадки підшипників і навіть в зоні газодинамічного ущільнення.

При серйозних пошкодженнях корпусу відновлювати турбіну економічно недоцільно. Швидше за все, всередині все набагато гіршими.

Зношення упорного підшипника. Упорний підшипник вала турбіни страждає через критичний перепад тиску на сторонах впуску та випуску. Це призводить до збільшення осьового люфту ротора з усіма наслідками, що випливають.

Зношування байпасного клапана. У турбін бензинових двигунів на сідлах байпасного клапана часто з'являються тріщини.

Витікання масла з турбіни (маслогон). У турбіні замість сальників на кінцях вала використовують газодинамічні ущільнення. Їх завдання - ізолювати центральний корпус ТК від впускної і випускної систем двигуна, тобто від холодного та гарячого корпусу турбіни. Тиск відпрацьованих газів і впускного повітря в певних режимах роботи мотора дуже високий, і без ущільнень вони «наддувалися» в картер двигуна через зливну масляну трубку турбіни.

За принципом роботи і конструкцією газодинамічні ущільнення схожі з поршневими компресійними кільцями. Вони встановлені нерухомо в корпусі турбіни і ізолюють порожнини тільки при обертанні вала, але не стикаються з ним, маючи певний зазор. Ці кільця не герметичні повністю і пропускають частину газів.

На деяких режимах роботи будь-якої турбіни виникає поєднання високого тиску відпрацьованих газів і надмірне зріджування на впуску. Через такий перепад тиску можливе проривання частини газів з гарячого корпусу в холодний. Разом з собою на «вхідну» сторону вони переносять і масляний туман, який виходить з корпусу підшипників і йде на зливання. Це і викликає запотівання стиків патрубків турбіни. Обсяг «маслогона» не нормується - він залежить від конкретної моделі турбіни і режимів роботи двигуна.

Дефектація. Важливе значення при ремонті має процес дефектації деталей.

Спочатку турбокомпресор надходить на розбірний стіл, де розбирається і дефектів. Потім його деталі піддаються двоступеневому очищенню. Піскоструминній обробці піддаються деталі зі слідами іржі, пригорілого масла, окалини, корозії.

Далі дефектують деталі. До подальшої роботи буде придатний ротор, який не має слідів торкання крильчатки по корпусу турбіни. По-друге, якщо у нього канавка під компресійне кільце розбита більше певного допуску, такий ротор слід замінити. Якщо ротор зігнутий на більш ніж 0.02 мм, він теж вибраковується. Про його непридатність до подальшої роботи свідчать і сліди припалів через відсутність мастила, оскільки через перегрівання сталь могла відпуститися, тобто втратити твердість. Вибракування проводиться візуально і за допомогою мікрометричних вимірювань і перевірки допусків. У деяких випадках, наприклад, якщо вал має деформацію, його розглядають під мікроскопом на предмет виявлення тріщин.

Висновки. В результаті аналізу літературних джерел виділено найбільш значущі фактори, що впливають на зношування деталей турбокомпресорів автомобільних двигунів. В даній роботі встановлено причини виникнення дефектів деталей турбокомпресорів автомобільних двигунів та їх наслідки та вплив на роботу двигуна.

Список літератури

1. Иншаков А. П. Автоматизированный комплекс для диагностирования систем наддува воздуха в двигателях МЭС / А. П. Иншаков, А. Н. Кувшинов, И. И. Курбаков // Тракторы и сельхозмашины. - 2012. - № 10. - С. 16 - 18.
2. Иншаков А. П. Диагностика турбокомпрессоров на стенде КИ-5543/ А. П. Иншаков, А. Н. Кувшинов, И.И. Курбаков, О.Ф. Корнаухов // Сельский механизатор. - 2013. - №12. - С. 39.
3. Иншаков А. П. Программный комплекс «ДИЗЕЛЬ РК» / А. П. Иншаков, И.И. Курбаков // Сельский механизатор. - 2013. - №12. - С. 45.
4. Иншаков А. П. Способ диагностирования системы воздухопадачи тракторного дизеля / А. П. Иншаков, И.И. Курбаков, А. Н. Кувшинов // Известия Самарской государственной сельскохозяйственной академии. - 2014. - №3. - С. 67 - 71.
5. Иншаков А. П. Диагностирование турбокомпрессора автотракторного дизельного двигателя на обкаточно-тормозном стенде КИ 5543 ГОСНИТИ / А. П. Иншаков, А. Н. Кувшинов, И.И. Курбаков, О.Ф. Корнаухов // Тракторы и сельхозмашины. - 2014. - №1. - С. 39 - 41.
6. Иншаков А. П. Экспериментальные исследования системы диагностирования турбонаддува автотракторного двигателя Д-245-35 / А. П. Иншаков, А. Н. Кувшинов, И.И. Курбаков, О.Ф. Корнаухов // Тракторы и сельхозмашины. - 2014. - №5. - С. 45 - 47.

УДК 004:005.3

Н. Струтинська, магістр гр. ПА-19МЗ(ДС)
Центральноукраїнський національний технічний університет

ОСОБЛИВОСТІ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ДІЯЛЬНОСТІ ПІДПРИЄМСТВ В УМОВАХ ЦИФРОВІЗАЦІЇ ЕКОНОМІКИ

Стаття присвячена дослідженню особливостей інформаційного забезпечення діяльності підприємств в умовах цифровізації економіки. Розглянуто сутність інформації та інформаційного забезпечення діяльності підприємств. Визначено основні складові у сфері управління інформаційним забезпеченням. Охарактеризовано підходи та новітні елементи інформаційного менеджменту в контексті розвитку цифрової економіки. Наведено напрями удосконалення інформаційного забезпечення діяльності підприємств у сучасних умовах.
інформація, інформаційне забезпечення, інформаційні ресурси, цифровізація

Постановка проблеми. Актуальність теми дослідження обумовлена тим, що в умовах цифровізації економіки, стрімкого поширення сучасних інформаційно-комунікативних технологій зростає необхідність ефективного інформаційного забезпечення діяльності підприємств. Цифровізація усіх сфер життя суспільства містить у собі як низку безпрецедентних можливостей, пов’язаних із прискоренням процесів обміну і поширення актуальної інформації, автоматизацією управління інформацією та виконання інформаційно-аналітичних функцій, так і певних ризиків, що обумовлені необхідністю приділення значної уваги захисту інформації від несанкціонованого доступу, збереження комерційної таємниці суб’єктів господарювання, забезпечення безпеки програмних і технічних засобів обробки і зберігання інформації.

На сьогоднішній день існуючі системи інформаційного забезпечення на багатьох вітчизняних підприємствах є недостатньо ефективними. Причинами зазначеного факту виступають як дефіцит фінансових ресурсів для придбання і відповідного технічного супроводу сучасних інформаційних систем, так і недостатність кваліфікації персоналу, відсутність досвіду ефективного управління інформаційними потоками. Зростає інформаційне навантаження для всіх категорій персоналу підприємств, а на пошук потрібної інформації та її опрацювання часто витрачаються невиправдано великі обсяги часу.

Аналіз останніх досліджень і публікацій. Різноманітні теоретико-методичні та прикладні аспекти інформаційного забезпечення діяльності підприємств, впровадження сучасних інформаційних систем є предметом наукових пошуків багатьох вітчизняних науковців, таких як: Бондар Д.С., Волот О.І., Герасименко В.М., Гнилянська Л.Й., Колоток В.О., Костирко А.Г., Олійник Т.Г., Пащенко О.П. та ін.

Мета й завдання дослідження. Метою дослідження є ідентифікація особливостей інформаційного забезпечення діяльності підприємства в умовах цифровізації економіки.

Завдання дослідження: розглянути сутність інформації та інформаційного забезпечення; визначити основні підходи та засоби інформаційного менеджменту в умовах розвитку цифрової економіки; обґрунтувати напрями вдосконалення інформаційного забезпечення діяльності підприємств.

Об'єктом дослідження є процес управління інформаційним забезпечення діяльності підприємств.

Предметом дослідження є теоретико-методичні аспекти вдосконалення інформаційного забезпечення діяльності підприємств в умовах формування цифрової економіки.

Методи дослідження: аналізу і синтезу, індукції та дедукції, узагальнення, порівняння та класифікації.

Виклад основного матеріалу дослідження. У сучасних умовах ефективність діяльності суб'єктів господарювання значною мірою залежить від реалізації процесу управління своєчасною, достовірною та релевантною інформацією, яка стосується їхнього зовнішнього та внутрішнього середовища. Завдяки стрімкому поширенню і розповсюдженню науково-технічного прогресу, сучасних інформаційно-комунікативних технологій на сьогодні суспільство не відчуває гострого дефіциту в інформації. Проте у зв'язку з інформатизацією усіх сфер суспільного життя проблеми раціонального інформаційного забезпечення вітчизняних підприємств набувають все більшої актуальності [6].

У даний час на базі мережі Інтернет відбувається формування єдиного світового інформаційного простору, а перехід від індустріальної до інформаційної (цифрової) економіки сприяє нарощуванню процесів інформатизації та віртуалізації в усіх сферах життя суспільства. Для економічного устрою інформаційного суспільства характерним є використання таких ключових ресурсів, як праця, капітал, економічна свобода суб'єкта господарювання та інформаційний ресурс, включаючи теоретичні і практичні знання, навички і вміння людей [3].

Згідно з Законом України «Про інформацію» від 02.10.1992 р. №2657-XII (зі змінами та доповненнями), інформація – це «будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді» [5].

Інформаційне забезпечення управління підприємством – це сукупність даних, здійснення процедур їх пошуку, введення, оброблення, передачі, зберігання, накопичення та розповсюдження у рамках відповідних повноважень суб'єктами управлінського впливу у найбільш зручному для них форматі [6].

До складу інформаційного забезпечення діяльності підприємств фахівці відносять чотири основні складові, які наведено на рис. 1.

Рисунок 1 – Структура інформаційного забезпечення діяльності підприємства

Джерело: складено автором на основі [6].

Серед фундаментальних якісних характеристик інформаційного забезпечення діяльності підприємств можна виділити такі: повнота, достовірність, своєчасність, змістовність, об'єктивність, зрозумілість, співставність, суттєвість, прогнозна цінність [7]. В цілому інформація, що застосовується в управлінському процесі, повинна бути достовірною, своєчасною та достатньою.

У рамках концепції інформаційного менеджменту виділяють наступні основні підходи:

– економічний (досліджується доцільність залучення інформації на основі порівняння її граничної корисності й необхідності та фінансових витрат на її отримання);

– організаційний (присвячений питанням впливу інформаційних ресурсів і технологій на організаційну й управлінську структуру суб'єкта господарювання);

– аналітичний (передбачає аналіз поточних і майбутніх потреб користувачів в інформаційних ресурсах певної кількості і якості, потреб у застосуванні сучасних інформаційно-комунікативних технологій);

– системний (по суті, являє собою комплексне поєднання трьох перелічених вище підходів, особливу увагу акцентує на оптимізації інформаційних ресурсів та каналів обміну інформацією, методах роботи з інформацією, фінансовій ефективності інформаційного забезпечення) [4].

В умовах цифровізації економіки та активного використання мережі Інтернет в діяльності суб'єктів господарювання особливої актуальності набувають такі сучасні елементи інформаційного менеджменту, як:

– засоби оперативних комунікації (електронна пошта, месенджери, чати, чат-боти, соціальні мережі, списки розсилок та ін.);

– фонди розподілених ресурсів (інформаційні портали, термінали, бази даних, бази знань тощо);

– засоби швидкого координування діяльності (форуми, електронні опитування, наприклад, із застосуванням Google-форм, електронні дошки оголошень тощо);

– засоби зворотного зв'язку і забезпечення інформаційного співробітництва;

– сучасні засоби інформаційного забезпечення професійної діяльності (специфічні і стандартні інструменти пошуку продукції, ресурсів, партнерів, спеціальні програмні засоби для вирішення потреб інформаційного менеджменту суб'єктів певної галузевої приналежності) [1].

В контексті забезпечення інформаційної безпеки на підприємстві варто виділяти чотири основних напрями:

− розробка методичних засад оцінювання ризиків та загроз, рівня інформаційної безпеки підприємства, переваг та недоліків системи її забезпечення;

− реалізація конкретних організаційних заходів щодо захисту інформації;

− впровадження та застосування засобів технічного захисту інформації;

− контроль, аналіз та моніторинг системи інформаційної безпеки суб'єкта господарювання [2].

До ключових напрямів удосконалення менеджменту інформаційного забезпечення діяльності підприємств можуть бути віднесені такі: стратегічний підхід до управління інформацією; впровадження сучасних технологічних рішень, спрямованих на підвищення якості інформаційного забезпечення; здійснення контролю за дотриманням інформаційної безпеки; пошук джерел фінансування оновлення технічних і програмних засобів інформаційного забезпечення; поліпшення процесу інформаційного забезпечення прийняття управлінських рішень.

Висновки. Отже, до найбільш суттєвих особливостей менеджменту інформаційного забезпечення підприємств в умовах сьогодення виступають віртуалізація процесів взаємодії та широке застосування сучасних засобів і технологій обміну й опрацювання інформації. Стрімкий розвиток інформаційно-комунікативних технологій забезпечує як низку переваг, пов'язаних з прискоренням процесів інформаційного забезпечення, так і обумовлює необхідність пошуку дієвих шляхів захисту інформації та протидії інформаційним ризикам у сучасних умовах.

Список літератури

1. Бондар Д.С., Пащенко О.П. Інформаційний менеджмент як основа управлінської діяльності. Підприємницька модель економіки та управління розвитком підприємства: тези II Міжнародної науково-практичної конференції (6-8 листопада 2019 р.). Житомир, 2019. С. 55-58.
2. Волот О.І., Колоток В.О. Інформаційне забезпечення інформаційної безпеки підприємств малого бізнесу в умовах ринкових відносин. Формування ринкових відносин в Україні. 2019. №9. С. 50-57.
3. Герасименко В.М. Система інформаційного забезпечення менеджменту харчового підприємства. Вісник економіки транспорту і промисловості. 2019. №67. С. 173-178.
4. Гнилянська Л.Й. Особливості інформаційного менеджменту на підприємстві в умовах зовнішньоекономічної діяльності. Сучасні проблеми економіки і менеджменту: тези доповідей міжнародної науково-практичної конференції (Львів, 10-12 листопада 2011 року). Національний університет «Львівська політехніка», Інститут економіки і менеджменту, Інститут післядипломної освіти. Львів: Видавництво Львівської політехніки, 2011. С. 159-160.
5. Закон України «Про інформацію» від 02.10.1992 р. №2657-XII (зі змінами та доповненнями). Офіційний сайт Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 25.11.2020).
6. Костирко А.Г., Олійник Т.Г., Костирко П.Д. Організація раціональної системи інформаційного забезпечення управління підприємством. Modern economics. 2019. №18. С. 74-78.
7. Мельник І.М. Формування інформаційного забезпечення аналітичних процедур щодо оцінки ефективності діяльності лісогосподарських підприємств. Ефективна економіка. 2018. №12. URL: http://nbuv.gov.ua/UJRN/efek_2018_12_90. (дата звернення: 02.12.2020).

УДК 336.717

Я. Тімонічева, магістр гр. ФС-19М (1,4)
Центральноукраїнський національний технічний університет

ОБГРУНТУВАННЯ ПОНЯТТЯ ЛЕГАЛІЗАЦІЇ ДОХОДІВ КЛІЄНТІВ БАНКІВСЬКОЇ УСТАНОВИ

У статті увага зосереджена на формуванні науково обґрунтованого визначення поняття «легалізація доходів клієнтів банківської установи». Здійснено аналіз міжнародного законодавства, національного законодавства та результатів попередніх досліджень з питань запобігання та протидії легалізації злочинних доходів клієнтів банківської установи щодо визначення понять. За підсумками аналізу доведено, що ні в законодавчих актах, ні в науковій літературі немає точного визначення дефініції «легалізація доходів» у контексті банківської діяльності. Для формування поняття «легалізація доходів клієнтів банківської установи» визначено морфологічну основу та найбільш використовувані ключові слова. Представлено авторське визначення дефініції «легалізація доходів клієнтів банківської установи», що враховує загальноприйняті у міжнародній практиці морфологічну основу, ключові слова та відповідає визначенням, які надані в законах України

банк, легалізація доходів, отриманих злочинним шляхом, відмивання коштів

Постановка проблеми. Однією з головних проблем забезпечення економічної безпеки на світовому та державному рівні є проблема запобігання та протидії легалізації (відмиванню) доходів, що отримані злочинним шляхом. Утворенню нових інструментів відмивання доходів та ускладненню злочинних схем посприяв швидкий розвиток інформаційних технологій та сфери фінансових технологій зокрема. На шляху до європейської інтеграції Україною було взято на себе ряд зобов'язань стосовно протидії легалізації злочинних доходів. Так, в останні роки було удосконалено законодавство щодо запобігання і протидії легалізації (відмиванню) доходів, що отримані злочинним шляхом, прийнята Стратегія розвитку системи запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення на період до 2020 року [1], Верховною Радою було імплементовано рекомендації ФАТФ. Але процес удосконалення законодавства та методичного забезпечення запобігання та протидії відмиванню коштів, отриманих злочинним шляхом, ще не завершено. З огляду на це, актуальним є розроблення теоретичних основ з питань запобігання та протидії легалізації злочинних доходів.

Аналіз останніх досліджень і публікацій. Теоретичні основи запобігання і протидії легалізації коштів розглянуті у працях таких провідних вчених, як: Внукова Н., Д'яконова І., Колодізєв О. Кузьменко Лебідь О., Лєонов С., Пономаренко В., Самородов Б., Чмутова І. Аналіз їхніх праць засвідчив, що має місце ряд питань, яким приділено недостатньо уваги, а окремі питання вимагають подальших досліджень. До таких питань необхідно віднести питання єдності трактування поняття легалізації доходів клієнтів банківської установи.

Формулювання мети статті. Метою статті є теоретичне обґрунтування поняття легалізації доходів клієнтів банківської установи на основі сучасних методів дослідження задля сприяння уніфікації та комплексного розуміння контексті банківської діяльності.

Виклад основного матеріалу. Для послідуючого вдосконалення системи запобігання і протидії легалізації доходів, що отримані злочинним шляхом, на рівні держави необхідним є вирішення завдання щодо формування відповідної системи саме на рівні банківської установи. Виконанню даного завдання має передувати визначення змісту та сутності таких понять: «легалізація доходів клієнтів банку», «легалізація доходів», що буде сприяти

узагальненню та всебічному розумінню питань боротьби, пов'язаної з відмиванням коштів у рамках банківської діяльності.

В сучасній науковій літературі представлено багато трактувань сутності поняття «відмивання доходів». Наприклад, вітчизняні науковці О. Глущенко та І. Семеген трактують відмивання злочинних доходів як: «…процес маскування суб'єктами нелегальної економічної діяльності дійсного (незаконного) джерела походження їхніх доходів з подальшою їх легалізацією» [2, с. 26]. Трактування О. Глущенка та І. Семеген на основі того, що легалізація доходів та відмивання коштів являються поняттями синонімічними, має характер циклічності, тобто дефініція «відмивання доходів» у кінцевому результаті визначається їхньою легалізацією.

Науковець В. Захаров розглядає поняття «легалізація (відмивання) доходів, одержаних злочинним шляхом» як: «…дії, які прямо чи опосередковано спрямовані на надання правомірності відносинам користування, володіння, розпорядження коштами, отриманими протиправним шляхом» [3, с. 182]. Слід відмітити лаконічність такого визначення, відсутність суперечностей, але у контексті поставленої мети єдиним недоліком є відсутність у приведеному визначенні посилання на суб'єкта даних дій та, як наслідок, відсутність взаємозв'язку з банком.

У відповідності до визначення В. Ортинського «…відмивання (легалізація) злочинних доходів – це приховування їх існування, незаконного походження та використання без ідентифікації доходів, одержаних незаконно» [4, с. 535]. Але визначення В. Ортинського містить деякі суперечності: відмивання доходів не може являтися приховуванням їх існування, оскільки якраз його метою є переведення грошових коштів з нелегальної економіки, де ці грошові кошти й приховані, до легальної.

Наступне визначення представлено в Кембриджському словнику бізнес-англійської: «відмивання коштів – це дія переміщення незаконно зароблених коштів через банки або інший бізнес, щоб вони здавались зробленими на законних підставах» [5]. Як бачимо, в Кембриджському словнику як основні установи, через які здійснюється переміщення коштів задля їх наступної легалізації, виокремлюються саме банки, визнаючи таким чином з-поміж суб'єктів фінансового моніторингу їх виняткове місце.

Міжнародною Асоціацією Комплаєнсу (ІСА) надано наступне визначення дефініції «відмивання коштів»: «…це процес, за допомогою якого злочинці маскують оригінальну власність та контроль над доходами, отриманими злочинним шляхом, роблячи такі надходження, такими, які здаються похідними від законного джерела» [6]. В якості недоліку цього визначення слід виокремити те, що в ньому суб'єкт легалізації визнається злочинцем, однак існують такі види діяльності, які не є легальними, проте не являються злочинами, а надання будь-якому суб'єкту статусу злочинця здійснюється лише на підставі рішення суду.

Також з огляду на необхідність та важливість координації процесів запобігання і протидії легалізації (відмиванню) доходів, що отримані злочинним шляхом, на міжнародному рівні та рівні держави необхідним є визначення базового поняття в офіційних документах. Прийнято вважати, що вперше поняття «відмивання (легалізація) доходів» визначене в офіційних документах у 1984 році Президентською комісією Сполучених штатів Америки по боротьбі з організованою злочинністю та розглядалось як: «…процес, завдяки якому можна приховати існування, незаконне джерело або незаконне використання доходу, а потім замаскувати цей дохід, щоб він видавався легальним» [7].

Статтею 4 Закону України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення» до легалізації (відмивання) доходів, одержаних злочинним шляхом, належать «…будь-які дії, пов'язані із вчиненням фінансової операції чи правочину з активами, одержаними внаслідок вчинення злочину, а також вчиненням дій, спрямованих на приховання чи маскування незаконного походження таких активів чи володіння ними, прав на такі активи, джерел їх походження, місцезнаходження,

переміщення, зміну їх форми (перетворення), а так само набуттям, володінням або використанням активів, одержаних внаслідок вчинення злочину» [8].

Статтею 209 Кримінального кодексу України криміналізація злочину щодо легалізації (відмиванню) доходів, які одержані злочинним шляхом, визначається як: «…вчинення фінансової операції чи укладення угоди з коштами або іншим майном, одержаними внаслідок вчинення суспільно небезпечного протиправного діяння, що передувало легалізації (відмиванню) доходів, а також вчинення дій, спрямованих на приховання чи маскування незаконного походження таких коштів або іншого майна чи володіння ними, прав на такі кошти або майно, джерела їх походження, місцезнаходження, переміщення, а так само набуття, володіння або використання коштів чи іншого майна, одержаних внаслідок вчинення суспільно небезпечного протиправного діяння, що передувало легалізації (відмиванню) доходів» [9].

В результаті здійсненого аналізу, можемо виокремити наступні головні морфологічні складові дефініції «легалізація доходів»:

наступає за деякий час після здійснення предикатного злочину;

в якості головної мети виступає приховування джерел походження доходів задля наступного їх застосування при здійсненні легальної економічної діяльності;

трактується як процес чи сукупність дій, методів, способів, заключення угод, проведення фінансових операцій.

Тобто, на підставі проведеного аналізу бачимо, що необхідно сформулювати деталізоване визначення дефініції «легалізація доходів» у контексті банківської діяльності. Задля визначення головних слів цієї дефініції на підставі вищенаведених трактувань науковців здійснено контент-аналіз. Його результати приведені на рис. 1.

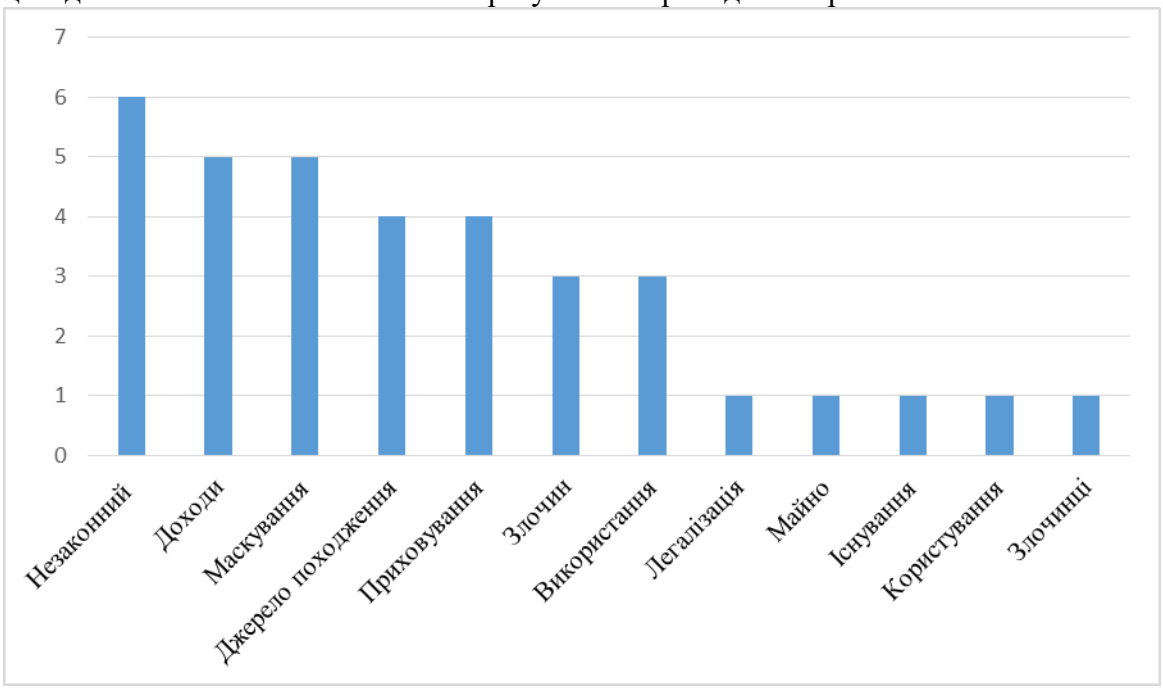


Рисунок 1 – Результати контент-аналізу дефініції «легалізація (відмивання) доходів, що отримані злочинним шляхом»

Джерело: побудовано автором

Результати контент-аналізу свідчать, що найчастіше при трактуванні дефініції «відмивання доходів» використовуються наступні слова: незаконний, доходи, маскування, джерело походження, приховування та злочин. Необхідно відмітити, що велика кількість визначень включають перерахування певних дій, які проводяться з коштами, що отримані злочинним шляхом, для того, щоб визнати даний процес їх легалізацією, зокрема, походження, існування, володіння, використання, розпорядження, контроль тощо. Однак,

також необхідно відзначити, що всякі дії щодо використання злочинних коштів, і насамперед з використанням фінансової системи при цьому, треба розглядати як приховування їх злочинного походження, а значить відповідно як легалізацію. До того ж, виходячи зі специфіки банківської діяльності не являється визначальним, які конкретно дії намагається робити злочинець з нелегальними коштами, оскільки вже саме їх потрапляння в банківську систему являється спробою надати таким коштам статусу законних.

Як бачимо, ні в міжнародному, ні в національному законодавстві, ні в науковій літературі немає чіткого формулювання поняття «легалізація (відмивання) доходів, отриманих злочинним шляхом». У нормативних документах цю дефініцію трактують через певний перелік злочинів, які здійснюються до цього, що не збігається зі змістом самої банківської діяльності та не виступає ціллю функціонування системи запобігання і протидії відмиванню доходів, а відповідно з позиції внутрішнього фінансового моніторингу банківської установи перелік злочинів не являється змістовною рисою процесу легалізації.

В результаті здійсненого аналізу головних слів та виокремлення морфологічних складових, виходячи з необхідності формулювання поняття із урахуванням специфіки діяльності банківських установ, дефініцію «легалізація доходів клієнтів банку» можливо визначити як процес здійснення юридичною або фізичною особою будь-яких дій із грошима та іншими фінансовими активами, які одержані внаслідок нелегальної і пов'язаної із нею діяльності, задля приховування їх походження та трансформування в законні активи шляхом використання чи спроб використання банківських послуг.

Висновки. У сформульованому визначенні наголошено на тому, що особа, яка здійснює спроби легалізувати злочинні кошти, являється клієнтом банку у відповідності до визначення у Законі України «Про банки та банківську діяльність» та підкреслено, що будь-які дії із незаконними коштами являються процесом їх легалізації, а також враховуються прийняті в переважній більшості офіційних документів головні слова та морфологічна основа. У визначенні немає складових методів та способів здійснення фінансових операцій, оскільки мова йде лише про банківські послуги та операції, які постійно супроводжуються заключенням відповідних угод.

Список літератури

1. Стратегія розвитку системи запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення на період до 2020 року, затверджена Розпорядженням Кабінету міністрів України від 30 грудня 2015 року № 1407-р. URL: http://zakon5.rada.gov.ua/laws/show/1407-2015-%D1%80/ (дата звернення: 08.09.2020).
2. Глущенко О. О., Семеген І. Б. Антилегалізаційний фінансовий моніторинг: ризик-орієнтований підхід: монографія / За заг. ред. д-ра екон. наук, проф. Р. А. Слав'юка. К.: УБС НБУ, 2014. 386 с.
3. Захаров В. П. Легалізація (відмивання) доходів, одержаних злочинним шляхом: теоретико-правовий аспект. Вісник Національного університету «Львівська політехніка». Юридичні науки. 2014. № 801. С. 180–186.
4. Ортинський В. Л. Характеристика легалізації (відмивання) доходів, одержаних злочинним шляхом: криміналістичні аспекти. Вісник Національного університету «Львівська політехніка». Серія: Юридичні науки: збірник наукових праць. 2016. № 850. С. 533–540.
5. Cambridge Business English Dictionary. Cambridge University Press. URL: https://dictionary.cambridge.org/dictionary/ english/money-laundering (Last accessed: 09.09.2020).
6. ICC Banking Commission Global Survey highlights impact of trade finance gap on SMEs (2018) // The International Chamber of Commerce (ICC). URL: https://iccwbo.org/media-wall/news- speeches/icc-banking-commission-global-survey-highlights-impact-of-trade- finance-gap-on-smes/ (Last accessed: 12.11.2020)
7. United States President's Commission on Organized Crime: The Cash connection: organized crime, financial institutions, and money laundering. President's Commission on Organized Crime: Washington, D.C., 1984. URL: https://catalog.hathitrust.org/Record/001541027 (Last accessed: 09.09.2020).
8. Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення: Закон України від 06.12.2019 року № 361-IX. URL: https://zakon.rada.gov.ua/laws/show/361-20#Text (дата звернення: 08.09.2020).
9. Кримінальний кодекс України: Закон України від 05.04.2001 р. № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14 (дата звернення: 09.09.2020).

УДК 543.3

К. Троцюк, магістр гр. ЕО-19М
Л. Коломієць, доцент
Центральноукраїнський національний технічний університет

ЕКОЛОГІЧНА ОЦІНКА СПОЖИВЧИХ ЯКОСТЕЙ ВОДНИХ РЕСУРСІВ ДЕЦЕНТРАЛІЗОВАНИХ ДЖЕРЕЛ КІРОВОГРАДЩИНИ

Робота носить дослідницький характер та вимагає досліджень споживчої якості води в децентралізованих джерелах міста Кропивницький.

Об'єктом і предметом дослідження є визначення проблем забруднення децентралізованих джерел та екологічна і споживча якість води децентралізованих джерел.

Метою роботи є проведення моніторингових досліджень екологічних показників споживчої якості колодязної води, з'ясування причин забруднення колодязів, використання методів для очищення, вплив на людину та навколишнє середовище.

Встановлено та проаналізовано високий рівень забрудненої колодязної води стічними скидами котелень, господарсько-побутовими стоками та тепловим забрудненням. Проведені моніторингові дослідження і аналізи проб відібраної води.

моніторинг, децентралізоване джерело, забруднення води, дезінфекція, кислотність, нітрати, аналізи показників

Постановка проблеми. Ефективне очищення води від різноманітних видів забруднень залишається одним з головних завдань людства. На жаль, ця проблема досі актуальна. Існуючі способи її вирішення або занадто дорого коштують, або займають тривалий час. Зараз звільнення води від домішок здійснюється комбінованим чином, починаючи з механічного етапу очищення, коли відбувається позбавлення води від макроскопічних домішок, і закінчуючи фізико-хімічними методами, призначеними для ліквідації токсичних речовин і елементів. Існуючі механізми біологічного очищення води володіють рядом недоліків. По-перше, їх тривалість становить кілька годин, а то й більше. По-друге, деякі з них засновані на технології пропускання води через спеціальні дорогі мембранні фільтри, які досить швидко забиваються і приходять в непридатність.

Результати досліджень.

Проблемі забезпечення населення якісною питною водою зараз приділяється підвищена увага не тільки тому, що вода є незамінною речовиною для життя людини, а й тому, що забруднення водопостачання та питної води визначає ступінь екологічної безпеки цілих регіонів, а питна вода низької якості безпосередньо впливає на здоров'я населення. Крім того, замість традиційних аспектів неблагополуччя з точки зору загальної жорсткості, вмісту заліза, фтору, на перший план вийшли показники вмісту у воді важких металів, нітритів, вірусів, збудників паразитарних хвороб, на перший план висувається загальна мутагенна активність води, яка призводять до більш значних загроз здоров'ю населення [1].

Виходячи з санітарного стану та якості питної води децентралізованих систем, можна констатувати, що цей тип водопостачання в країні є найбільш проблематичним. У сільській місцевості проблема водопостачання населення посилюється через хімічне та бактеріальне забруднення джерел води. Сільське населення України переважно споживає воду з колодязів та окремих свердловин, які (в переважній більшості) перебувають у незадовільному технічному та санітарному стані. Саме тому об'єктом дослідження було обрано аналіз якості питної води цього виду водопостачання на Кіровоградщині, оскільки він найкраще характеризує стан водоносних горизонтів та розташування джерел водопостачання в господарській діяльності регіону [2].

Важливим є те, що деякі хімічні речовини (зокрема нітрати) навіть при високих концентраціях ніяким чином не змінюють органолептичні властивості води (смак, запах, мутність, прозорість). Єдиним дієвим способом дізнатись про якість та безпечність води є проведення лабораторних досліджень [3].

В ході дослідження було взято десять проб води децентралізованих джерел за адресами :

1. Провулок Середній, 46.
2. Вулиця Херсонська, 59.
3. Вулиця Б.Хмельницького, 288.
4. Вулиця Будівельників, 17.
5. Провулок Степовий, 37.
6. Вулиця Колодязна, 61.
7. Вулиця Гетьмана Сагайдачного, 91.
8. Вулиця Нікопольська, 11.
9. Вулиця Радіщева, 20а.
10. Вулиця Лелеківська,19.

Дані моніторингових та лабораторних досліджень наведені в таблицях 1 та 2.

Таблиця 1 – Органолептичні показники

№ з/п	Об'єм проби	Характеристика запаху	Інтенсивність запаху	Прозорість	Смак
1	500мл	Запаху немає	0	Прозора	Дуже слабкий
2	500мл	Запаху немає	0	Прозора	Ніякого смаку
3	500мл	Запаху немає	0	Прозора	Ніякого смаку
4	500мл	Запаху немає	0	Прозора	Ніякого смаку
5	500мл	Дуже слабкий	1	Прозора	Дуже слабкий
6	500мл	Запаху немає	0	Прозора	Ніякого смаку
7	500мл	Дуже слабкий	1	Прозора	Дуже слабкий
8	500мл	Запаху немає	0	Прозора	Ніякого смаку
9	500мл	Дуже слабкий	1	Прозора	Дуже слабкий
10	500мл	Запаху немає	0	Прозора	Ніякого смаку

Нормативи фізико-хімічних показників.

Кислотність. pH питної води коливаються в межах від 6,5 до 8,0 вода повинна мати активну реакцію близько до нейтральної.

Жорсткість води. Нормальна жорсткість води - близько 3 - 4 ммоль / дм^3. Згідно державним санітарним нормам, максимально допустима жорсткість води - не більше 7 ммоль / дм^3.

Сухий залишок. Кількість сучого залишку у воді залежить від кількості розчинених у ній солей. Сухий залишок як показник ступеня мінералізації води допускається в кількості 1000 мг/л. Лише для окремих раціонів ця величина збільшена до 1500 мг/л.

Хлориди. Визначення хлоридів грунтується на реакції між хлором хлористих сполук з азотнокислим сріблом. При цьому утворюється хлористе срібло – майже нерозчинна сполука

у вигляді білої каламуті або осаду. Відповідно до ГОСТу 2874 – 73 у питній воді допускається наявність хлоридів органічного походження до 20-30 мг/л; хлоридів мінерального походження – до 350 мг/л**.**

Сульфати. Відповідно до ГОСТу 2873 у воді допускається наявність сульфатів органічного походження – до 80 мг/л; мінерального – до 500 мг/л.

Примітка: номер проби у таблиці відповідає порядку адрес наведеному на початку статті.

Таблиця 2 – Фізико-хімічні показники

№ з/п	Кислотність	Загальна жорсткість, ммоль / дм^3	Сухий залишок, мг/л	Хлориди, мг/л	Сульфати мг/л	Невідповідність вимогам нормативних документів
1	7,0	3,5	770	18	65	Показники відповідають нормам
2	7,1	4,0	935	20	69	Показники відповідають нормам
3	6,8	3,7	920	21	72	Показники відповідають нормам
4	7,0	4,3	990	28	45	Показники відповідають нормам
5	7,2	6,3	1250	24	95	Загальна жорсткість, сухий залишок, сульфати
6	7,0	6,1	1120	19	110	Загальна жорсткість, сухий залишок, сульфати
7	6,8	4,4	810	28	80	Показники відповідають нормам
8	7,1	6,4	730	24	55	Загальна жорсткість
9	7,2	4,0	920	19	62	Показники відповідають нормам
10	6,3	4,6	880	25	76	Кислотність

Бактеріологічний аналіз та санітарно-токсикологічні показники

Моніторинг інфекційної захворюваності свідчить, що кожний другий-третій спалах кишкових інфекцій пов’язаний із вживанням неякісної питної води. Чисельними спостереженнями і дослідженнями встановлено значення питної води в розповсюдженні кишкових інфекцій (холера, черевний тиф, дизентерія), вірусних та інших.

Ступінь забруднення води патогенними (хвороботворними) мікробами визначають за наявністю в ній кишкової палички, що живу в кишківнику людини і тварин. У ряді країн такими організмами, окрім кишкової палички, є ентерококи, які відрізняються найбільшою стійкістю і виживаністю в зовнішньому середовищі. Велика концентрація санітарно-показових мікроорганізмів свідчить про забрудненість води і можливості вмісту в ній патогенних мікроорганізмів та вірусів [4].

Дані аналізу за бактеріологічними та санітарно-токсикологічним показникам наведені у таблицях 3 та 4.

Таблиця 3 – Бактеріологічні показники відібраних проб

№ з/п	Контрольна точка відбору проби води	Бактеріологічні показники	Не відповідає вимогам нормативних документів, за показниками
1	Провулок Середній, 46	Загальні коліформи, E.Coli(кишечка паличка)	Показники відповідають нормам
2	Вулиця Херсонська, 59	Загальні коліформи, E.Coli(кишечка паличка)	Показники відповідають нормам
3	Вулиця Б.Хмельницького, 288	Загальні коліформи, E.Coli(кишечка паличка)	Показники відповідають нормам
4	Вулиця Будівельників, 17	Загальні коліформи, E.Coli(кишечка паличка)	Загальні коліформи, E.Coli
5	Провулок Степовий, 37	Загальні коліформи, E.Coli(кишечка паличка)	Загальні коліформи
6	Вулиця Колодязна, 61	Загальні коліформи, E.Coli(кишечка паличка)	Показники відповідають нормам
7	Вулиця Гетьмана Сагайдачного, 91	Загальні коліформи, E.Coli(кишечка паличка)	Загальні коліформи, E.Coli
8	Вулиця Нікопольська, 11	Загальні коліформи, E.Coli(кишечка паличка)	Показники відповідають нормам
9	Вулиця Радіщева, 20а	Загальні коліформи, E.Coli(кишечка паличка)	Загальні коліформи
10	Вулиця Лелеківська,19	Загальні коліформи, E.Coli(кишечка паличка)	Загальні коліформи

Гранично допустима концентрація або норма нітратів у питній воді – 50 мг/дм³. Але є ще й нітрити – це сполуки, які отримуються в основному в процесі життєдіяльності мікроорганізмів, їх ГДК - 0,5 мг/дм³.

Таблиця 4 – Санітарно-токсикологічні показники

№ з/п	Контрольна точка відбору проби води	Нітрати, мг/дм³	Нітрити, мг/дм³.	Не відповідає вимогам нормативних документів, за показниками
1	Провулок Середній, 46	70	0,4	Нітрати
2	Вулиця Херсонська, 59	46	0,2	Показники відповідають нормам
3	Вулиця Б.Хмельницького, 288	38	0,3	Показники відповідають нормам
4	Вулиця Будівельників, 17	65	0,5	Нітрати
5	Провулок Степовий, 37	73	0,3	Нітрати
6	Вулиця Колодязна, 61	69	0,4	Нітрати
7	Вулиця Гетьмана Сагайдачного, 91	50	0,2	Показники відповідають нормам
8	Вулиця Нікопольська, 11	48	0,3	Нітрати
9	Вулиця Радіщева, 20а	44	0,2	Показники відповідають нормам
10	Вулиця Лелеківська,19	58	0,2	Нітрати

Висновок. Проблеми якості води децентралізованих джерел завжди були і будуть актуальні, так як це безпосередньо впливає на здоров'я кожного споживача води таким шляхом.

Було виконано ряд дослідів якості за такими показниками, як: органолептичні, фізико-хімічні, бактеріологічні та санітарно-токсикологічні. Високий рівень забруднення джерел питного водопостачання, недостатня ефективність технології водопідготовки та водопостачання, низький рівень забезпеченості води на душу населення призвели до низької якості питної води, що є серйозною загрозою для здоров'я людей.

Проаналізувавши отримані в ході дослідження дані, можна зробити декілька висновків:

- ситуація з якісним станом води у джерелах децентралізованого водопостачання Кіровоградщини за хімічними та бактеріологічними показниками впродовж останніх років залишається незадовільною й має нестійкий характер.
- У м. Кропивницький за комплексним дослідженням по всім показникам майже кожна друга взята проба води не відповідає нормативним документам.
- Деякі проби, які не відповідають мікробіологічним показникам є наявним прикладом бактерій групи кишкової палички у децентралізованих джерелах. Тому в цих містах треба проводити постійні аналізи на її виявлення, для запобігання підхоплення людиною коліформ.
- На подолання вказаних проблем у галузі оцінки якості питної води в джерелах децентралізованого водопостачання рекомендується розвивати систему моніторингу джерел водопостачання міста, а також створити інформаційні центри з обробки та узагальнення інформації з підготовкою прогнозних розрахунків із метою підвищення ефективності управління водним господарством. Необхідно постійно контролювати комплекс всіх показників води у децентралізованих джерелах.

Список літератури

1. Бережнов С. П. Питна вода як фактор національної безпеки. // СЕС профілактична медицина. – 2006, №4. – С. 8–13.
2. Прокопов В. О., Кузьмінець О. М., Соболь В. А. Стан децентралізованого господарсько-питного водопостачання України // Гігієна населених місць. – 2008, №51. – С. 63–67.
3. Александров В. Д., Ємельянов В. І. Отруйні речовини. Москва: Воениздат, 1990. – 310 с.
4. Орадовская А.Е. Санитарная охрана водозаборов подземных вод/ А.Е. Орадовкая, Н.Н. Лапшин. - М.:Недра, 1987. - 167 с.

УДК 025.5:023.5

В. Ухалін, магістр гр. ІС-19М-1,4
Центральноукраїнський національний технічний університет

НОВІ НАПРЯМИ ДІЯЛЬНОСТІ БІБЛІОТЕК В ІНФОРМАЦІЙНОМУ СУСПІЛЬСТВІ (НА ПРИКЛАДІ КІРОВОГРАДСЬКОЇ ОБЛАСНОЇ БІБЛІОТЕКИ ДЛЯ ЮНАЦТВА ІМ. Є. МАЛАНЮКА)

У статті висвітлюється зміни діяльності бібліотеки шляхом нарощування інформаційного потенціалу, інтеграції бібліотечних ресурсів та забезпечення швидкого доступу до інформації. Сьогодні бібліотека розширює діапазон своїх можливостей, трансформуючись в сучасну, комфортну, прогресивну інформаційну структуру, справжній науково-інформаційний центр.

інформаційний простір, інформаційне суспільство, інформація, знання, сучасна бібліотека, інформаційні процеси, інформаційні технології, інформаційні центри

Відбувається еволюція соціальної ролі бібліотек до традиційних завдань просвітницького характеру, збереження і примноження культурного надбання, додалися функції інформаційних центрів, що забезпечують доступ до національних і світових інформаційних мереж та баз даних.

Активне впровадження сучасних технологій сприяло створенню нової інформаційної інфраструктури, в якій бібліотеці відведено роль посередника між інформаційними ресурсами та користувачем[1. с. 5].

Трансформація традиційної бібліотечної діяльності, приведення її у відповідність із новими суспільними запитами інформаційного обслуговування – ці завдання постали перед бібліотечним співтовариством зі стрімким поширенням електронних інформаційних технологій. Інтернет дедалі більшою мірою конкурував з бібліотечними інформаційними центрами[3].

Об’єктивні процеси розвитку інформаційного суспільства обумовлюють необхідність збереження модернізованої системи бібліотечних установ – інформаційних центрів нинішнього суспільства.

По – перше, бібліотечні установи продовжують відігравати істотне значення в технологіях продукування нової суспільно значущої інформації.

По – друге, система бібліотек може бути ефективним інструментом реалізації завдань інформатизації, надання доступу всім категоріям громадян до інформаційних ресурсів.

По – третє, удосконалення соціальної структури нового суспільства потребує від бібліотек поширення в суспільстві здобутків сучасного суспільствознавства як способу впорядкування нового рівня знання, уявлень про закономірності соціального розвитку в умовах прискорення темпів суспільного розвитку.

По – четверте, бібліотечні установи можуть значною мірою зменшити проблеми, що постають нині перед органами державної влади, науковими установами, громадськими організаціями, бізнесом в пошуку якісної електронної інформації.

По – п’яте, в умовах розвитку комп’ютерних технологій бібліотеки, як сучасні інформаційні центри, мають змогу розширити контингент своїх користувачів, використовуючи дистантні форми інформаційного обслуговування.

Головна функція інформаційно – бібліографічної роботи Кіровоградської обласної бібліотеки для юнацтва ім. Є. Маланюка – інформаційне забезпечення потреб користувачів[2, с. 30].

Основні напрями інформаційної роботи бібліотеки:

– формування інформаційного ресурсу в традиційному та електронному режимах;

– створення систем вторинних документів (бібліографічних, реферативних, оглядово – аналітичних);

– довідково – інформаційне обслуговування, проведення інформаційних заходів.

Особливість інформаційної функції Кіровоградської обласної бібліотеки для юнацтва ім. Є. Маланюка полягає в тому, що вона реалізується, тісно взаємодіючі з іншими суб'єктами інформаційного процесу та використовуючи різні канали поширення інформації. Бібліотека бере активну участь в оцінці, інтерпретації та фільтрації інформації, у встановленні певних зв'язків між інформаційними масивами, щоб забезпечити користувачам доступ до широкого спектру джерел знання, соціально значущої інформації. Інформаційна робота бібліотеки була орієнтована на застосування електронних засобів комунікації, широко використовувалися можливості інтернету та інтернет – маркетингу[4, с. 14].

Одним з головних інформаційних продуктів бібліотеки є "Електронний каталог", що відображає весь активний фонд бібліотеки та створює основу для виконання різноманітних запитів користувачів. Електронний каталог забезпечує одночасний багатоаспектний оперативний пошук.

Отже, можемо зробити висновки, що інформаційна діяльність Кіровоградської обласної бібліотеки для юнацтва ім. Є. Маланюка досить різнопланова і бібліотека забезпечує інформаційні потреби користувачів, займається виховною роботою серед молоді, організовую культурно – просвітницькі заходи, надає інформацію віддалено за рахунок електронного інформування у режимі віртуальних довідок.

Реалізація інформаційної діяльності бібліотеки передує:

– створення бібліотечно – бібліографічної інформації та публікаційних текстів в електронному вигляді;

– забезпечення доступу через Інтернет до бібліографічної інформації і повнотекстових баз даних;

– забезпечення електронних засобів пошуку і обслуговування запитів на інформаційні ресурси бібліотеки.

Все це в комплексі дає змогу в повній мірі задовольнити потреби користувачів бібліотеки, підвищувати рейтинг закладу та здійснювати культурно – просвітницьку діяльність[7, с. 53].

Важливим кроком у розвитку бібліотек і забезпечення ними інформаційних потреб користувачів є обов'язкове створення інформаційно-бібліотечних мереж. Будучи однією з ланок у мережі бібліотечних та інформаційних установ, вона зможе працювати так, щоб забезпечувати доступ до інформації кожній людині, де б та не перебувала. Така мережа має бути спрямована не лише на розвиток інформаційного потенціалу країни, а й на те, щоб забезпечити рівність усіх громадян у можливості доступу до потрібних їм джерел, задовольнити їхні особисті й суспільні інтереси в інформації та підняти престиж освіченості, культури й авторитет бібліотечних установ[6, с. 26].

Сьогодні у зміцненні ресурсно-інформаційної бази віртуального освітнього середовища провідне місце належить бібліотечному інформаційному порталу та віртуальній бібліотеці. Вони є сучасною структурно-функціональною інтерактивною формою інформаційно- комунікаційної архітектури бібліотеки, фактично визначають пріоритети у формуванні електронного культурного середовища, ландшафтну документно - когнітивну, інформаційну єдність[5, с. 223].

Своєчасне інформування, оперативне та ефективне задоволення потреб читачів сьогодні забезпечують веб-сайти, які дозволяють розширити та урізноманітнити спектр бібліотечно - інформаційного сервісу.

Інтернет-сайт бібліотеки відіграє значну роль не лише в забезпеченні інформаційної, культурної та освітньої підтримки користувачів бібліотеки, але й у наданні методичної допомоги колегам, обміні досвідом та формуванні бібліотечної спільноти.

Бібліотека – це доволі складна структура, де знаходиться велика кількість різноманітних видань (документів): книги, журнали, газети, карти та ін., а останнім часом ще й електронні ресурси. Впровадження автоматизованих бібліотечно-інформаційних технологій стає якісно новим етапом в розвитку бібліотек, посилює вимоги до професійного рівня кадрів[9, с. 69].

За умов активного розвитку інформаційно-комунікаційних технологій в електронному середовищі вагомою складовою документно-інформаційного ресурсу сучасної бібліотеки є електронні ресурси. Це інформаційні ресурси, що створюються, керуються та використовуються за допомогою комп'ютера і містять дані та програми, зафіксовані в електронній (цифровій) формі на певних носіях.

Для задоволення потреб сучасного користувача, забезпечення оперативного доступу до всіх бібліотечно-інформаційних ресурсів як власного виробництва, так і придбаних, бібліотека освоює і активно впроваджує сучасні досягнення в галузі інформаційних, комунікаційних і мультимедійних технологій в бібліотечні процеси. Інноваційний клімат є умовою розвитку бібліотеки[8, с. 43].

Впровадження комп'ютерних та телекомунікаційних технологій в роботу бібліотек є вже не модою, а нагальною вимогою до підвищення продуктивності та якості бібліотечно-інформаційного обслуговування на основі створення, використання та інтеграції електронних ресурсів, а також автоматизації бібліотечних процесів.

Створені електронні каталоги та масиви цифрових документів разом із засобами телекомунікацій необхідні для виконання головного завдання – забезпечення доступу користувачів до різних типів інформаційних ресурсів бібліотек.

Висновки. Сучасна бібліотека є складним соціально-комунікаційним комплексом, який в умовах інформаційного суспільства розглядається як інформаційно-бібліотечний центр, де генерується інформаційно-освітнє та соціокультурне середовище для молодої людини.

Визначено, що інформаційна діяльність бібліотеки, спрямована на збирання, упорядкування, аналітико-синтетичну переробку, збереження, пошук та поширення інформації як на традиційних так і електронних носіях.

Основними напрямками інформаційної роботи є:

– формування інформаційного ресурсу в традиційному та електронному режимах;

– створення системи вторинних документів (бібліографічних, реферативних, оглядово-аналітичних);

довідково-інформаційне обслуговування (обслуговування спеціалістів у режимах вибіркового розповсюдження інформації, диференційоване обслуговування користувачів, організація книжкових виставок, віртуальних виставок та виставок нових надходжень, інформаційних переглядів);

проведення інформаційних заходів.

А також створення бібліотечно-бібліографічної інформації та публікаційних текстів в електронному вигляді та забезпечення доступу через Інтернет до бібліографічної інформації і повнотекстових баз даних.

Список літератури

1. 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.
2. Бібліотека. Наука. Комунікація: формування національного інформаційного простору. Матеріали Міжнар. наук. конф., Київ, 4–6 жовт. 2016 р. НАН України, Нац. б-ка України ім. В. І. Вернадського, Асоц. б-к

України, Рада дир. б-к та інформ. центрів – членів МААН. К., 2016. 640 с.
3. Воробйова О. Інформаційне суспільство та його вплив на становлення електронного бізнесу. Науковий вісник. 2010. №5. URL: http://www.lvivacademy.com/vidavnitstvo_1/visnik5/fail/+Vorobjova.pdf (дата звернення: 13.12.2020).
4. Горный Е. Развитие электронных библиотек: мировой и российский опыт, проблемы, перспективы. Интернет и российское общество. М.: Гендальф, 2002. 279 с.
5. Горова С. Інформатизація суспільства й нові завдання бібліотечних структур. Наукові праці Національної бібліотеки України ім. В. І. Вернадського. 2010. Вип. 27. С. 225−230.
6. Колесникова Т. О. Інформатизація бібліотек ВНЗ: шляхи еволюції та сучасний стан. Вісник Книжкової палати. 2010. № 2. С. 25–28.
7. Сучасні проблеми діяльності бібліотеки в умовах інформаційного суспільства [Текст]: матеріали IV міжнар. наук.-практ. конф., Львів, 25 жовт. 2012 р. Нац. ун-т «Львів. Політехніка», Наук.-техн. б-ка; [редкол.: Шишка О. В. та ін.]. Л.: Вид-во Львів. політехніки, 2012. 595 с.
8. Шрайберг Я. Л. Бібліотеки, електронна інформація і змінне суспільство в інформаційному столітті. Науч. і техн. б-ки. 2007. № 1. С. 25–56.
9. Шрайберг Я. Роль бібліотек у забезпеченні доступу до інформації та знань в інформаційному столітті. Вища школа. 2007. № 4. С. 60–74.

УДК 621.431.3

О. Чайка, магістр гр. АТ19М
Центральноукраїнський національний технічний університет

АНАЛІЗ ПРИЧИН ЗНОШУВАННЯ ТА РУЙНУВАННЯ КОЛІНЧАСТИХ ВАЛІВ АВТОМОБІЛЬНИХ ДВИГУНІВ

Встановлено основні дефекти колінчастих валів: лінійний знос, риски, задирання, тріщини, деформації. Визначено, що колінчасті вали, які не можуть більше піддаватися механічній обробці під ремонтні розміри і, відповідно, використовуватися в автомобільних двигуна, доцільно відновлювати методами наплавлення з використанням зносостійких наплавочних матеріалів.

колінчастий вал, двигун, дефект, зношування

Постановка проблеми. В процесі експлуатації автомобілів відбувається зміна їх технічного стану, основними причинами якого є зношування, втомне руйнування, пластична деформація, корозія. Пластична деформація і втомне руйнування є наслідком конструктивно-технологічних недоробок або порушення правил експлуатації, а також відбувається внаслідок природнього зношування деталей.

Для зниження витрат при експлуатації автомобільних двигунів внутрішнього згорання доцільно використовувати відновлення зношених деталей та повторне їх використання. В першу чергу це стосується базових деталей двигунів. До таких деталей відноситься зношений колінчастий вал, який часто становить майже половину вартості двигуна.

Аналіз останніх досліджень та публікацій. Вибором ефективних методів відновлення деталей почали займатися з появою промислових видів ремонту. Значний внесок у вирішенні цих питань внесли провідні фахівці в галузі ремонту, такі як: Черновол М.І., Карагодин В.І., Латипов Р.А., Молодик Н.В., Новіков О.М., Серебровский В.І, Шадрічев В.А., Червоіванов В.І., Ульман І. Е. та інші. [1-5]

Мета і завдання досліджень. Метою роботи - є дослідження дефектів колінчастих валів, причин їх виникнення та можливих способів усунення дефектів.

Для досягнення поставленої мети вирішувалися наступні задачі досліджень:

1. виконати аналіз можливих дефектів колінчастих валів автомобільних двигунів;
2. проаналізувати причини виникнення дефектів колінчастих валів.

Об'єкт дослідження - колінчасті вали двигунів автомобілів, що підлягають відновленню.

Предмет дослідження – технологія відновлення зношених колінчастих валів плазмово-порошковим наплавленням.

Методи досліджень базуються на експериментальних методах досліджень стану поверхні шийок колінчастих валів.

Колінчасті вали автомобільних двигунів зазвичай виготовляють з вуглецевих сталей, які, в порівнянні з легованими, менш схильні до виникнення різного роду дефектів і не вимагають складної термічної обробки. Якщо необхідні більш високі механічні властивості, застосовують низьколеговану сталь 40Х з підвищеною в'язкістю. Колінчасті вали, в залежності від ступеня напруженості, виготовляють з сталей 45, 40Х, 30ХМА, 40ХМА.

Поверхневу твердість і зносостійкість шийок валів із сталей 45, 40Х підвищують до 50-55 HRC високочастотним загартуванням. Твердість шийок і втомлену міцність всього вала іноді збільшують азотуванням.

Характерними дефектами колінчастих валів двигунів є знос і задири шийок, деформації, тріщини і поломки [1, 2, 3.]. Тріщини і поломки валів виникають як в шийках в області галтелей, так і в щоках. Причиною тріщин і поломок є циклічні напруження, що призводять до виникнення втомлених тріщин. В процесі експлуатації межа витривалості колінчастих валів знижується на 25-30%. Ресурс роботи колінчастого вала залежить від його межі витривалості і зносостійкості робочих поверхонь [4].

Основною причиною відмов колінчастих валів більшості двигунів є знос шийок [3, 4, 5]. Знос має нерівномірний характер як по колу, так і по довжині шийки. В результаті зношування зазори в парі тертя «вкладиш - шийка колінчастого вала» і параметри шорсткості шийок зростають, що призводить до розриву мастильної плівки і задирам робочих поверхонь. Задири шийок в свою чергу призводять до провертання вкладишів, деформації валу і підплавлення антифрикційного шару вкладишів.

Слід зазначити, що швидкість і нерівномірність зношування шийок більша, ніж швидкість і коефіцієнт нерівномірності зношування вкладишів [5].

Передчасне зношування робочих поверхонь колінчастих валів вище граничних значень веде, як правило, не тільки до значних витрат на ремонт або заміни валів, а й до збитків через простій автомобіля в ремонті. Через підвищення швидкості зношування робочих поверхонь колінчасті вали часто експлуатуються шліфованими під останній ремонтний розмір, або вибраковуються через зношування вище граничних значень, при цьому не відпрацювавши до нормативного ресурсу.

Відомі положення про можливість розривання мастильної плівки при нестаціонарних режимах роботи, які спостерігаються в період пуску в роботу підшипникового вузла ковзання, що може привести до явищ задирання і, як наслідок, до катастрофічного руйнування підшипникового вузла колінчастого валу.

Оцінка надійності колінчастих валів дизелів після ремонту шляхом шліфування під ремонтний розмір показала, що вони мають низький ресурс внаслідок зниження межі витривалості, тому необхідно застосування методів їх зміцнення. Крім того, при використанні технології перешліфування під ремонтний розмір часто знімається загартований або азотований поверхневий шар, що забезпечує необхідну зносостійкість шийки вала.

Таким чином, основною причиною відмов колінчастих валів двигунів є знос і задири шийок. Отже, підвищення довговічності колінчастих валів можливо тільки шляхом збільшення зносо- і задиростійкості шийок технологічними методами. Однак, в літературі недостатньо інформації за видами причин і наслідків відмов колінчастих валів.

Колінчастий вал двигуна внутрішнього згоряння працює в умовах дії змінних сил і моментів від тиску газів у циліндрі двигуна, інерційних сил через нерівномірність руху деталей шатунно-поршневої групи й вібрацій від крутильних і згинаючих коливань вала.

Під впливом одночасного впливу тиску газів і сил інерції (а також їх моментів) у колінчастому валу виникають циклічно змінні напруження кручення й згину. Напруження кручення можуть досягати дуже великої величини, особливо у випадку співпадіння частоти зміни збуджучої їх сили із частотою власних крутильних коливань вала. Це приводить до утворення в найбільш напружених місцях втомлених тріщин, розвиток яких може викликати поломку вала.

Руйнування колінчастих валів від утоми починається, звичайно, біля вихідного отвору для мащення корінних і шатунних шийок і в галтелях у сполученнях шийок із щоками. Запас втомної міцності для автотракторних валів невеликий і рівний 1,5...3,0. Тому, утома може виявитися лімітуючим фактором, що визначає службову довговічність вала, його витривалість.

Зміни величин зазорів і овальності шийок вала по мірі зносу впливають на роботу підшипника. Встановлено, що в підшипниках двигунів мінімальна товщина мастильного шару може зменшуватися від 11,5 мкм при початкових умовах експлуатації до 5 мкм при граничних зазорах (0,35 мм) і максимальних рекомендованих в експлуатації температурах масла (до 67 °С). При граничних зазорах і максимальних рекомендованих температурах масла на вході (75 °С) середня мінімальна товщина мастильного шару зменшується до величин, коли не забезпечується рідинне тертя в вузлі. Ще більше зменшення товщини шару має місце в підшипниках.

В процесі роботи двигуна відбувається знос шийок валу і вкладишів. Причому знос нерівномірний по колу шийки, в результаті чого виникає овальність шийок вала, яка надає складного впливу на характеристики підшипників. У зонах найбільшого зносу радіус кривизни поверхні збільшується, що зменшує різницю радіусів і підвищує реакцію мастильного шару в цій зоні. Одночасно овальність викликає значні додаткові переміщення шийки уздовж лінії центрів з більшими, ніж у незношених вала, швидкостями, що призводить до зменшення мінімальної товщини мастильного шару. Установлено, що зі збільшенням овальності шийок товщини мастильного шару в усіх вимірюваних точках шийки вала зменшуються.

По мірі збільшення овальності шийок зростає биття колінчастого вала, яке, в свою чергу, впливає на їх зношування. Встановлено, що між зносом шийок колінчастих валів і биттям є кореляційна залежність. Биття не тільки збільшує знос шийок, що в свою чергу ще більше збільшує биття, але і збільшує дисбаланс колінчастого вала і вібрацію двигуна, а це веде до зменшення втомної міцності вала.

Конусоподібність шийок веде до збільшення зносу деталей циліндро-поршневої групи внаслідок зростання непаралельності осі шатуна осям гільзи циліндра і поршня.

Таким чином, знос шийок валу викликає погіршення умов роботи підшипників і всієї циліндро-поршневої групи, тому величини овальності і конусоподібності слід обмежувати. Однак, як показує досвід, гранична овальність шийок встановлюється головним чином з міркувань забезпечення необхідного запасу міцності колінчастого вала.

Відзначено, що середня величина відхилення від номінального діаметра в зоні найбільшого зносу (при нормальному зносі) корінних шийок становить 0,027 мм, а шатунних 0,029 м. Биття середньої шийки для нормально зношених валів знаходиться в межах від 0,02 мм до 0,17 мм, при цьому середня величина биття становить 0,054 мм, а для аварійного зносу в межах від 0,040 мм до 0,730 мм, при середній величині биття - 0,227 мм.

Висновки. Встановлено основні дефекти колінчастих валів: лінійний знос, риски, задирання, тріщини, деформації. Для підвищення довговічності та поліпшення умов експлуатації підшипників колінчастих валів двигунів необхідно:

- підвищувати зносостійкість шийок валів;
- забезпечувати більш високу зносостійкість шийок в порівнянні з зносостійкістю антифрикційного шару вкладишів підшипників ковзання.

Список літератури

1. Балабанов, В. И. Повышение ресурса дизелей фрикционным латунированием шеек коленчатых валов в ремонтном производстве: автореф. дис. . канд. техн. наук: 05.20.03 / Балабанов Виктор Иванович. - М., 1992. - 18 с.
2. Буравцев, С. К. О состоянии характеристик коленчатых валов и их влияния на показатели двигателей / С. К. Буравцев // Двигателестроение. - 2006. - № 1. - С. 38-42.
3. Ильиных, С. А. Восстановление коленчатых валов двигателей Камаз методом плазменного напыления / С. А. Ильиных, В. А. Крашанин, Е. В. Исаков, И. А. Попова // Технологии ремонта, восстановления, упрочнения и обновления машин, механизмов, оборудования и металлоконструкций: Материалы 6-й меж дунар. научно-практ. конференции. - СПб. - 2004. - С. 231.
4. Кубич, В. И. Износостойкость деталей трибосопряжения «шейка- вкладыш» / В. И. Кубич, Л. И. Ивщенко // Проблемы трибологии. - 2011. - №2. - С. 103-110.
5. Захаров, С. М. Моделирование работы трибосистемы коленчатый вал- подшипники-опоры блока цилиндров двигателей внутреннего сгорания /С.М. Захаров, И. В. Сиротенко, И. А. Жаров // Трение и износ. - 1995. - Т. 16, № 1. - С. 47-54.

УДК 631.1

Г. Чернякова, магістр гр. МЕ-19М-1,4
Центральноукраїнський національний технічний університет

ОСОБЛИВОСТІ УПРАВЛІННЯ СІЛЬСЬКОГОСПОДАРСЬКИМ ПІДПРИЄМСТВОМ

У статті розглянуто особливості управління сільськогосподарським підприємством на базі сучасного фермерського господарства. Здійснено аналіз передумов успішного управління, сучасних причин низького рівня ефективності українського аграрного сектору. Обґрунтовано інноваційні напрямки удосконалення ефективності управління сільськогосподарським підприємством.

управління, сільськогосподарське підприємство, фермерське господарство

Постановка проблеми. Трансформаційні зміни економічних відносин у сільському господарстві зумовили потребу у розвиткові різних підприємств. У поєднанні з ринковими засадами діяльності нова організаційно-економічна структура аграрної сфери суттєво змінила зміст та складові економічних відносин. Сьогодні сільськогосподарське виробництво все частіше називають агробізнесом. У зв'язку з цим підприємництво, безумовно, стає вагомою ознакою аграрного виробництва.

Створення великої кількості суб'єктів господарювання різних організаційно-правових форм є однією з умов формування конкурентного ринкового середовища в аграрній сфері нашої держави. Специфіка формування та функціонування сучасних фермерських господарств поруч із підприємствами інших форм господарювання чітко регламентована законодавчо, що дозволяє уникати певних колізій на етапах пов'язаних із їх заснуванням. Проте деякі труднощі чекають на менеджерів підприємств вже в процесі управління ними. Зокрема дані проблеми базуються на відсутності традицій функціонування приватної власності в сільському господарстві, низьким рівнем матеріально-технічного забезпечення, що стає причиною особливостей управління внутрішнього господарства і не дає можливості оперативно реагувати на різкі зміни зовнішнього середовища.

Однак, в умовах конкурентного ринку, виразно відзначаються переваги такої форми організації бізнесу як одноосібне фермерське господарство, оскільки таке управління дає можливість самостійно і швидко приймати рішення без додаткового узгодження із будь-яким колективним органом, а також відсутність потреби у розподілі прибутків, що значно зменшує потенційну ймовірність поділу таких підприємств. Зазначені переваги роблять сільськогосподарське підприємництво в аграрній сфері вигідним і дозволяють здійснювати

порівняно ефективну господарську діяльність, створювати робочі місця і, навіть, частково відновлювати соціальну інфраструктуру сільських територій. Практична значимість вирішення проблем удосконалення управління сільськогосподарським підприємством зумовлює вибір актуальної теми нашої роботи.

Аналіз останніх досліджень і публікацій. Різні аспекти управління підприємствами в науковому дискурсі не є новими, оскільки аспекти її дослідження змінюються разом із економічними, політичними, соціальними векторами держави (В. Андрійчук, О. Березін, Н. Бутенко, О. Величко, М. Малік, П. Саблук, М. Федорова, К. Петросян, А. Моїсеєва).

Особливості управління сільськогосподарським підприємством стали об'єктом досліджень багатьох науковців, зокрема акцентуація на фермерські господарства знайшла своє відображення у працях Т. Дьолог, О. Зеленко, О. Клокар, А. Третяк, Т. Яворської [1; 2; 3; 6; 7] та інших.

Мета й завдання дослідження. Метою статті є аналіз особливостей управління сільськогосподарським підприємством на базі сучасного фермерського господарства, та напрацювання пропозицій щодо удосконалення ефективності господарювання.

Виклад основного матеріалу. На сьогодні розвиток сучасного аграрного бізнесу як сектору економіки України відбувається в динамічних, трансформаційних умовах на усіх рівнях, зокрема і на рівні інституційної структуризації господарських суб'єктів. Важливого значення у забезпеченні соціально-економічного розвитку села як середовища і об'єкта господарювання набуло вирішення проблеми функціонування дрібних селянських підприємств з метою сприяння їх конкурентоспроможній інституціоналізації в загальну систему організованого аграрного ринку.

Згідно Концепції розвитку фермерських господарств та сільськогосподарської кооперації на 2018-2020 роки глобальні виклики останнього десятиріччя спричинили структурні зміни в економіці країни та регіонів. Загальними тенденціями 2010-2019 років стало збільшення частки сільського господарства (на 3,8 в.п. - з 8,3% до 12,1%) та державного управління (на 1,3 в.п. з 5,2% до 6,5%) при зменшенні питомої ваги інших складових: сфери послуг (на 3,6 в.п. - з 57,3% до 53,7%), промисловості (на 0,7 в.п. – з 25,% до 25,2%), будівництва (на 0,8 в.п. – з 3,3% до 2,5%) [4]. Отже, регулювання діяльності сільськогосподарських підприємств вимагає концептуальних змін з метою зростання їх ефективної.

Сучасна економічна ситуація, дія інституційного механізму ринку характеризується динамічністю різних за напрямком змін у рівнях соціально-економічного розвитку села та сільських територій, що визначним чином вмотивовує активізацію процесів щодо вдосконалення системи управління універсальних блоків аграрного сектору.

О. О. Зеленко зауважує, що рівень ефективності управління сільськогосподарськими підприємствами, насамперед, «залежить від методів, інструментів, що застосовуються, кваліфікації керівних кадрів, технічного забезпечення, кількості та якості інформації» [2, с. 72]. Система, на основі якої реалізовуються функції управління, називається системою управління. За А. М. Третяком, у ній виокремлюють два ключові складники, а саме управляючу й керовану системи. Управляючою системою є суб'єкт, що здійснює функції управління, натомість керована – це його об'єкт. Якщо управління здійснюється свідомо, то управляюча система створюється суб'єктом управління. Його головне завдання полягає саме в тому, щоб зорієнтувати розвиток об'єкта в бажаному напрямі за допомогою управлінського впливу [6].

У цілому ефективність сільського господарства в державі формується завдяки ефективності її структурних елементів – областей та регіонів. Так, різні області мають індивідуальну спеціалізацію, структурні особливості, специфічні відмінності щодо становлення та формування організаційно-правових форм господарювання.

В Україні організаційно-правові форми сільськогосподарських підприємств та об'єднань визначаються чинним законодавством і класифікацією організаційно-правових форм господарювання, затвердженою наказом № 97 Державного комітету України з питань

технічного регулювання та споживчої політики від 28 травня 2004 р [2]. Виокремлення різних типів економічної власності обумовлено тим, що в межах кожного з них функціонують окремі форми, види власності, що формуються в окремі види підприємств, що, у свою чергу, зумовлює існування різних видів і форм підприємницької діяльності.

Зазначимо, що на сьогодні у науковій парадигмі сільськогосподарські підприємства класифікується за п'ятьма ознаками, а саме:

- за формою власності – державні, приватні, колективні, змішані підприємства;
- за організаційно-правовою формою господарювання – господарські товариства, фермерські господарства, приватні та державні підприємства, кооперативи, інші;
- за масштабами виробництва – великі, середні, малі;
- за спеціалізацією – спеціалізовані, багатогалузеві;
- за розміщенням – місцеві, регіональні, національні, транснаціональні.

Незважаючи на низку типів за специфічними ознаками, ключовим для всіх підприємств є те, що аграрне підприємство – це юридична особа, основним видом діяльності якої є виробництво та/або переробка сільськогосподарської продукції, виручка від реалізації якої становить не менше 75% від загальної суми виручки.

Однією із особливостей аграрних підприємств є те, що вони працюють в умовах високого ризику та відіграють важливу роль у формуванні соціальної сфери на селі, а також способу життя сільських мешканців. В Україні всі підприємства здійснюють свою діяльність у відповідності до правового статусу закріпленого в Господарському кодексі України.

Для формування продуктивних умов управління повинне бути чітке й свідоме розуміння, за яких умов може бути здійснення успішної підприємницької діяльності в аграрному секторі, до яких ми відносимо наступне:

1. Власне бажання підприємця здійснювати таку діяльність, наявність фінансових ресурсів, яких буде достатньо, щоб започаткувати власну справу, ключові якості менеджера – готовність до ризиків, нестандартне мислення, націленість на результат та успіх;

2. Самостійність у виборі форм і напрямів підприємницької діяльності, організації виробничо-господарських процесів та управління ними;

3. Свобода та самостійність у підприємницькій діяльності мають бути помірними для успішної роботи, проте це не має суперечити чинному законодавству та наносити шкоду споживачам, державі та суспільству загалом.

Так, до головних причин, що стримують розвиток сільськогосподарського підприємства в Україні, зокрема на рівні управління, варто віднести:

1. Відсутність реальної фінансового-кредитної підтримки;
2. Диспаритет цін на сільськогосподарську продукцію і промислову продукцію;
3. Недосконале законодавство в напрямі захисту підприємництва, особливо в галузі земельних відносин;
4. Неналежна державна підтримка аграрних підприємств;
5. Нестабільна економічна і політична ситуація в державі;
6. Постійне втручання державних органів в діяльність господарських суб'єктів [7, с. 47-48].

Т. І. Дьолог зауважує, що управління сільськогосподарськими підприємствами потребує від керівників всіх ієрархічних рівнів врахування специфіки аграрної галузі, що, у свою чергу, визначає особливості функціонування і розвитку цих підприємств. Зокрема, до зазначених особливостей доречно віднести наступне:

1. Взаємозв'язок сільського господарства з природою (клімат, ландшафт, зокрема непередбачувані природні збитки) та середовищем існування людей.

2. Враховуючи стратегічну важливість аграрної галузі, можливість і необхідність здійснення у деяких випадках виробництва сільськогосподарської продукції навіть за умови збитковості зазначеного виробництва (надання збитковим підприємствам державної підтримки).

3. Існування значного ступеня ризику (пов'язаного з природно-кліматичними факторами), високої конкуренції в межах даної галузі і повільної швидкості грошового обігу.

4. Існування певних технологічних особливостей здійснення сільськогосподарського виробництва.

5. Нееластичність зв'язку між цінами на продукцію сільського господарства і попитом.

6. Стратегічна важливість аграрної галузі, так як вона безпосередньо пов'язана з продовольчою безпекою держави [1, с. 101-102].

Удосконалення системи управління сільськогосподарським підприємством повинно базуватися на сучасних інноваційних підходах. Так, в аспекті управління, інноваційною є така діяльність, що спрямована на пошук можливостей інтенсифікації операційної діяльності та виробництва, зокрема запит на реалізацію суспільних потреб у конкурентоспроможній сільськогосподарській продукції, товарах та послугах завдяки використанню науково-технічного та інтелектуального потенціалів. Дана управлінська діяльність менеджера господарства пов'язана з отриманням якісно нової, радикально покращеної продукції, технології її виробництва, організаційних форм і методів господарювання та системи управління.

Висновки. Отже, існує певне коло викликів, з якими зустрічається управлінець в агробізнесі, проте їхнє вирішення потребує державної підтримки, змін та трансформації економічних потоків. Успішне функціонування фермерських господарств місцевого типу можливе за умови стратегічного, цільового управління керівником із чітким планом, що передбачає специфічні особливості аграрного сектору. Інноваційна система управління є перспективним аспектом дослідження, що сприятиме практичній реалізації ефективного менеджменту сучасного сільськогосподарського підприємства.

Список літератури

1. Дьолог Т. І. Проблеми і особливості управління вітчизняними сільськогосподарськими підприємствами. Інноваційна економіка. 2013. № 3. С. 101-104.
2. Зеленко О. Особливості управління сільськогосподарськими підприємствами. Економічний часопис Східноєвропейського національного університету імені Лесі Українки. 2017. № 1. С. 71-75. URL: http://nbuv.gov.ua/UJRN/echcenu_2017_1_11 (дата звернення: 11.11.2020)
3. Клокар О. О. Аналіз та підвищення ефективності підприємницької діяльності в аграрному секторі економіки. Формування ринкових відносин в Україні. 2011. № 7 (122). С. 67-69.
4. Про схвалення Концепції розвитку фермерських господарств та сільськогосподарської кооперації на 2018-2020 роки : Розпорядження Кабінету Міністрів України від 13.09.2017 року № 664-р. База даних «Законодавство України» / ВР України. URL : http://zakonO.rada.gov.ua/laws/show/664-2017-%D1%80 (дата звернення: 11.11.2020).
5. Сільське господарство України: Стат. збірник за 2018 рік / за ред. Ю.М. Остапчука. К.: Держстат України, 2018. 370 с.
6. Третяк А. М. Управління земельними ресурсами : навч. посіб. Вінниця : Нова кн., 2006. 360 с.
7. Яворська Т. І. Малий бізнес у сільському господарстві: теорія і практика: монографія. Т. І. К. : ННЦ ІАЕ, 2012. 386 с.

УДК 338.439

Б. Шайда, магістр гр. ЕО-19мз
Л. Коломієць, доцент
Центральноукраїнський національний технічний університет

АНТРОПОГЕННИЙ ВПЛИВ НА ВЛАСТИВОСТІ ГРУНТІВ УРБАНІЗОВАНИХ ТЕРИТОРІЙ

Проаналізовано питання антропогенного впливу на грунти урбанізованих територій, з метою покращення їх властивостей та виявлення дій які шкодять йому.

Сучасні екологічні дослідження свідчать про те, що під впливом діяльності людини міські ґрунти сильно змінюються і, у зв'язку з цим, мають низку специфічних особливостей. Їх основні групи – природні та штучні насипні ґрунти – кардинально відрізняються один від одного як за фізико-хімічними показниками, так і за особливостями акумуляції забруднюючих речовин. Для них характерна близька до нейтральної реакція ґрунтового розчину, підвищений порівняно з приміськими ґрунтами вміст фосфору, калію.

Актуальність. Сучасний стан навколишнього середовища і подальше його погіршення викликає обґрунтовану тривогу, оскільки цим зумовлені численні екологічні, санітарно-гігієнічні та інші проблеми. Особливе місце за гостротою цих проблем посідають урбанізовані території – складні багатофункціональні природно-антропогенні системи, у яких домінує людина. Вони являють собою «згущення» населення і енергоспоживання, де мало що збереглося від вихідного стану природних ландшафтів.

Мета дослідження. Метою є дослідження екологічних властивостей грунтів урбанізованих територій.

Завдання:

- проаналізувати функції грунтів в урбоекосистемі
- виявити характерні особливості урбоземів м. Кропивницький на основі аналізу їх фізико-хімічних та морфологічних властивостей
- надати пропозиції щодо покращення екологічного стану урбаноземів

Об’єкт дослідження: зміна властивостей грунтів під впливом урбанізації.

Предмет дослідження: грунти урбанізованих територій.

Результати досліджень.

Людська цивілізація набирає стрімкого розвитку а разом і з нею розвивається науковий та технічний прогрес. Такий різкий розвиток призводить до більших потреб населення, а саме збільшення обсягів промисловості, розвитку транспорту, урбанізації територій, розвитку енергетики на сам перед ядерної, а це є приводом до збільшення радіації у повітрі. Тому данні чинники дуже сильно сказуються на екологічній ситуації не тільки нашої країни, а й усього людства в цілому.

Однією з найважливіших рис сучасності є урбанізація, що охоплює все більшу кількість країн і територій. Ця проблема зачіпає і Україну де із 42 млн. чол., 29 млн.

Під урбанізацією розуміється зростання і розвиток міст, збільшення ваги і ролі міського населення в даному регіоні. Індустріальні, особливо великі за чисельністю населення, міста стали виникати і множитися з середини XIX ст. У XX в. індустріальне виробництво зросло в 50 разів. Міста вмістили нові види складних виробництв, в них сформувалися промислові зони, площа яких порівнянна з площею житлових районів.

Сучасна урбанізація супроводжується значним відчуженням земель, часто продуктивних, під міські забудови та промислові об'єкти і площа таких земель повсюдно збільшується.

Найбільш урбанізованими регіонами є Австралія, Нова Зеландія, Північна і Західна Європа, Де рівень міського населення перевищує 80 %, в Південній Європі цей показник дорівнює 66 %, в Східній Європі і Колишньому СССР- 66 %, відповідно. Особливо багато міських земель в Європі, так у Бельгії вони складають 28 %, Великобританії - 12 %, Німеччині - 12 % площ. За даними Організації економічного співробітництва і розвитку, за останні двадцять років площа під забудовами росла в 2 рази швидше, ніж населення.[6]

Таблиця 1. – Площа земель міст в населених пунктах

Республіка	Площа %
Азербайджан	2
Вірменія	3,50
Білорусія	4,20
Киргизія	0,85
Грузія	1,63
Казахстан	0,89
Молдавія	8,29
Латвія	1,81
Литва	2,11
Україна	8,95
Росія	0,65
Узбекистан	1,02
Естонія	1,67
Таджикистан	0,66
Туркменія	0,22
СРСР в цілому	0,98

Площа урбанізованих земель, включаюча площа населених пунктів (міст, селищ і сільських населених пунктів) і земель під будівлями, дворами, вулицями і площами, зайнятими промисловими підприємствами, залізничним транспортом і так далі, значно коливається (табл. 1.1). Найбільші площі займають у більше сільськогосподарських розвинених республіках - Україні (8,95%, в т.ч. сільські населені пункти - 6,30%) і Молдавії (8,29% в т.ч. сільські - 7,35%). [2]

Вперше термін «міські ґрунти» був введений Бокгеймом (J. Bockheim, 1974), визначив його як «грунтовий матеріал, що містить антропогенний шар несільськогосподарського походження.

Таблиця 2. – Характеристика міських грунтів

Blume,1998	Міські,індустріальні грунти	Поділяється на 3 групи: -змінені природні грунти; -грунтові суміші, або антропогенні грунти на основі субстрату; -запечатані грунти
Burghardt,2002	Міські грунти	-грунти знаходяться на початку свого розвитку; -навколишнє середовище грунтів змінилося; -грунти з перенесеними

		горизонтами проявляють ознаки перенесених грунтів
Грунтова карта світу, 1985,2002	Антропогенні грунти	-виникли під впливом людської діяльності
Fiedler,2001	Міські грунти	-антропогенні грунти класифікують як: наземні культурні грунти, болотні культурні грунти, гірські грунти, перенесені грунти, запечатані грунти, зрошувані грунти та редуктосолі
Pietsch und Kamieth 1991	Міські грунти	-грунти в якості компонентів міської промислової екосистеми
Scheffer und Schachtschabel,2002	Міські індустріальні грнути	-антропогенна зміна факторів розвитку грунтів розглядається, зокрема, як вплив на грунт та його функції, як місця зростання рослин, життєвий простір для організмів, фільтр для забруднюючих речовин, регулятор водного балансу

З таблиці видно, що однією з особливостей міських ґрунтів є наявність запечатанних ґрунтів, ґрунтів, що знаходяться під штучним покриттям.

У всьому світті вважають що запечатаність грунтів досягає приблозно до 0.5 % від усієї території світу. На самперед в країних Європи цей показник складає близько 14 % станом на 2020 рік. Це пов'язано з тим, що формується все більше транспортних узлі, що призводить до зростання дорожнього покриття, для задоволення потреб країн.

Збільшення запечатаності грунтів пов'язують з стрімким зростанням населення. Людини переїєжають у міста, а тому виникає потреба у будівництві нових будинків для проживання, що вже викликає запечатанність та водонепроникненість, а й на додаток призводить до зростання асфальтного покриття тобто будівництву доріг.

Грунти України багато років формувалися під впливом різноманітних чинників а саме: діяльністю людини, кліматом, життєдіяльністю тварин та рослин, мікроорганізмами, геологічними особливостями, тощо.[1]

Тварини,які є мешканцями грунту чинять на нього дію яка призводить ро розпушення та остаточно побрібнюють залишки рослин. Ці залишки слугують добривом для грунту, а тому є досить важливими.

Також на процес грунтоутворення впливає рельєф. Від рельєфу залежить стану грунту, оскільки якщо це крутий схил то вимивання буде проходити інтенсивніше ніж у рівнині.

Дослідженя урбанізація було розглянуто на прикладі м. Кропивницький.

Кропивницький є адміністративним центром Кіровоградської області розташований в центральні частині України, на берегах ріки Інгул, при впаданні в неї менших річок – Сугоклії та Біянки., в межах Придніпровської височини.

Клімат Кропивницького обумовлений його розташуванням у степовій зоні. Середня температура січня тановить − 5,6 С, липня +20,2 С. Середньорічна кількість опадів – 474 мм (у середньому за рік у місті спостерігається 130 днів з опадами), найменше — у березні та жовтні, найбільше – у липні.

Геологічна будова території Кропивницького зумовлена його розташуванням на площі Українського кристалічного щита.

Ґрунти – чорноземи звичайні, глибокі мало- і середньогумусні на лесових породах. Мають високу природну родючість, хоч в орному шарі розпушені і частково втратили в минулому грудкувату структуру.

На території Кропивницького корисні копалини представлені у вигляді матеріалів для будівництва. Такими прикладає є: гранітне родовище, що розташовано біля річки Сугоклея, запаси вогнетривких глин, вугілля. [5]

Кропивницький перетинає річка Інгул та Сугоклея, також є невелика кількість струмків. Головною ознакою данних річок є те що вони утворюють своєрідні каньйони зі скелястими крутими схилами. Також в наявності є два водосховища, а саме Кіровоградське та Лелеківське. Обсяг стіку Інгулу розподілився таким чином:

- Березень – травень – 75 %;
- Червень – серпень – 7 %;
- Вересень – листопад – 5%;
- Грудень – лютий – 13 %.

Середня тривалість льодоставу – 2,5 місяці.

Товщина льоду сягає 20-40 см.

Урбанізація територій в наш час досить тісно пов'язана з глобальними проблемами які виникають в наслідок цієї урбанізації. Розвиток великих країн та міст призводить до збільшення викидів шкідливих речовин у грунт, воду, повітря, тощо.[38].

Грунти напевно є одним з найголовніших компонентів у біогеоценозі. Грунт досить щільно пов'язаний з атмосферою, тваринним та рослинним світом, людино, та екологічною системою взагалом.

Останнім часом проводяться дослідження, що до стану грунту в Україні та стану грунту в цілому у світі. Дані дослідження стосуються тільки викидів важкиї металів у грунт підприємствами, що не дає нам змоги детально оцінити стан грунту, оскільки критерій дуже мало.[7]

Урбанізовані територія це – усе навколишнє серодовище з яким в певній мірі кожного дня контактує людина. До таких територій належать: житлові будинки, парки, зони відпочинку, міські та приміські будівлі, будівлі державного типу, школи, дитсадки, університети, дороги у місті, траси за містом, місця зведення заводів та підприємств та багато іншших територій.

Останнім часом відбувається інтенсивна амортизація ґрунтів забудованих територій. Лише парковками для автомобілів зайнято близько трьох четвертих територій які прилагяють до житлових будинків. Комунікації які необхідні для життєдіяльності людини займають близько 35% територій, а саме це стічні труби, каналізації, елементи водопостачання та водовідведення. Тільки ці фактори призводять що року до стрімкого виснаження грунтового покриву та гумусу, шляхом забруднення грунту, та знищенням корисних микроорганізмів та утворенням патогенних.[8]

Існує так званий процес рівноваги урбанізованих територій. Тобто урбанізація природного ннастилу не повинна перевищувати сам природний настил, повинна існувати рівновага, щоб забудова не шкодила навколишньому серидовищу і щоб останнє в свою чергу не втрачало своїх біологічних, хімічних та фізиологічних властивостей.

Таблиця 3. Структура земельного фонду м. Кропивницький

Розподіл земель за цільовим призначенням та функціональним використанням	Тис. га
Територія, усього	10,3
У тому числі: сільськогосподарські угіддя	2,7

З них: рілля	1,6
Ліси та інші вкриті лісом площі	0,7
Забудовані землі	6,3
Води	0,4
Інші землі	0,6

До великого жалю що року якість міських земель втрачають свої корисні властивості, а стан грунту погіршується до неповоротних наслідків.

Спостерігається більша гумусованість поверхневого шару у лісопаркових зонах. Під деревами у яких є досить потужний травостій ми бачимо вміст гумусу який сягає 7%. З цього ми бачимо що насадження в лісопаркових злнах слугуть не тільки вітровим барьєром та за для утворення мікроклімату міста, а й мають дуже важливе значення у відношенні рослина – грунт.

Значення pH (водн.). Практично в усіх ґрунтах міста спостерігається підлужнювання верхньої частини профілю в порівнянні з зональними ґрунтами. Можна з упевніністю стверджувати, що зсув значення pH пов'язаний з підвищеним виявленням лужності у поверхневому шарі грунту. А вміст солей обумовлений тим, що в зимову пору року в грунт потрапляють частки хімічних елементів які входять у суміш для посипання доріг, щоб зменшити небезпечність підсовзнутися.[4]

Спостерігається дуже малий відсоток озеленіння територій у таких приміських районах як Героїв України, 101 – мікрорайону,космонавта Попова. В даних спальніих районах проживає кількість людей більша ніж наявність зелених насаджень. Це пов'язано з тим, що данні райони досить молоді а тому, різкий зріст населення в місті призводив до того, шо мість на проживання не вистачало, а данні територій у певний час були сільськогосподарськими, тому на так звану користь почалась урбанізація данних територій, а про озеленіння не було часу розмірковувати. А той метой догляду за територією яким користуються у наш час приззводить до так званої деградації.

Виходячи з цього потрібно досить швидко реагувати на виявлення погіршення властивостей грунтів за для запобігання катастрофічних наслідків, а саме деградації грунту, зменшення вмісту гумусу, часткове, або повне зникання корисних мікроорганізмів на зміну яким прийдуть патогенні, що виникли шляхом знехтування зелених насаджень.

Відомо, що грунт має буферну властивість за допомогою якої може розкладати деякі речовини. Але той викид сміття та продуктів життєдіяльності людини який потрапляє до грунту, він вже розкласти не може, тому що по трохи втратив цю властивість. Це сталося тому,що обсяг на найменування викидів не може переребити грунт. До таких речовин та матеріалів відносять, полителеновi пакети, цигарки, пластмасу, целофан та багато інших речовин. Для іх переробки повинні буду спеціальні установи. Але на жаль іх не вистачає в тій кількості в якій вони є на данний проміжок часу.

Рішення проблеми урбанізації змусила об'єднатися не тільки екологів між собою, а й представників інших соціальних та технічних процесів з усіх країн світу. В загалому до таких входять представники психології, геології, океанології, представники природничих наук, соціологи, астрологи, технологи, архітектори та багато інших представників яких можна перелічувати до безкінченності.

З плином часу виникло безліч модернізованих ідей будівництва, щоб покращити екологічний стан грунтів. До таких проектів першими вдалися представники Японії. Вони почали будувати приміські зони, бази відпочинку, навіть аєропорти у окені, щоб зменшити навантаження на грунтовий покрив та використовувати його більш за сільськогосподарським призначенням ніж для урбанізації. На данний проміжок часу вже створені штучні острови в океані на яких будуть житлові будівлі. Ці штучні насипні острови мають назви усіх країн світу, там навіть є острів під назвою Україна. Цей своєрідний проект впершу чергу був створений для багатіїв,щоб ті могли відпочити у власній країні. Згодом ця ідея зацікавали інженерів з Китаю, Франції, Австралії.

Сучасна техніка дозволяє інженерам будувати такі штучні країни острови. На них будуть всі ті самі умови для комфортного проживання,інтернет,газ,гаряча вода,спутникове телебачення,магазини, лікарні та вся інфраструктура яка є у місті тільки в океані. Такий підхід до преблеми урбанізації дає змогу не тільки зменшити негативний ввплив на грунт,але й дає дорогу новітнім інтеграціям які не будуть чинити шкоду природі, а навпаки будуть покращувати її стан.[3]

Одним з варіантів успошної екологізації є встановлення так званих обмежувачів міст,тоб то навколо міст створюється густий лісний масив який нагадую пояс. У центрі цього масиву існує місто-мегаполіс. У ньому розвивається все те що і було до цього. Навколо цього міста мегаполіся створюються окремі острови посилення чи окремі соціальні будівлі, а саме школи, магазини, університети та багато іншого, ці всі вузли зв'язані транспортними магістрялями що ведуть до мегаполісу,а в свою чергу той зелений пояс з насаджень повинен охоронятися від вирубки,будівництва та завдаванню шкоди. (приклад – Портланд, США).

Висновок. Незважаючи на фактори урбанізації земель які впливають на стан екологічної системи м.Кропивницький та в цілому усієї України,ми бачимо різке зростання урбанізації в Уукраїні та зниження у інших країнах зарубіжжя. Така тенденція пов’язана насамперед з розуміння того, що природа і так знищується з кожним днем все більше і більше та не встигає відновлюватися. Нажаль це розуміють багато країн, але не Україна. З кожним роком все більше будується будівель,торгових центрів,доріг, а в замін знищуються зелені насадження, водойми, якість грунту. Така політика забудовників не тільки шкодить природі, але й самій людині, чим менше насаджень, тим менше повітря. Знищення водойм на користь доріг погіршує стан фауни. Тваринам все складніше стає добувати собі воду. Тому нам потрібно що найшвидше схаменутися, щоб не загубити те що у нас залиилося.

Список літератури

1. Дорогунцов С.І., Федорищева А.М. Техногенна-екологічна безпека урбанізованих територій України // Екологія та ноосферологія. 1998. – Т.4. - № 1-2 С. 81-91.
2. ДБН 360-92 “Містобудування. Планування і забудова міських і сільських поселень” К: Дуржбуд України. - 2002. – 102 с.
3. Строганова М. Н. Городские почвы: генезис, классификация, экологическое значение (на примере г. Москвы): дис. В форме научного доклада на соискание ученой степени д-ра. биол. наук: спец. 03.00.27. – «Почвоведение» / М. Н. Строганова. – М., 1998. – 71 с.
4. Социальная Хартия городов-членов Союза Балтийских городов, принята на IV Генеральной Конференции СБГ, Росток, 13 октября 2001 г.
5. Кучерявий В.П. Урбоекологія. -Львів: "Світ", 2001. -440 с.
6. Урбанізація навколишнього середовища: охорона природи та здоров’я людини. – К.: Національний екологічний центр України, 1996. – 251 с.
7. Кучерявый В.А. Зеленая зона города. – К.: Наук. думка, 1981. – 248 с.
8. Стародубцев С.Є.Механізм державного управління природокористуванням урбанізованих територій на інноваційній основі/ автореферат дисертації на здобуття наукового ступеня кандидата наук з державного управління, Київ, 2010. - 7с.

УДК 621.431.3

М. Шеломієнко, магістр гр. АТ19М
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ШЛЯХІВ ПІДВИЩЕННЯ ПРОДУКТИВНОСТІ АРГОНОДУГОВОГО НАПЛАВЛЕННЯ ПРИ ВІДНОВЛЕННІ АВТОМОБІЛЬНИХ ДЕТАЛЕЙ

В роботі визначено основні напрямки підвищення продуктивності методу аргонодугового наплавлення та обрано найбільш ефективний, з точки зору автора, метод підвищення швидкості плавлення електрода – нахилом електроду та наданням йому обертального руху.

аргонодугове наплавлення, відновлення, захисний газ

Постановка проблеми. Відновлення деталей є технічно обґрунтованим і економічно виправданим процесом насамперед в зв'язку з можливістю повторного і неодноразового використання 60...75% зношених деталей. Собівартість відновлення зношених ремонтопридатних деталей не перевищує 30...50% вартості нових, а витрата матеріалів в 25...45 разів нижча, ніж на їх виготовлення.

Більшість розроблених до теперішнього часу електродугових способів відновлення деталей малопродуктивні через невисокі швидкості процесу, невиправдано великі питомі енергетичні вкладення, які можуть досягати 108 Дж/м^2. Внаслідок чого відбувається значний термічний вплив на деталь.

Підвищення точності розрахунків параметрів процесу наплавлення, розробка принципово нових і вдосконалення ресурсозберігаючих технологічних способів нанесення покриттів, поверхневого зміцнення електричною дугою, спрямовані на комплексне забезпечення необхідної якості, є актуальною проблемою ремонтного та машинобудівного виробництва.

Аналіз останніх досліджень та публікацій. Вибором ефективних методів відновлення деталей почали займатися з появою промислових видів ремонту. Значний внесок у вирішенні цих питань внесли провідні фахівці в галузі ремонту, такі як: Черновол М.І., Карагодин В.І., Латипов Р.А., Молодик Н.В., Новіков О.М., Серебровский В.І, Шадрічев В.А., Червоіванов В.І., Ульман І. Е. та Н. Машрабов [1-5].

Мета і завдання досліджень. *Метою роботи* є підвищення продуктивності аргоно-дугового методу наплавлення при відновленні автомобільних деталей.

Для досягнення поставленої мети вирішувалися наступні задачі досліджень:

1. виконати аналіз недоліків аргонодугово наплавлення;

2. проаналізувати шляхи усунення низької продуктивності електродугового наплавлення.

Об'єкт дослідження – технологічні процеси відновлення зношених деталей з використанням високопродуктивних методів нанесення покриття.

Предмет дослідження – технологія відновлення зношених колінчастих валів аргонодуговим наплавленням.

Методи досліджень базуються теоретичному аналізі технологічних методів наплавлення.

Практика застосовуваних методів наплавлення показує, що кожен з них має свої позитивні та негативні сторони. Із переліку цих методів найбільш простий, з точки зору

реалізації в умовах невеликого ремонтного чи сервісного підприємства є метод наплавлення в середовищі захисних газів [1-4]. Даний метод не потребує високоенергетичного та дорого обладнання, високої кваліфікації зварювальника та дорогих матеріалів.

Більшість деталей, що потребують відновлення - це вироби виготовлені з легованих сталей. Для нанесення покриттів високої якості доцільним є використанням в якості захисних газів саме аргону. У порівнянні з вуглекислим газом, покриття отримані в аргоні мають меншу пористість та меншу кількість дефектів [5-7].

Властивості деяких металів і сплавів помітно погіршуються при впливі на них при високих температурах кисню, а в окремих випадках азоту і водню. Для виключення такого шкідливого впливу застосовують зварювання в інертних газах. Захист реакційного зварювального простору в цих випадках здійснюють або струменем захисного інертного газу, відтісняє повітря із зони горіння дуги, або проведенням зварювання в спеціальних камерах зі створенням в них атмосфери необхідного складу.

Найбільш універсальним захисним газом є аргон. У ряді випадків до інертного газу для поліпшення стійкості дугового розряду, формування шва, підвищення продуктивності додають різні активні гази.

Завдяки надійному захисту розплавленого металу від шкідливого впливу кисню та азоту повітря при аргонодугового наплавлення з'являються можливості відновлення деталей з важкозварювальних матеріалів, в тому числі алюмінію і його сплавів, бронзи, латуні, нержавіючих сталей і інших матеріалів. У ремонтному виробництві наплавлення із захистом аргоном найбільш широко використовується для відновлення автомобільних деталей з алюмінію і його сплавів.

Аргонодугове зварювання здійснюється електродами, що не плавляться або такими, що плавляться електродами [5]. При відновленні використовується в основному наплавлення неплавким вольфрамовим електродом з ручною або механічною подачею присадочного матеріалу в зону горіння дуги.

Наплавочні матеріали, що використовуються при цьому виді наплавлення, - це вольфрамові електроди, присадочний матеріал і газ. При зварюванні неплавким електродом останній не повинен брати участь у формуванні складу наплавленого металу або металу шва. Основним завданням неплавких електродів є забезпечення стійкого горіння дуги при мінімальній їх витраті.

Найбільшого поширення в якості неплавких електродів отримали вольфрамові стрижні. Такі електроди мають необхідну електропровідність, високу механічну міцність, що дозволяє їх використовувати у вигляді стрижнів малого діаметра. Температура плавлення найбільш тугоплавкого з металів - вольфраму - дорівнює 3377°С, а температура його кипіння близько 4700°С. Такі властивості забезпечують неплавким електродам високої стійкості.

Плавкі електроди з вольфраму відносяться до дорогих і дефіцитних зварювальних матеріалів. Тому при зварюванні вольфрамовим електродами необхідно виконувати певні умови для зниження витрати вольфраму в процесі горіння дуги. Так посилюється витрачання електродів в результаті плавлення внаслідок утворення на їх торцях більш легкоплавких сплавів вольфраму з зварювальними складовими. Ці складові потрапляють на торець електрода як в результаті прямого контакту електрода зі зварюваним виробом при короткому замиканні під час запалювання дуги, так і в результаті конденсації пари і попаданні крапель з зварювальної ванни на торець електрода. Тому, зазвичай прагнуть виключити контакт електрода з виробом при запалюванні дуги. Запалювання виконують на додатковій графітовій пластині або накладенням в момент запалювання на дугового проміжок високої напруги великої частоти, що викликає пробивання міжелектродного простору без контакту. Для полегшення збудження дуги плавкий електрод повинен містити речовини з малою роботою виходу електронів. Хороші результати дає добавка в порошок вольфраму перед пресуванням двоокису торію (ThO_2) в кількості 1,5 - 2%. Такі торовані електроди марки ВТ-15 значно більш стійкі проти оплавлення торця.

В якості присадочного матеріалу використовують прутки, дріт, смугу з того ж алюмінієвого сплаву, що і зварюваний (наплавляється) матеріал, або застосовують електродний дріт, що містить кремній Св-АК5, Св-АК10, Св-АК12 і ін.

Інертний газ аргон отримують з повітря методом ректифікації в спеціальних розділових колонах. Отриманий таким чином "сирий" аргон містить значну кількість домішок, зокрема кисню. Подальше його очищення здійснюється безполуменевий з'єднанням кисню з додаються воднем в присутності каталізаторів. У чистому аргоні в якості домішок залишається невелика кількість азоту, кисню і вологи.

Аргон сорту А призначений для зварювання хімічно активних металів (титану, цирконію, ніобію), сплавів на їх основі, а також для зварювання алюмінієвих сплавів, що плавиться. Аргон сорту Б використовується для зварювання неплавким електродом сплавів алюмінію, магнію та інших матеріалів, чутливих до домішок кисню та азоту. Аргон сорту В застосовують для зварювання нержавіючих сталей різних класів.

Аргон, будучи більш важким, ніж повітря, своєї струменем краще захищає метал при зварюванні в нижньому положенні. Розтікаючись по поверхні виробу, що зварюється, він захищає досить тривалий час широку і протяжну зону як розплавленого, так і нагрітого при зварюванні металу.

Аргон поставляється в балонах, в які він нагнітається під тиском 15 МПа. Щоб не допустити потрапляння повітря і вологи в балони їх забороняється використовувати до повного зниження надлишкового тиску. При, наявності залишкового тиску, рівного 0,3…0,5 МПа, потрапляння в балон вологи і повітря малоймовірне, і при подальшому наповненні аргон матиме необхідну чистоту. Устаткування, режими і техніка зварювання, що застосовуються при аргонодугового зварювання, багато в чому визначають якість відновлених деталей. Для відновлення автомобільних деталей використовують спеціальні установки УДГ-301, УДГ-501, -УДАР-500, що працюють на змінному струмі.

Після закінчення зварювання дугу обривають поступово для заварювання кратера. Це здійснюють при ручному зварюванні поступовим розтягуванням дуги, а при автоматичній - спеціальним пристроєм заварки кратера, що забезпечує плавне зменшення зварювального струму. Довжина зварювальної дуги при повинна бути в межах 1,5 - 3 мм, а її діаметр повинен становити 0,8 1,5 діаметра електрода.

У ремонтному виробництві використовують для відновлення деталей аргонодугове зварювання електродом, що плавиться. Наплавлення відбувається з крапельним і струменевим перенесенням. З підвищенням струму крапельне перенесення металу електродного дроту змінюється струменевим, і глибина проплавлення збільшується. Критичне значення струму, при якому крапельний перенесення змінюється струменевим, становить при зварюванні алюмінію 70 А.

З метою вибору напрямку підвищення продуктивності процесу наплавлення було розглянуто основні технологічні прийоми підвищення продуктивності.

Підвищити продуктивність наплавлення можливо наступними методами:

1. Наплавлення трифазною дугою. Використовується трифазне джерело живлення. Можливе наплавлення двофазною дугою від двофазного джерела живлення.

2. Використання двох або більше електродів. Для цього електроди збирають в пучки. Пучки електродів використовуються і при зварюванні від однофазного джерела живлення. Пучки електродів із загальним струмопідведенням часто використовуються при наплавленні. Це дуже зручно, так як виходить широка смуга наплавлення. Використовується при наплавленні великої товщини. Таким чином підвищується продуктивність на 10% (ефективне використання тепла і за рахунок організації робіт). При наплавленні пучком електродів зварювальний струм вищий, ніж одиночним.

3. Наплавлення з глибоким проплавленням спеціальними електродами.

Електроди з товстим покриттям які містять в покритті, матеріали з високим потенціалом іонізації. Іноді наплавлення ведуть з зануренням.

4. Наплавлення електродами великих діаметрів 6.. . 8 мм.

5. Застосування електродів з металевим порошковим покриттям.

6. Наплавлення лежачим електродом (спеціальні електроди довжиною до 2 мм.). Широко застосовується в суднобудуванні. Раціональна область застосування - короткі шви в важко доступних місцях на матеріалах малих і середніх товщин.

7. Наплавлення похилим електродом або гравітаційне наплавлення. Ведеться з опиранням на козирок.

Одним із шляхів підвищення продуктивності наплавлення є збільшення швидкості процесу.

Аналіз факторів, що впливають на якість нанесеного шару при швидкісному наплавленні, особливості формування наплавленого шару при високих швидкостях, було запропоновано спосіб відновлення на підвищених швидкостях, для реалізації якого запропоновано схема подачі електродного матеріалу.

За цим методом присадці надають обертання навколо своєї осі, притискають до поверхні наплавлюваної деталі, запалюють дугу, потім здійснюють подачу наплавочної головки уздовж осі деталі, яка наплавляється. Наплавлення проводять електродом, що не плавиться, в середовищі інертного газу (аргону), встановлюють електрод відносно присадочного матеріалу на відстані більшій або рівній відстані до деталі, як відновлюється; струмопровідну присадку попередньо вводять в контакт з деталлю (двостадійний процес), а подачу починають одночасно із збудженням дуги

Висновки. Аргонодугове наплавлення є ефективним методом нанесення покриттів і забезпечує можливість відновлення легованих деталей, до яких відноситься більшість валів та інших деталей. В роботі визначено основні напрямки підвищення продуктивності методу аргонодугового наплавлення та обрано найбільш ефективний, з точки зору автора, метод підвищення швидкості плавлення електрода – нахилом електроду та наданням йому обертального руху.

Список літератури

1. Машрабов, Н. Способы и средства повышения эффективности восстановления деталей сельскохозяйственной техники. [текст] / Н. Машрабов, Ю. Н. Ломоносов, В. П. Лялякин, Г. С. Игнатьев, А. К. Ольховацкий // Технологические рекомендации. – М. – Челябинск: – 2009. – 35 с.
2. Машрабов, Н. Контроль усталостного повреждения коленчатого вала [текст] / Н. Машрабов Н. // Сельский механизатор. – 2005.– № 9.– С. 7-8.
3. Машрабов, Н. Моделирование тепловых полей при механической обработке металлов численным методом [текст] / Н. Машрабов // Технология машиностроения. – 2008. – №9. – С. 19-21.
4. Машрабов, Н. Восстановление деталей сельскохозяйствен-ной техники высокоскоростной аргонодуговой наплавкой [текст] / Н. Машрабов, А. К. Ольховацкий // Труды Государственного научного учреждения «Всероссийский научно-исследовательский технологический институт ремонта и эксплуатации машинно-тракторного парка». (Труды ГОСНИТИ). – 2008. – Т. 102. – С. 93-96.
5. Машрабов, Н. Устройство для подачи вращающейся наплавочной проволоки [текст] / Н. Машрабов // Сварочное производство. – 2008. – №12. – С. 33-34.
6. Машрабов, Н. Высокоскоростная аргонодуговая наплавка изношенных цилиндрических деталей [текст] / Н. Машрабов,
7. Г. С. Игнатьев // Механизация и электрификация сельского хозяйства. – 2009. – №1. – С.32-33.
8. Машрабов, Н. Диагностирование усталостных повреждений коленчатого вала [текст] / Н. Машрабов // Тракторы и сельхозмаши-ны. – 2009. – №2. – С.40-42.
9. Машрабов, Н. Скоростная электродуговая наплавка цилиндрических деталей [текст] / Н. Машрабов // Международный научный журнал. – 2010. – №1. – С.43-46.

УДК 621.431.3

М. Яценко, магістр гр. АТ19МЗ
Центральноукраїнський національний технічний університет

ВІДНОВЛЕННЯ КОЛІНЧАСТИХ ВАЛІВ АВТОМОБІЛЬНИХ ДВИГУНІВ КОМБІНОВАНИМИ ТЕХНОЛОГІЯМИ

В роботі виконано аналіз стану проблеми відновлення шийок колінчастих валів автомобільних двигунів показав. Встановлено, що традиційні технології, які не забезпечують необхідних продуктивності отримання і якості покриттів. Для них характерні такі основні недоліки, які знижують експлуатаційні властивості покриттів: низькі адгезійна і когезійна міцність, твердість і зносостійкість, високі залишкові напруги, неоднорідна структура, наявність пір, раковин і тріщин, деформація валів і ін. Для усунення дефектів покриттів, отриманих за традиційними технологіями доцільно використовувати технологію, що дозволяє об'єднати в одному процесі дві технологічні операції - плазмового напилювання і електромеханічної обробки. Це дозволяє усунути недоліки, характерні при виконанні кожної операції окремо і забезпечує синергетичний ефект при їх об'єднанні.

колінчастий вал, напилювання, дефект, електромеханічна обробка

Постановка проблеми. Удосконалення ремонтного та машинобудівних виробництв неможливе без застосування нових прогресивних технологічних процесів, що дозволяють підвищити ресурс і надійність, забезпечити працездатність деталей та вузлів самих жорстких умовах експлуатації, при високих температурах та агресивних середовищах, дії динамічних і контактних навантажень. Цим викликано поширення застосування процесів зміцнюючих технологій у ведучих галузях машинобудування і широкі дослідження проведені за кордоном. Розробляються нові способи і технології нанесення покриттів, зокрема, багатошарові багатокомпонентні, отримують розвиток методи нанесення зносостійких покриттів, поверхневого легування і зміцнення, удосконалюються процеси поверхневого пластичного деформування тощо.

Найбільш характерними дефектами колінчастих валів автомобільних двигунів при ремонті є зношення корінних і шатунних шийок, обумовлене високими питомими поверхневими навантаженнями, а також тріщини втомленого характеру внаслідок знакозмінних і циклічних навантажень, що впливають на шийки. Відновлення колінчастого вала є складною проблемою, оскільки до якості і геометричних параметрів його робочих поверхонь висуваються високі вимоги.

Найбільш перспективним напрямком відновлення колінчастих валів автомобільних двигунів, є нанесення на зношені поверхні зміцнюючих покриттів.

Методи поверхневого зміцнення значно відрізняються один від одного фізико-хімічною природою зміцнюючої дії, галуззю застосування, технічними показниками та ефективністю. В силу тих чи інших причин сфера використання багатьох, без сумніву ефективних процесів зміцнення, істотно обмежується. В подібних випадках поєднання їх з іншим способом зміцнення (які знижують шорсткість, підвищують втомлену міцність, усувають пористість тощо) можливо досягти необхідного стану поверхневого шару і тим самим забезпечити високий рівень експлуатаційних властивостей, розширити технологічні можливості. Комбінованою обробкою можливо вирішити також завдання підвищення міцності зчеплення покриттів з основою, зміцнення основи перед нанесенням покриття, отримання мастильних канавок тощо. Різноманіття зміцнюючи ефектів і способів зміцнення визначає ширину можливостей по їх комбінуванню.

Комбіновані технології зміцнення (відновлення) є ефективними, однак вони трудомісткі, і їх доцільно використовувати лише для відповідальних деталей автомобілів зокрема, колінчастих валів, і у випадках, коли традиційні технології не забезпечують необхідних експлуатаційних властивостей.

Найбільш характерними дефектами колінчастих валів автомобільних двигунів при ремонті є зношення корінних і шатунних шийок, обумовлене високими питомими поверхневими навантаженнями, а також тріщини втомленого характеру внаслідок знакозмінних і циклічних навантажень, що впливають на шийки. Відновлення колінчастого вала є складною проблемою, оскільки до якості і геометричних параметрів його робочих поверхонь висуваються високі вимоги.

Серед відомих способів нанесення покриттів при відновленні шийок колінчастих валів до прогресивних відносять плазмового напилювання, так як воно відрізняється: можливістю використання найбільш широкої номенклатури матеріалів покриттів на різні матеріали, високою продуктивністю процесу, відносною простотою технології, незначним термічним впливом на основну деталь, можливістю повної автоматизації процесу. Проте, покриття, отримані таким способом, мають недостатню міцність зчеплення з основою при значних знакозмінних навантаженнях, структурну неоднорідність, високі залишкові напруження розтягу, що призводять до розтріскування покриття, що наноситься на шийки колінчастих валів. Для усунення цих недоліків застосовують зміцнення покриттів, як в процесі напилювання, так і після нього, за допомогою різних видів енергетичних впливів. Одним з таких способів є подальша електромеханічна обробка напилених покриттів, що дозволяє підвищити адгезійну і когезійну міцність, мікротвердість, створити стискаючі залишкові напруги для підвищення опору втоми і отримати більш однорідне покриття.

Однак, подальша після напилювання електромеханічна обробка має обмеження по максимальній товщині покриттів, при яких вони не руйнуються. Ця обставина призводить до підвищення трудомісткості нанесення і зміцнення покриттів товщиною, порівнянної з різницею між діаметром шийок нового колінчатого вала і їх останнім ремонтним розміром. У зв'язку з цим дослідження, виконані в даній магістерській роботі є актуальними.

Аналіз останніх досліджень та публікацій. Вибором ефективних методів відновлення деталей почали займатися з появою промислових видів ремонту. Значний внесок у вирішенні цих питань внесли провідні фахівці в галузі ремонту, такі як: Черновол М.І., Карагодин В.І., Латипов Р.А., Молодик Н.В., Новіков О.М., Серебровский В.І, Шадрічев В.А., Червоіванов В.І., Ульман І. Е. та інші. [1-5]

Мета і завдання досліджень. *Метою роботи* - є вдосконалення технології відновлення шийок колінчастих валів автомобільних двигунів комбінованою технологією, яка включає плазмове напилювання та електромеханічну обробку.

Для досягнення поставленої мети вирішувалися наступні задачі досліджень:

1. Проаналізувати дефекти колінчастих валів та причини виникнення дефектів колінчастих валів.
2. обґрунтувати доцільність і визначити напрямок дослідження щодо вдосконалення технології відновлення і зміцнення шийок колінчастих валів автомобільних двигунів новим комбінованим способом плазмового напилювання з одночасною електромеханічної обробкою;

Об'єкт дослідження - колінчасті вали двигунів автомобілів, що підлягають відновленню.

Предмет дослідження – технологія відновлення зношених колінчастих валів плазмово-порошковим наплавленням.

Методи досліджень базуються на експериментальних методах досліджень покриттів, отриманих за комбінованою технологією.

Серед нових технологічних процесів великий інтерес для процесу відновлення деталей автомобілів представляє способи нанесення металопокриттів з використанням плазмового струменя як джерела теплової енергії. Найбільш перспективним способом

відновлення деталей нанесенням зносостійких металопокриттів є плазмове напилювання з наступним оплавленням покриття. При цьому в металі оплавленого покриття частка основного металу мінімальна. Покриття має високу зносостійкість, без пор і тріщин. Процес є високопродуктивним. Недоліком цього способу є високі початкові капіталовкладення в устаткування. У нинішніх умовах при відсутності обігових коштів у підприємств цей недолік не дозволяє рекомендувати спосіб до широкого використання.

При плазмовому способі нанесення покриттів напилюваний матеріал розігрівається до рідкого стану і переноситься на оброблювану поверхню за допомогою потоку плазми з високою температурою. Напилюваний матеріал випускається у вигляді прутків, порошків або дроту. Порошковий спосіб найбільш поширений.

Унікальність методу плазмового напилювання полягає у високій температурі (до 50 тис. град. за Цельсієм) плазмового струменя і високій швидкості (до 500 м/с) руху частинок в струмені. Нагрівання самої поверхні, на яку наноситься покриття - невелике і складає не більше 200°С.

Продуктивність плазмового напилювання становить 3…20 кг/год для плазмотронів установок потужністю 30...40 кВт і 50…80 кг/год для обладнання потужністю 150...200 кВт.

Міцність зчеплення покриття з поверхнею деталі в середньому дорівнює 10…55 МПа на відривання, а деяких випадках - до 120 МПа. Пористість покриття знаходиться в межах 10...15%. Товщина покриття, як правило, не більше 1 мм, тому що при її збільшенні в напилюваному шарі виникають напруги, які прагнуть відокремити його від поверхні деталі.

Плазмово-дугове напилювання в поєднанні з одночасною обробкою поверхні обертової металевої щіткою дозволяє зменшити пористість покриття до 1…4%, а загальну товщину напилювання збільшити до 20 мм.

Плазмоутворюючими газами служать азот, гелій, аргон, водень, їх суміші та суміш повітря з метаном, пропаном або бутаном.

Для плазмового напилювання використовують дріт, в тому числі порошкового типу, порошки з чорних і кольорових металів, нікелю, молібдену, хрому, міді, оксиди металів, карбіди металів і їх композиції з нікелем і кобальтом, сплави металів, композиційні матеріали (нікель-графіт, нікель-алюміній і ін.) і механічні суміші металів, сплавів і карбідів. Регулювання режиму напилювання дозволяє наносити як тугоплавкі матеріали, так і легкоплавкі.

Основою для плазмового напилювання можуть служити метали і неметали (пластмаса, цегла, бетон, графіт і ін.). Для нанесення покриттів на невеликі поверхні застосовується мікроплазмовий спосіб напилювання, який дозволяє заощадити втрати напилюваного матеріалу (ширина напилювання 1-3 мм).

З метою підвищення адгезії напилених покриттів, захисту від окислення, зменшення пористості використовується метод плазмового напилювання в захисному середовищі (вакуум, азот, суміш азоту з аргоном і воднем) і з застосуванням спеціальних сопел, що закривають область між розпилювачем і оброблюваної поверхнею.

Процес плазмового напилювання включає 3 основних етапи:

1) підготовка поверхні.

2) напилювання і додаткова обробка покриття для поліпшення властивостей.

3) механічна обробка для досягнення чистових розмірів.

Попередні розміри поверхонь під напилювання повинні бути визначені з урахуванням товщини напилювання і припуску на подальшу механічну обробку. Переходи поверхонь повинні бути плавними, без гострих кутів, щоб уникнути відшаровування покриття.

Деталі перед напилюванням повинні бути ретельно очищені і знежирені. Ремонтні деталі, що мають замаслені пази або канали, слід нагріти в печі при температурі 200…340 °С протягом 2…3 годин для випарювання масла.

Далі проводиться активація поверхні - надання їй певної шорсткості для забезпечення адгезії. Активацію виконують за допомогою обдування деталі стисненим повітрям з абразивом або нарізуванням рваної різьби.

Абразив вибирають зернистістю 80...150 по ГОСТ3647, або застосовують чавунний/сталевий дріб ДЧК, ДСК №01...05 по ГОСТ 11964.

Металевий дріб не застосовується для обробки жаростійких, корозійностійких сталей і кольорових металів і сплавів, тому що може викликати їх окислення.

Шорсткість поверхні під плазмового напилювання повинна складати 10...60 Rz, поверхня повинна бути матовою.

Поверхні, що не підлягають абразивній обробці, захищають екранами. Зона обдування на 5 +/- 2 мм повинна бути більше, ніж номінальний розмір напилювань поверхні.

Тонкі деталі закріплюють у пристосуваннях з метою запобігання їх викривлення під час обробки.

Відстань від сопла до деталі при абразивно-струменевій обробці має перебувати в межах 80 ... 200 мм, менших значень набувають для більш твердих матеріалів, великі - для м'яких. Після цього з деталі видаляють пил шляхом обдування стисненим повітрям.

Проміжок часу між очищенням і напилюванням повинен складати не більше 4 год, а при покритті алюмінію та інших швидко окислюються матеріалів - не більше години.

Нарізування рваною різьбою замість абразивно-струменевої обробки застосовують для деталей з формою тіл обертання. Різьбу нарізають на токарному верстаті звичайним різьбовим різцем, зміщеним нижче осі деталі. Різьбу нарізають без охолодження за один прохід.

Для плазмового напилювання слід застосовувати порошки однієї фракції, форма частинок - сферична. Оптимальний розмір часток для металів складає близько 100 мкм, а для кераміки - 50 ... 70 мкм. У разі, якщо порошки зберігалися в негерметичній тарі, їх потрібно прожарити при температурі 120 ... 130 градусів протягом 1,5-2 год в сушильній шафі.

Ті частини деталі, що не піддаються напилюванню, захищають екранами з азбесту або металу, або обмазками.

Попередній підігрів деталі перед напилюванням здійснюють плазмотроном до температури 150...180 градусів.

Режими обробки визначають дослідним шляхом. Середні значення режимів плазмового напилювання наступні:

1) відстань від сопла до деталі - 100...150 мм.

2) швидкість струменя - 3...15 м/хв.

3) швидкість обертання деталі - 10...15 м/хв.

4) кут напилювання - 60...90 градусів.

Загальну товщину покриття набирають декількома циклами з перекриттям смуг напилювання на 1/3 діаметра плями напилювання.

Після напилювання деталь знімають з плазмотрона, видаляють захисні екрани і охолоджують до кімнатної температури.

Для поліпшення якості напилених покриттів застосовують такі прийоми:

1) обкатка роликами під електричним струмом;

2) напилювання з одночасною обробкою металевими щітками;

3) оплавлення покриттів з самофлюсуючих сплавів.

Оплавлення виконують за допомогою печей, СВЧ, нагрітих розплавів солей і металів, плазмовим, лазерним або газополуменевим способом. Температура оплавлення покриття нікель-хром-бор-кремній-вуглець становить 900..1200 градусів.

Чистові розміри деталей після плазмового напилювання отримують гострінням і шліфуванням з охолодженням водними розчинами і водно-олійними емульсіями. Шліфкруги вибирають з електрокорунду марки Е на керамічній зв'язці, зернистістю 36...46, твердістю СН. Режими шліфування наступні: швидкість обертання кола 25...30 м/с, подача кола 5...10 мм/об, швидкість обертання деталі 10...20 м/хв, подача деталі 0,015...0,03 мм/подв.х.

Далі проводять остаточний контроль, в разі, якщо на поверхні деталі з напилюванням є тріщини, відшарування, ризики, чорнота, що не витримані чистові розміри, то деталь

повертають на виправлення дефекту (не більше 1 разу), при цьому область напилювання повинна бути збільшена на 10...15 мм по периметру.

Висновки. Аналіз стану проблеми відновлення шийок колінчастих валів автомобільних двигунів показав, що в даний час використовуються традиційні технології, які не забезпечують необхідних продуктивності отримання і якості покриттів. Для них характерні такі основні недоліки, які знижують експлуатаційні властивості покриттів: низькі адгезійна і когезійна міцність, твердість і зносостійкість, високі залишкові напруги, неоднорідна структура, наявність пір, раковин і тріщин, деформація валів і ін. Ці недоліки пояснюються відсутністю або недосконалістю: нових ефективних способів та технологій відновлення і відповідного обладнання; обґрунтованих раціональних режимів і параметрів нанесення покриттів.

Доцільно для відновлення шийок колінчастих валів використовувати технологію, що дозволяє об'єднати в одному процесі дві технологічні операції - плазмового напилювання і електромеханічної обробки. Це дозволяє усунути недоліки, характерні при виконанні кожної операції окремо і забезпечує синергетичний ефект при їх об'єднанні.

Список літератури

1. Буравцев, С. К. О состоянии характеристик коленчатых валов и их влияния на показатели двигателей / С. К. Буравцев // Двигателестроение. - 2006. - № 1. - С. 38-42.
2. Ильиных, С. А. Восстановление коленчатых валов двигателей Камаз методом плазменного напыления / С. А. Ильиных, В. А. Крашанин, Е. В. Исаков, И. А. Попова // Технологии ремонта, восстановления, упрочнения и обновления машин, механизмов, оборудования и металлоконструкций: Материалы 6-й меж дунар. научно-практ. конференции. - СПб. - 2004. - С. 231.
3. Кадырметов, А. М. Перспективы упрочнения покрытий методом плазменного напыления с одновременной электромеханической обработкой [Текст] / А. М. Кадырметов, В. О. Никонов, В. Н. Бухтояров, Е. В. Снятков, А. Ф. Мальцев // Технологии упрочнения, нанесения покрытий и ремонта: теория и практика: В 2 частях : материалы 14-й международной научно-практической конференции. Часть 1 – СПб: Изд-во политехн. ун-та, 2012. – С. 75-79.
4. Багмутов, В. П. Исследование структуры и свойств наноматериалов, полученных комбинированной обработкой [Текст] / В. П. Багмутов, В. И. Калита, И. Н. Захаров, Иванников Е. Б., Захарова // Известия ВолГТУ. – Волгоград, 2008. – №10. – С. 102-106.
5. Кадырметов А. М. Исследование процессов плазменного нанесения и упрочнения покрытий и пути управления их качеством / А. М. Кадырметов // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета (Научный журнал КубГАУ) [Электронный ресурс]. – Краснодар: КубГАУ, 2012. –№07(81).
6. Кубич, В. И. Износостойкость деталей трибосопряжения «шейка- вкладыш» / В. И. Кубич, Л. И. Ивщенко // Проблемы трибологии. - 2011. - №2. - С. 103-110.
7. Захаров, С. М. Моделирование работы трибосистемы коленчатый вал- подшипники-опоры блока цилиндров двигателей внутреннего сгорания /С.М. Захаров, И. В. Сиротенко, И. А. Жаров // Трение и износ. - 1995. - Т. 16, № 1. - С. 47-54.

УДК 351.77

Є. Сімбаба, магістр гр. ФС-19М
Центральноукраїнський національний технічний університет

ОСНОВНІ НАПРЯМИ РЕФОРМУВАННЯ СФЕРИ ОХОРОНИ ЗДОРОВ'Я В УКРАЇНІ

Розглянуто положення нормативно-правових актів щодо пріоритетних напрямів державної діяльності з реформування системи охорони здоров'я в Україні. Висловлено точку зору автора щодо найбільш вагомих факторів, які впливають на ефективне функціонування цієї системи.

система охорони здоров'я, реформування, медичні кадри, державне управління системою охорони здоров'я

Постановка проблеми. З метою забезпечення сталого соціально-економічного розвитку будь-якої країни одним із пріоритетів державної політики має бути збереження і зміцнення здоров'я населення як найбільшої соціально-економічної цінності та одного із основних факторів національної безпеки держави. В Україні охорону здоров'я визначено одним з пріоритетних напрямів державної діяльності Основами законодавства України про охорону здоров'я (ст. 12) [4]. У цьому Законі, зокрема, зазначено, що держава формує та забезпечує реалізацію політики охорони здоров'я в Україні. Така політика полягає у формуванні вищими органами державної влади пріоритетів, доктрин, концепцій і програм, спрямованих на зміцнення здоров'я населення, забезпечення діяльності і розвиток системи охорони здоров'я.

Зміни та реформи у сфері охорони здоров'я на різних етапах суспільного розвитку мають здійснюватися органами управління державою усіх рівнів. Вони повинні містити поетапний комплексний характер і передбачати суспільно очікувані результати [2, с. 161]. Саме тому проблеми охорони здоров'я та діяльність, спрямована на збереження і зміцнення здоров'я, вимагають постійної уваги з боку держави і науковців у галузі державного управління.

Аналіз останніх досліджень і публікацій. Сучасний стан справ у медичній сфері, а також рекомендації щодо виходу з кризи вивчалися багатьма дослідниками, в числі яких Т. Бахтеєва, М. Білинська, Т. Грузєва, З. Гладун, Л. Жаліло, Д. Карамишев, О. Кучеренко, В. Москаленко, Я. Радиш, І. Солоненко, С. Стеценко та інші.

Формулювання цілей статті (постановка завдання). Основною метою публікації є аналіз пріоритетних напрямів державної діяльності щодо реформування системи охорони здоров'я в Україні та висловлення точки зору автора щодо основних факторів, що чинять вплив на ефективне функціонування цієї системи.

Виклад основного матеріалу дослідження. Важливими кроками на шляху запровадження системних реформ в системі охорони стало затвердження Національного плану розвитку системи охорони здоров'я на 2008-2010 рр., Концепції розвитку первинної медико-санітарної допомоги на засадах сімейної медицини, постанови Кабінету Міністрів України "Деякі питання удосконалення системи охорони здоров'я", прийняття законів України "Про внесення змін до Основ законодавства України про охорону здоров'я щодо удосконалення надання медичної допомоги"[1, с. 27]. У зазначених актах йде мова про такі основні напрями функціональної і структурної перебудови системи охорони здоров'я в Україні:

- удосконалення законодавчого забезпечення системи охорони здоров'я, що передбачає визначення базового пакета надання медичних послуг, з метою забезпечення гарантованої державою безоплатної медичної допомоги;
- збільшення ресурсного забезпечення шляхом розвитку багатоканального

фінансування системи охорони здоров’я, перерозподілу ресурсів між закладами охорони здоров'я, що надають первинну, вторинну (спеціалізовану), третинну (високоспеціалізовану) та екстрену медичну допомогу;

- планування та прогнозування розвитку мережі державних та комунальних закладів охорони здоров'я з урахуванням профілю, спеціалізації та інтенсивності надання медичної допомоги, нормативів медичного обслуговування населення за видами медичної допомоги;

- розширення послуг з охорони здоров’я через запровадження системи індикаторів якості первинної, вторинної (спеціалізованої), третинної (високоспеціалізованої), а також екстреної медичної допомоги;

- запровадження громадського контролю шляхом побудови зв’язку між державою, сферою охорони здоров’я і громадянським суспільством, забезпечення фахової громадської експертизи управління, галузевого законодавства тощо;

- підвищення якості кадрового забезпечення системи охорони здоров’я, шляхом запровадження системи прогнозування на довгострокову перспективу за категоріями медичного персоналу у відповідності до потреб охорони здоров’я;

- створення національної моделі охорони здоров’я, метою якої стане пошук найбільш оптимальної для України моделі охорони здоров’я, при якій діяльність та інфраструктура відповідатимуть потребам населення;

- розроблення компенсаторних механізмів з метою подальшого реформування системи охорони здоров’я у напрямі запровадження обов’язкового соціального медичного страхування [3].

Слід зазначити, що у переліку розроблених та рекомендованих законодавством напрямів реформування системи охорони здоров’я не передбачається створення чіткої моделі управління, особливо на регіональному та місцевому рівнях. Існуюча сьогодні модель обмежує можливості запровадження реформ через недосконаліть організаційно-правових механізмів.

Наявність суміжної компетенції місцевих державних адміністрацій та органів місцевого самоврядування породжує дублювання, а звідси і втручання одних органів у справи інших. Розмежування функцій і повноважень в управлінні охороною здоров’я між різними ланками державного управління на теперішній час постає важливою теоретичною та практичною проблемою [5, с. 68].

Головною метою реформи визначено побудову моделі охорони здоров’я, яка б забезпечувала рівний і справедливий доступ усіх членів суспільства до необхідних медичних послуг, високу якість та економічність цих послуг при збереженні соціально прийнятного обсягу державних гарантій. Для підвищення ефективності функціонування існуючої державної системи охорони здоров’я необхідно реалізувати такі кроки:

1) удосконалення законодавчого забезпечення системи охорони здоров’я, зокрема:

- формування чіткої структурно-функціональної моделі державного управління охороною суспільного здоров’я на основі нормативно-правового визначення функцій, повноважень і відповідальності органів виконавчої влади та місцевого самоврядування, розмежування повноважень органів місцевого самоврядування та місцевих органів державної виконавчої влади;

- визначення на законодавчому рівні базового пакета надання медичних послуг безоплатної медичної допомоги, гарантованого державою, що в подальшому стане базовим для запровадження медичного страхування;

2) посилення ресурсного забезпечення системи охорони здоров’я, у т. ч.:

- уведення механізму цільового використання акцизних зборів на шкідливі для здоров’я продукти (алкоголь, тютюнові вироби, напої з великим вмістом цукру тощо) на потреби охорони здоров’я;

- удосконалення процедури державного забезпечення населення України базовим пакетом лікарських препаратів і створення Державного реєстру цін на лікарські засоби. Для цього на державному рівні слід запровадити систему фіксування цін на низку найбільш

соціально важливих лікарських засобів з одночасним введенням державного замовлення на їх виробництво:

- упровадження системи моніторингу, яка б оцінювала ефективність державних видатків з погляду якісних наслідків для здоров'я суспільства, а не лише за даними статистики звернень до медичних закладів чи тривалості перебування на стаціонарному лікуванні;

- сприяння розвитку соціального партнерства між державою та представниками приватної медицини завдяки залученню їх до соціальних програм:

- побудови та фінансування хоспісів, фінансування протитуберкульозних програм тощо;

- організаційне забезпечення співпраці державного, відомчого та приватного секторів медичного обслуговування населення;

3) стимулювання розвитку добровільного медичного страхування, що потребує:

- забезпечення принципу багатоканальності фінансування системи охорони здоров'я, сприяння подальшому розвитку добровільного медичного страхування, лікарняних кас; ширшому використанню ресурсів приватних медичних закладів;

- стимулювання застосування системи офіційних спільних оплат населення у процесі медичного обслуговування. Має бути передбачено пільги з оподаткування (податок на доходи) для тих, хто користується приватними медичними послугами;

- відпрацювання системи підвищення якості медичної допомоги, цілеспрямованого та контрольованого використання коштів, сприяння подальшому розвитку лікарняних кас, залученню до них підприємств, установ, організацій незалежно від форм власності;

- запровадження механізмів фінансування страховими компаніями профілактичних заходів, спрямованих на зниження ризиків захворюваності, підвищення рівня здоров'я населення і тим самим скорочення кількості страхових випадків;

4) підвищення якості послуг з охорони здоров'я:

- забезпечення розроблення нових та оновлення чинних медичних стандартів і клінічних протоколів надання медичної допомоги на основі доказової медицини з паралельним забезпеченням процедури контролю МОЗ України, місцевими органами виконавчої влади, органами місцевого самоврядування та інститутами громадянського суспільства над реалізацією і дотриманням цих стандартів;

- запровадження системи диференційованої стимулюючої оплати праці в системі охорони здоров'я і системи укладання контрактів між надавачами медичних послуг (медичними закладами, приватно-практикуючими лікарями) та платником – державними органами управління з прив'язкою до якості та шкали складності надання медичної допомоги;

- створення програми безперервного підвищення якості надання послуг з охорони здоров'я (у т.ч. за рахунок дистанційного навчання, комп'ютеризації робочих місць лікарів тощо), які надаються на різних рівнях СОЗ, удосконалення системи позавідомчого (ліцензування, акредитація, атестація) та відомчого (незалежна експертиза) контролю якості;

- формування на основі узгоджених державної та регіональних програм відповідної мережі закладів первинної медико-санітарної допомоги, проведення реорганізації дільничних лікарень в амбулаторії загальної практики сімейної медицини з денним стаціонаром;

- розроблення та введення в дію мережі реабілітаційних закладів, спрямованих на відновлення активного способу життя і працездатності громадян;

- розвиток механізмів диспансеризації населення, започаткування механізмів економічного стимулювання та власної відповідальності кожного громадянина за стан свого здоров'я;

5) підвищення якості кадрового забезпечення системи охорони здоров'я:

- усунення диспропорції в кадровому забезпеченні охорони здоров'я, запровадження системи прогнозування на довгострокову перспективу за категоріями медичного персоналу

відповідно до потреб охорони здоров'я з урахуванням стратегії та темпів системних перетворень сфери, зовнішніх і внутрішніх міграційних процесів та природного вибуття кадрів;

- забезпечення випереджальними темпами підготовки та перепідготовки лікарів загальної практики сімейної медицини, сімейних медичних сестер, середнього медичного персоналу з вищою освітою;

6) продовження реалізації реформ у пілотних регіонах:

- завершення структурування медичної допомоги на первинний, вторинний і третинний рівні, закладення фінансування на первинну медичну допомогу в розмірі 25–30 % від загального бюджету сфери;

- розроблення порядку формування та затвердження планів-схем госпітальних округів;

- завершення формування територіальних центрів екстреної медичної допомоги з мережею станцій, підстанцій і пунктів тимчасового базування бригад.

Цілком погоджуємося з тим, що результатом такого реформування має стати створення національної моделі охорони здоров'я, діяльність та інфраструктура якої відповідатимуть потребам населення та враховуватимуть географічні, історичні й культурні особливості України. Під час розроблення та здійснення реформ обов'язково слід врахувати такі регіональні особливості як структура захворюваності, матеріальний стан лікувально-профілактичних закладів, наявність та характеристика спортивних, лікувально-оздоровчих, рекреаційних закладів, щільність населення, стан транспортно-логістичної сфери, кліматичні та природні умови, екологічне становище регіонів тощо. Обов'язковим є проведення роз'яснювальної роботи серед населення, представників політичної еліти, посадових осіб органів державної виконавчої влади та місцевого самоврядування, керівників установ і підприємств, медичної громадськості про зміст, переваги, наслідки та можливі ризики під час проведення реформ.

Результатом реформування має стати створення національної моделі охорони здоров'я, діяльність та інфраструктура якої відповідатимуть суспільним потребам та враховуватимуть географічні, історичні й культурні особливості України. Під час розроблення і здійснення реформ обов'язково мають враховуватися такі регіональні особливості, як структура захворюваності, матеріальний стан лікувально-профілактичних закладів, наявність та характеристики спортивних, лікувально-оздоровчих, рекреаційних закладів, щільність населення, стан транспортно-логістичної сфери, кліматичні і природні умови, екологічне становище в регіоні тощо.

Необхідним є проведення роз'яснювальної роботи серед населення, представників політичної еліти, посадових осіб органів державної виконавчої влади та місцевого самоврядування, керівників установ і підприємств, медичної громадськості про зміст, переваги, наслідки та можливі ризики під час проведення реформування сфери охорони здоров'я.

Висновки. Система охорони здоров'я – це сукупність організацій, інститутів і ресурсів, головною метою яких є поліпшення здоров'я. Для функціонування системи охорони здоров'я необхідні кадрові ресурси, фінансові кошти, інформація, обладнання та матеріали, транспорт, комунікації, а також загальне управління і керівництво. На нашу думку, ефективне функціонування системи охорони здоров'я визначається такими основними системоутворюючими факторами:

- вдосконалення організаційної системи (що дозволить в рамках державних гарантій забезпечити формування здорового способу життя та надання якісної безкоштовної медичної допомоги всім громадянам країни);

- розвиток інфраструктури та ресурсного забезпечення охорони здоров'я (що включає фінансове, матеріально-технічне та технологічне оснащення лікувально-профілактичних установ на основі інноваційних підходів та принципів стандартизації;

- наявність достатньої кількості підготовлених медичних кадрів (які зможуть

вирішувати поставлені перед охороною здоров'я завдання).

Перспективною темою для подальших досліджень у даному напрямі може стати вивчення питань, пов’язаних з пошуком національної моделі розвитку системи охорони здоров’я в Україні**.**

Список літератури

1. Державна політика у сфері охорони здоров’я : кол. моногр. : у 2 ч. / [кол. авт. ; упоряд.п.. Я. Ф. Радиш ; передм. та заг. ред. проф. М. М. Білинської, проф. Я. Ф. Радиша]. – К. : НАДУ, 2013. – Ч. 1. – 396 с.
2. Державне управління реформуванням системи охорони здоров’я в Україні навч.-наук. вид. / авт. кол. М. М. Білинська, Я. Ф. Радиш, І. В. Рожкова та ін. ; за заг. ред. М. М. Білинської. – К.; Львів: НАДУ, 2012 – 240 с.
3. Деякі питання удосконалення системи охорони здоров'я: Постанова Кабінету Міністрів України від 17 лютого 2010 р. N 208. – Режим доступу : zakon1.rada.gov.ua
4. Основи законодавства України про охорону здоров’я : Закон України від 19 листоп. 1992 року № 2801-XII // Відомості Верховної Ради України 1993, № 4. – С. 19.
5. Пак С. Я. Розвиток державної політики з функціональної та структурної перебудови системи охорони здоров’я на місцевому рівні в Україні / С.Я Пак // «Актуальні проблеми державного управління на сучасному етапі державотворення» : матеріали V наук.-практ. конф. 27 жовтня 2011 р.: тези допов. – Луцьк, 2011. – С. 68 – 70.

УДК 657

С. Волошин, магістр гр. ООУД 20М (1,4)
С. Акімов, магістр гр. ОО(П) 19М (1,9)
О. Коляса, магістр гр. ООУД 20МЗ
Центральноукраїнський національний технічний університет

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ФОРМУВАННЯ ЗВІТНОСТІ ПІДПРИЄМСТВ

У статті розглянуто інформаційне забезпечення 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, інформаційне забезпечення, система бухгалтерського обліку, процесний підхід, обліковий інформаційний ресурс, обліковий (бухгалтерський) продукт

Постановка проблеми та її актуальність. Система бухгалтерського обліку «відноситься до складних, має цілісну ієрархічну структуру з багатогранними зв’язками та складними функціями управління, що пов’язано з обміном зовнішніх і внутрішніх інформаційних потоків, багатоваріантністю видів інформації, яка циркулює в цій системі» [1, с. 145]. Подальший її розвиток пов’язаний із розвитком потреб користувачів облікової інформації. Зміни соціально-економічних умов функціонування підприємств обумовлюють необхідність зміни змісту бухгалтерської звітності [2, с. 44], виділення нових видів показників бухгалтерської звітності [13] обумовлюють необхідність удосконалення теоретико-методологічних аспектів функціонування облікової системи. Саме тому питання інформаційного забезпечення формування звітності є актуальними.

Аналіз останніх досліджень і публікацій. Питання формування звітності досліджували у своїх працях вітчизняні вчені: Ю. Верига, С. Голов, В. Жук, Г. Кірейцев, М. Коцупатрий, М. Корягін, В. Палій, М. Пушкар, В. Савчук, В. Сопко, Л. Сук, В. Швець, І. Яремко та ін. За цим напрямом працювали провідні зарубіжні дослідники:, М. Ф. Ван

Бреди, П. Ф. Друкер, В. Ф. Палій, Л. Петришин, Ф. Сафанова, Я. В. Соколов, Е. С. Хендріксен, Ч. Хоргрен та інші. Результати цих досліджень характеризуються глибиною теоретичних висновків, значущістю висвітлених питань і узагальнень та становлять значний вклад у розвиток системи обліку та звітності. Протее, потребують подальшого дослідження питання інформаційного забезпечення формування фінансової звітності.

Метою статті є дослідження інформаційного забезпечення формування фінансової звітності підприємств та розробка напрямів їх оптимізації.

Виклад основного матеріалу. В останні роки з метою 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 [7]. 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 [6, 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.

Савченко В. М. зазначає, що «сучасний етап розвитку економіки має високий рівень інтернаціоналізації, що зумовлює зміну суб'єкта облікової політики, а також зміну ідеології нормативної регламентації: від централізованої регламентації технології та процедур до централізованої регламентації принципів та децентралізованої регламентації облікової політики суб'єктів господарювання» [10, с. 30].

Проданчук М. А. 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 [9]. 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 [5, 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.

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.

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 [10, 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 [12, 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 [11, 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. Еболі, 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 [3]. 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 [11, 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 обліку та інтернет-ресурси; навчальні заклади, що здійснюють підготовку спеціалістів з бухгалтерського обліку; бухгалтерські служби юридичних осіб [4, 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.

Висновки та перспективи подальших досліджень. 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.

Інформація, що наведена у фінансовій звітності 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. Кононенко Л. В. Інноваційний розвиток системи бухгалтерського обліку як інформаційного забезпечення діяльності підприємства. Наукові праці Кіровоградського національного технічного університету. Економічні науки: зб. наук. пр. Кропивницький: ЦНТУ, 2018. Вип. 33. С. 144-152. URL: http://economics.kntu.kr.ua/archive/34.html (дата звернення: 12.05.2021).
2. Кононенко Л.В., Юрченко О.В. Социальная составляющая интегрированной отчетности. The VIII International Science Conference «Problems and tasks of modernity and approaches to their solution», March 02 – 05, 2021, Tokyo, Japan. Pp. 43 - 46 URL: https://books.google.com.ua/books?hl=en&lr=&id=4AAiEAAAQBAJ&oi=fnd&pg=PA43&dq=info:BTmBRmHADt0J:scholar.google.com&ots=3O4pZOBoi_&sig=3Z1U_URdOiu7sjAmiDls_8yMn4A&redir_esc=y#v=onepage&q&f=false (дата звернення: 11.05.2021).
3. Корягін М. В., Куцик П. О. Проблеми та перспективи розвитку бухгалтерської звітності [Текст] : монографія. Київ : Інтерсервіс, 2016. 276 с.
4. Кузнецова Л. Н. Совершенствование методики и методологии бухгалтерского учета на основе премии качества. Вестник Адыгейского государственного университета. Экономика. Майкоп : изд-во АГУ. 2010. Вып. 3(66). С. 73-82.
5. Левицька С. О. Обліковий інформаційний ресурс: теоретичний аспект. Зимові читання, присвячені видатним вченим в галузі бухгалтерського обліку, аналізу і контролю : збірник тез Одинадцятої Всеукраїнської наукової Internet- конференції ЖДТУ. 2013. С. 65-68.
6. Малюга Н. М. Бухгалтерський облік в Україні: теорія й методологія, перспективи розвитку : [монографія]. Житомир : ЖДТУ, 2005. 548 с.
7. Облікова політика: навч. посіб. / Г.М. Давидов та ін.; за заг. ред. Г.М. Давидова. 2-ге вид., перер. і доп. Кропивницький: ПП «Ексклюзив-Систем», 2017. 364 с
8. Поплаухина Т. Д. Качество учетно-аналитической информации как научная категорія. Актуальные вопросы экономики и управления : материалы междунар. науч. конф. (г. Москва, апрель 2011 г.). – Т. I. – М. : РИОР, 2011. – С. 202-205
9. Проданчук М. А. Продукт бухгалтерського обліку у системі прийняття управлінських рішень. Ефективна економіка. 2014. № 7. URL: http://www.economy.nayka.com.ua/?op=1&z=3203

10. Савченко В. М.Система бухгалтерського обліку як складова системи управління. Наукові праці Кіровоградського національного технічного університету. Економічні науки. 2010. Вип. 18 (2). С. 27-33. URL: http://nbuv.gov.ua/UJRN/Npkntu_e_2010_18%282%29__7 (дата звернення: 11.05.2021).
11. Соколов Я. В. История бухгалтерского учета : [учебник]. [2-е изд., перераб. и доп.]. М., 2006. 274 с.
12. Соколова Е. С. Методы оценки качества учетной информации. Экономические науки. 2009. № 5(54). С. 293-299.
13. Юрченко О.В. Звітність в системі управління соціальними витратами. Вісник Бердянського університету менеджменту і бізнесу. 2011. № 2(14). URL: http://dspace.kntu.kr.ua/jspui/bitstream/123456789/5848/1/zvitnist_v sistemi_upravlinnya_socialnimi_vitratami.pdf (дата звернення: 12.05.2021).

УДК 657

О. Хитрук, магістр гр. ООУД 19М (1,9)
Центральноукраїнський національний технічний університет, м. Кропивницький

УДОСКОНАЛЕННЯ ОБЛІКУ І КОНТРОЛЮ РОЗРАХУНКІВ ЗА ТОВАРНИМИ ОПЕРАЦІЯМИ

У статті розглянуто стан обліку і контролю розрахунків за товарними операціями. Окреслено основні проблеми цієї ділянки обліку і контролю. Запропоновані форма Реєстру документів до сплати, відомість обліку прострочених договорів, аналітична таблиця розрахунків з постачальниками та підрядниками, відомість обліку прострочених договорів, таблиця рішення про списання безнадійної дебіторської заборгованості. Розроблено напрями удосконалення контролю розрахунків за товарними операціями.

товарні операції, розрахунки, дебіторська заборгованість, кредиторська заборгованість, резерв сумнівних боргів, зобов'язання, договори

Постановка проблеми та її актуальність. Одним з найважливіших завдань ефективної роботи вітчизняних підприємств в сьогоднішніх українських економічних реаліях є забезпечення ефективного управління активами та зобов'язаннями підприємства. Особливе місце у складі майна та джерел його формування займають розрахунки підприємства з дебіторами та кредиторами за товарними операціями. Найбільша питома вага у загальній структурі дебіторської і кредиторської заборгованостей підприємства займають зобов'язання перед постачальниками і вимоги до покупців, які безпосередньо впливають на платоспроможність і фінансову стійкість суб'єктів господарювання. Проблеми вірогідності і своєчасності облікової, звітної й аналітичної інформації про розрахункові операції з партнерами за товарними операціями, що впливають на ефективність тактичного і стратегічного управління, стають особливо актуальними.

Несприятлива економічна та політична ситуації, інколи відсутність чітких методичних рекомендацій щодо обліку, низький професійний рівень топ-менеджменту сучасних підприємств призвели до напруження стану розрахунків на підприємствах, що виражається, перш за все, у збільшеннях сум заборгованості та зростанні строків непогашення боргів.

За цих умов особливу актуальність набувають проблеми теорії і методики бухгалтерського обліку та контролю розрахункових операцій, використання міжнародних принципів і стандартів обліку і звітності, оцінки стану й ефективності розрахунково-платіжних відносин підприємств, розробка науково обґрунтованих рекомендацій з подальшого поліпшення обліково-аналітичної роботи щодо розрахунків підприємства за товарними операціями.

Аналіз останніх досліджень і публікацій. Питання теорії та практики відображення розрахунків за товарними операціями в обліку розглядаються в працях вітчизняних та зарубіжних вчених-економістів та бухгалтерів, а саме: Г.М. Азаренкової, В.І. Бачинського,

І.А. Бланка, Ф.Ф. Бутинця, А.Г. Грязнової, С.Ф. Голова, Д.А. Єндовицького, М.В. Круглова, О.І. Лучкова, В.Ф. Палія, С.М. Петренко, А.М. Петрова, В.І. Прудникова, В.С. Рудницького, Я.В. Соколова, В.В. Сопка, Ю.Л. Фадєєва та інших.

Однак, незважаючи на наявність численних науково-методичних розробок, окремі проблеми дослідження сутності, складу та відображення в обліку розрахунків за товарними операціями залишаються не дослідженими та потребують подальшого наукового обґрунтування. Водночас через постійні зміни, що відбуваються у законодавстві України та в системі управління, постійно виникають проблемні питання, організації та методики обліку та контролю розрахунків за товарними операціями на підприємствах, які потребують подальшого розгляду і опрацювання.

З огляду на це потребує подальшого дослідження проблематика обліку та контролю розрахунків за товарними операціями.

Метою статті є вивчення організаційних та методичних аспектів обліку і контролю розрахунків за товарними операціями та розробка напрямків щодо їх удосконалення.

Виклад основного матеріалу. Стан розрахунків за товарними операціями на вітчизняних підприємствах є напруженим, що виявляється у значних сумах заборгованості та тривалих термінах її погашення. Крім того, спостерігається їх зростання [4, с. 105].

Не дивлячись на те, що облік розрахунків за товарними операціями в Україні регулюється численними нормативними документами, в обліку залишаються невирішеними актуальні проблеми [6], що представлено на рисунку 1.

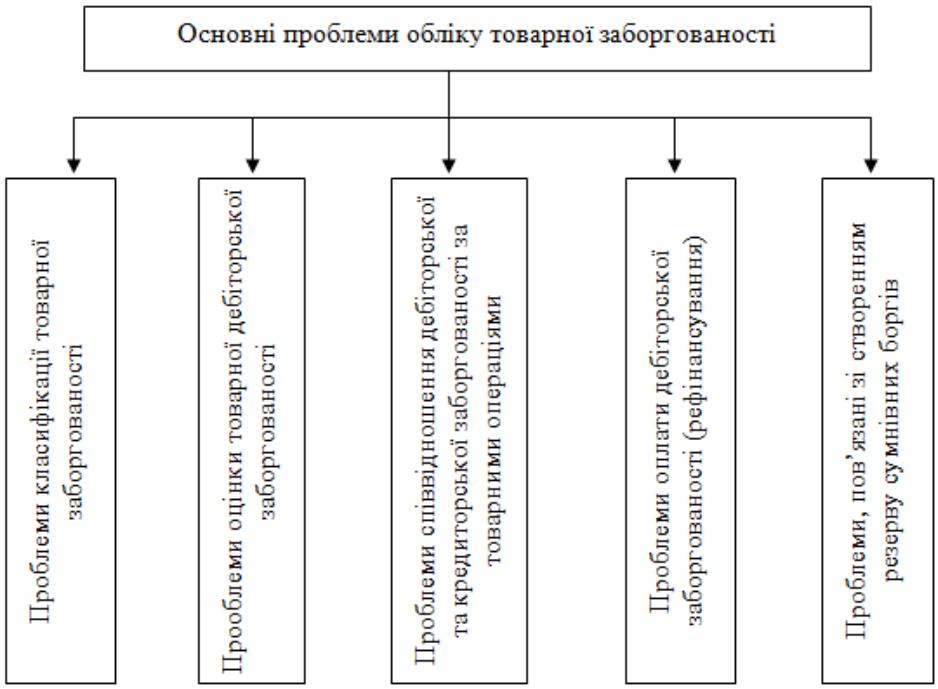


Рисунок 1 – Проблеми обліку розрахунків за товарними операціями

Стосовно такого важливого аспекту товарної дебіторської заборгованості, як її оцінка, то основним проблемним моментом є методика розрахунку резерву сумнівних боргів. На рисунку 2 наведено методи визначення резерву сумнівних боргів та їх характеристика відповідно до П(С)БО 10 «Дебіторська заборгованість» [7], яким передбачено, що «поточна дебіторська заборгованість за товарними операціями відображається в балансі за чистою реалізаційною вартістю, тобто за вирахуванням резерву сумнівних боргів».

Національною методологією обліку передбачається визначення резерву сумнівних боргів із застосуванням абсолютної суми сумнівної заборгованості або коефіцієнта сумнівності.

В табл. 1 відображено порівняльний аналіз існуючих методів визначення резерву сумнівних боргів. При застосуванні абсолютної суми сумнівної заборгованості нівелюється принцип обачності в обліку, оскільки формування резерву сумнівних боргів та нарахування доходу від реалізації здійснюється у різних звітних періодах, що спричинює завищене відображення суми дебіторської заборгованості на дату балансу.

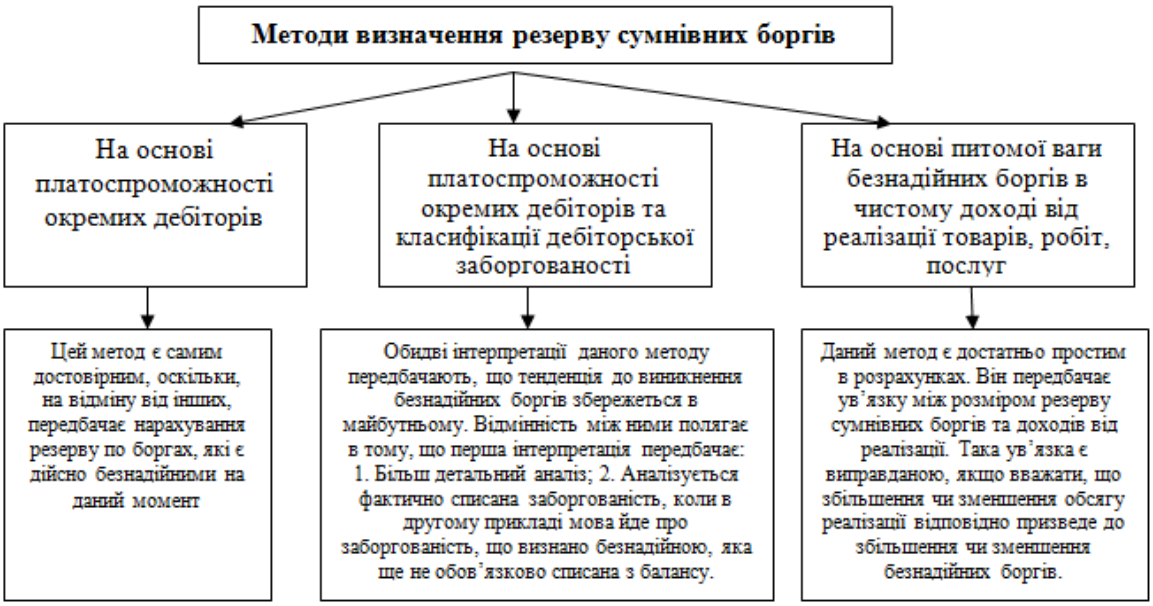


Рисунок 2 – Методи розрахунку резерву сумнівних боргів, передбачені П(С)БО 10 «Дебіторська заборгованість»

Другий метод (застосування коефіцієнта сумнівності) містить в собі три способи розрахунку коефіцієнта сумнівності, що мають переваги та недоліки у застосуванні (табл. 1). Так, наприклад, при застосуванні способу класифікації дебіторської заборгованості за строками непогашення, П(С)БО 10 не передбачено розподіл дебіторської заборгованості за видами в залежності від періоду непогашення для розрахунку резерву сумнівних боргів.

Крім того, при класифікації дебіторської заборгованості необхідно застосовувати інтервальні показники (наприклад, строк непогашення від 1 до 6 міс.). Також, на підприємстві може виникнути ситуація наявності великої кількості дебіторів з різними строками непогашення, що робить застосування даного методу практично неможливим через високу трудомісткість процесу. У способу розрахунку коефіцієнта сумнівних боргів виходячи з питомої ваги безнадійних боргів у чистому доході існує невідповідність між показниками, на підставі яких він розраховується.

При використанні даного способу необхідно використовувати не чистий дохід, а дохід (виручку) від реалізації продукції (товарів, робіт, послуг) за вирахуванням наданих знижок та повернення проданих товарів, що пояснюється наступним чином: чистий дохід не містить ПДВ та інших непрямих податків, а до складу безнадійної заборгованості входить ПДВ.

Недостатньо розкритим на сьогодні залишається питання стосовно невикористаних сум резервів сумнівних боргів на кінець звітного періоду. Слушною є думка деяких науковців, що у такому разі підприємство має право не списувати сформований резерв, а використовувати його у наступному звітному періоді до закінчення терміну позовної давності або до погашення боргу. Інструкцією про застосування Плану рахунків передбачено зменшення нарахованих резервів у кореспонденції з рахунком обліку доходів. Виходячи із зазначеного, правомірною та вірною буде операція списання суми резерву сумнівних боргів в кінці періоду на рахунок 719 «Інший операційний дохід».

Таблиця 1 – Порівняльна характеристика методів визначення резерву сумнівних боргів

№ з/п	Порядок розрахунку	Переваги	Недоліки
1	2	3	4
1. Метод застосування абсолютної суми сумнівної заборгованості			
	Визначається на підставі аналізу платоспроможності окремих дебіторів	Одержання найбільш точної чистої реалізаційної вартості дебіторської заборгованості Надає можливість здійснювати аналіз по кожному дебітору	Трудомісткий, оскільки потребує детального вивчення платоспроможності всіх дебіторів і визначення тих з них, які не погасять своєчасно заборгованість. Труднощі в отриманні реальної інформації про стан платоспроможності дебіторів. Ступінь точності результату має суб'єктивний характер, так як залежить від наявності достовірної інформації про дебіторів та кваліфікації експертів, що надають інформацію про них. Можливо застосовувати лише за незначної кількості дебіторів, з якими ведуться постійні розрахунки
2. Метод застосування коефіцієнта сумнівності			
	Визначається шляхом множення суми залишку дебіторської заборгованості на початок періоду на коефіцієнт сумнівності (Кс), який розраховується шляхом:		
	Визначення питомої ваги безнадійних боргів у чистому доході	Дотримання принципу обачності. Порівняна простота розрахунку. Можливість застосу-вання лише за наявності тісного взаємозв'язку між обсягом реалізації та сумою безнадійних боргів за попередні роки	Недотримання принципу відповідності доходів і витрат (так як періоди, у яких була здійснена реалізація та відображені безнадійні борги є різними)
	Класифікації дебіторської заборгованості за строками непогашення	Ґрунтується на інфор-мації, що є в наявності у бухгалтера. Можливість застосування підпри-ємствами з великою кількістю дебіторів	Труднощі пов'язані з неможливістю розподілу дебіторів у зв'язку з встановленням для кожного з них різних термінів погашення. Розрахунок є трудомістким процесом та досить складною процедурою для виконання. Відсутнє нормативне регулювання кількості попередніх періодів, що

			потрібно враховувати для розрахунку. Коефіцієнт сумнівності за заборгованостями дебіторів колишніх періодів застосовується для оцінки теперішніх дебіторів, що є не цілком коректним Відсутня можливість оперативного контролю за переміщенням «сумнівних» дебіторів з однієї групи сформованої за строками непогашення в іншу
	Визначення середньої питомої ваги списаної протягом періоду ДЗ у сумі ДЗ на поч. відпов. періоду за попередні 3-5 р.	Ґрунтується на інформації, що є в наявності у бухгалтера. Дотримання узгодже-ності доходів та витрат	Трудомісткий з відносною складністю розрахунків через використання великого обсягу інформації (за останні 3-5 років). Визначення теперішнього резерву сумнівних боргів на основі минулого досвіду

Також науковці пропонують відносити залишок невикористаної суми нарахованого резерву на кредит рахунка 716 «Відшкодування раніше списаних активів». Проте, операцію створення резерву сумнівних боргів неправомірно прирівнювати до списання заборгованості, адже резерв сумнівних боргів створюється на заборгованість стосовно якої лише існують сумніви в погашенні, а не впевненість в непогашенні.

Безнадійна дебіторська заборгованість повинна бути списана і відображена на позабалансовому рахунку 071 «Списана дебіторська заборгованість» з метою подальшого контролю та у разі можливості її стягнення у зв'язку з виникненням нових обставин операції на пр отязі певного періоду. Даний період має лише нижню межу − 3 роки, тобто, як зазначають деякі практики з обліку, підприємство має можливість визначати самостійно термін перебування списаної заборгованості на позабалансовому обліку. Однак, оптимальним строком є 4 роки з дати списання дебіторської заборгованості з балансу, оскільки ЦКУ (ст. 259) передбачена можливість збільшення строку позовної давності за домовленістю сторін за умови укладення договору у письмовій формі.

У структурі зобов'язань підприємства розрахунки з постачальниками (кредиторська заборгованість за товари, роботи, послуги) займають значну питому вагу. При цьому одним із важливих елементів організації обліку кредиторської заборгованості за товари, роботи, послуги є відокремлення обліку за функціональними ділянками (фінансовий, управлінський, податковий) та забезпечення належного внутрішнього контролю. І хоча більшість з цих елементів не впливає безпосередньо на величину показників фінансової звітності, вони, на нашу думку, повинні знайти відображення при формуванні облікової політики на досліджуваному підприємстві щодо кредиторської заборгованості за товари, роботи, послуги з метою прийняття управлінських рішень.

З метою ефективної договірної політики порядок проходження документації, пов'язаної з укладанням і виконанням господарського договору з постачальниками пропонуємо врегульовувати Положенням про договірну політику, основна мета якого полягає в досягненні різних економічних вигод як в частині бухгалтерського обліку, так і оподаткування операцій, які підлягають договірному врегулювання.

Організацію договірної роботи можна розбити на такі етапи: вивчення існуючого порядку укладання договорів; ознайомлення і систематизація існуючих видів договорів

залежно від предмета останніх, типу контрагента та інших критеріїв; розробка нової схеми документообігу з врахуванням обов'язків працівників договірного відділу і відповідальних посадових осіб з визначенням компетенції бухгалтерії, фінансового відділу, юридичної служби; розробка посадових інструкцій відповідальних за укладання договорів; розробка і утвердження типових договорів; впровадження системи автоматизації договірної роботи.

Відповідно до затвердженого на підприємстві Положення про договірну політику пропонуємо провести наступні заходи: видати наказ, в якому довести до відома всіх працівників, що договір складається тільки тоді, коли надходить відповідне завдання від виконавця; якщо ж дане завдання не надійшла, відповідальність за це несе виконавець (наприклад, без укладання договору відділ постачання придбав матеріали або відділ маркетингу розмістив рекламу в журналі, в таких ситуаціях відповідальність несуть виконавці); затвердити стандартну форму подачі такого завдання (у формі окремого документа або у формі журналу (реєстру)).

В господарській діяльності підприємств виникають обставини, які впливають на своєчасне виконання зобов'язань або взагалі припиняють їх здійснення. Такими обставинами можуть бути тимчасова або стійка фінансова неплатоспроможність, надзвичайні події. Це означає, що при здійсненні операцій із розрахунків з постачальниками та підрядниками у бухгалтерському обліку може виникати як дебіторська заборгованість – у випадку здійснення передоплати, так і кредиторська заборгованість – за умови такої оплати або іншого погашення зобов'язань.

З метою вдосконалення обліку розрахунків з постачальниками за товарними операціями пропонуємо документ під назвою «Реєстр документів до сплати» (табл. 2).

Таблиця 2 – Запропонована форма Реєстру документів до сплати

№ з/п	Постачальник	Номер рахунку до сплати, дата	Термін оплати, дні	Сума оплати з ПДВ, грн.	Сальдо з рахунком на кінець дня	Сальдо за рахунком накопичувально за місяць	Дата оплати
	Назва ТМЦ	Сума рахунку з ПДВ, грн.					
1							
…							
Всього							

Наведений вище документ сприятиме зростанню ефективності облікової роботи на підприємстві. Він містить перелік рахунків за кожним постачальником та інформацію про те, за що платить підприємство, якими повинні бути строки оплати. Найголовнішою перевагою даного документа є те, що в ньому наводяться залишки за кожним рахунком на кінець дня, а також присутня накопичувальна інформація на кінець місяця. Цей документ дозволить контролювати кредиторську заборгованість за конкретним рахунком від постачальника.

Для запобігання факту виникнення простроченої кредиторської заборгованості та раціоналізації контролю над своєчасним погашенням заборгованості перед постачальниками та підрядниками рекомендуємо використовувати форму Аналітичної таблиці розрахунків із постачальниками та підрядниками, що представлена в табл. 3.

Таблиця 3 – Запропонована Аналітична таблиця розрахунків з постачальниками та підрядниками

№ з/п	Постачальник	Номер рахунку до сплати, дата	Термін оплати,дні	Відстрочена заборгованість, термін, дні				Прострочена заборгованість, термін рік, квартал (місяць), дні												Сума оплати з ПДВ, грн.	Сальдо по рахунку на кінець дня	Сальдо по рахунку накопичувально за	Дата оплати
				20_ рік				20_ рік				20_ рік				20_ рік							
	Назва ТМЦ	Сума рахунку з ПДВ, грн.			I	II	V		I	II	V		I	II	V		I	II	V				
1	2	3		5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20				
…																							
Всього		x																					

Господарські зв’язки підприємств оформляються й закріплюються договірними відносинами у випадках, коли одне підприємство є постачальником матеріальних цінностей або послуг, а інше – їх покупцем, споживачем, а отже, і платником. При цьому є доцільним вести облік прострочених договорів за допомогою спеціальної відомості (табл. 4).

Таблиця 4 – Запропонована Відомість обліку прострочених договорів

№ договору	Назва підприємства	Дата підписання договору	Термін дії договору, міс.	Дата закінчення терміну дії договору	Термін прострочення, міс.

Відомість обліку прострочених договорів, куди вносяться дані договорів, у яких закінчився строк дії, повинна щоденно завірятися підписом начальника відділу постачання та головного бухгалтера. Це дасть змогу систематизувати роботу з договорами, що, врешті сприятиме упорядкуванню роботи з дебіторами на підприємстві.

Також доцільним є ведення на підприємстві додаткової Відомісті-реєстру покупців. Необхідність ведення додаткової відомості-реєстру зумовлена тим, що у регістрах синтетичного обліку у стовпчику «Найменування покупця (замовника)» передбачено місце лише для скороченого найменування контрагента, що може призвести до помилок та непорозумінь з боку бухгалтера (табл. 5).

Таблиця 5 – Відомість-реєстр покупців (замовників) за _____місяць _____року

№ з/п	Найменування покупця	Юридична адреса	ПІБ керівника, конт.телеф.	ПІБ головного бухгалтера, конт.телеф.	Банківські реквізити
1	2	3	4	5	6

При веденні обліку дебіторської заборгованості надзвичайно важливою операцією, що потребує достовірного документального оформлення є списання безнадійної дебіторської заборгованості. Списання безнадійної дебіторської заборгованості здійснюється за рішенням керівника підприємства, проте, визначена форма рішення не передбачена жодним законодавчим актом. В табл. 6 подано форму рішення керівника про списання безнадійної дебіторської заборгованості.

Таблиця 6 – Рішення про списання безнадійної дебіторської заборгованості

№ з/п	Найменування дебітора	Сума, грн.	Дата винекнення	Причина винекнення	Дата списання	Підстава для списання	За рахунок (резерву сумнівних боргів, інших операційних витрат)
1	2	3	4	5	6	7	8

Вищезазначена форма є корисною для бухгалтерського та податкового обліку підприємства, так як враховує їх вимоги, є джерелом достовірної інформації та достатньою підставою для списання безнадійної дебіторської заборгованості з балансу.

В умовах ринку господарюючі суб’єкти вступають в договірні відносини щодо використання майна, грошових коштів, здійснення комерційних операцій та інвестицій. Раціональна організація контролю за станом розрахунків за товарними операціями сприяє зміцненню договірної і розрахункової дисципліни, виконанню зобов'язань з постачання продукції в заданому асортименті і якості, підвищенню відповідальності за дотримання платіжної дисципліни, скороченню дебіторської і кредиторської заборгованості, прискоренню оборотності оборотних коштів, поліпшенню фінансового стану підприємства, а також дозволить приймати скоординовані й ефективні управлінські рішення.

З погляду системного підходу на кожному підприємстві відбувається постійний кругообіг інформаційних потоків. Управління будь-якою системою здійснюється на основі інформації, що циркулює в системі, яка надходить на її «вході» і та, яка виходить з неї (рис. 3).

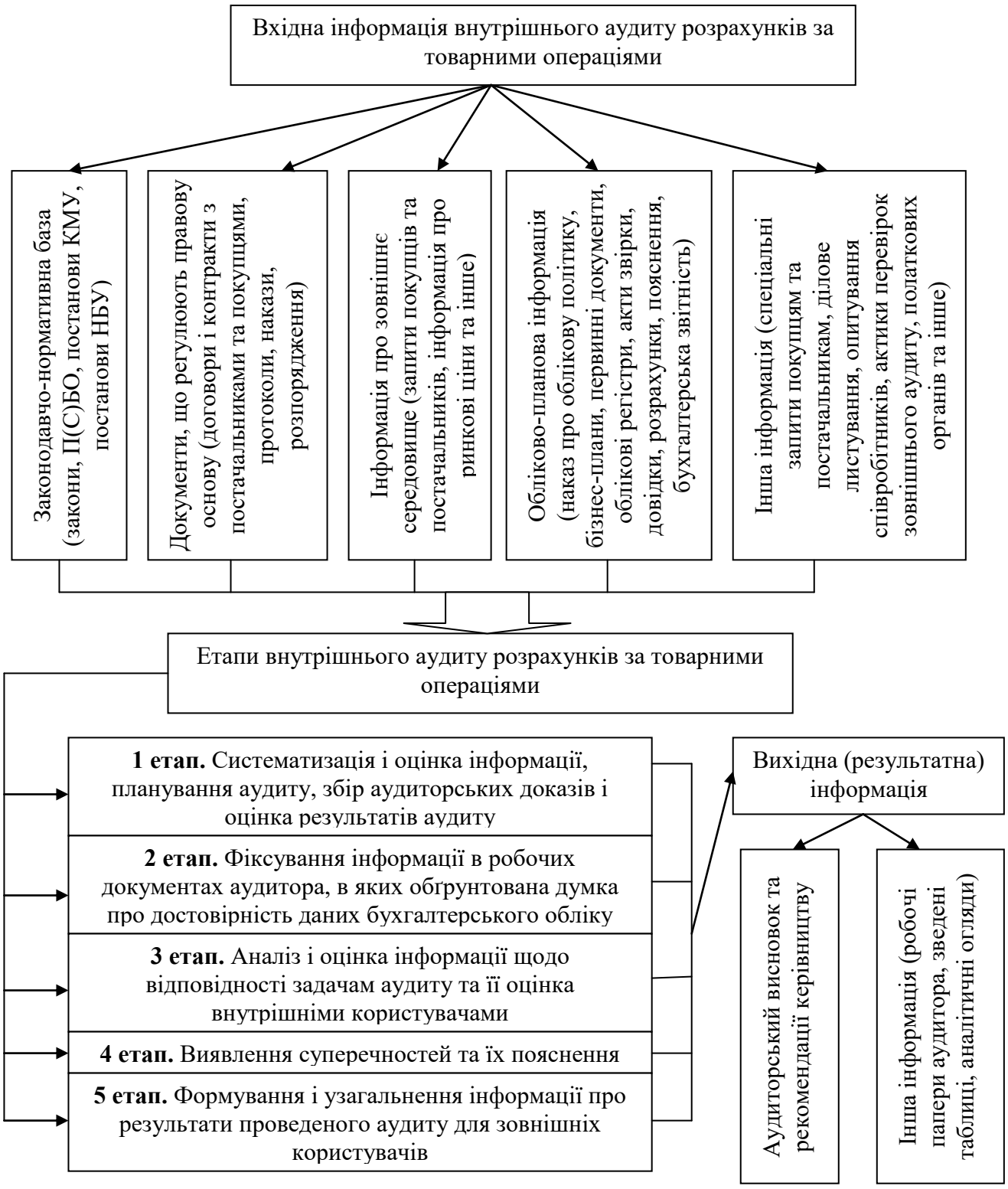


Рисунок 3 – Процес систематизації інформаційних ресурсів на підприємстві при аудиті розрахунків за товарними операціями

Об'єктом аудиту розрахунків виступають первинні і зведені документи бухгалтерського обліку, фінансової звітності й інші матеріали, які містять явища і дії, що мають відношення до виконання завдання.

Такий підхід дозволяє розглядати об'єкт аудиту в двох проекціях: з урахуванням його форми і виходячи з економічного змісту. Форма відображає зовнішні ознаки об'єкта, а зміст - його внутрішні властивості.

Дослідження об'єкта аудиту розрахунків за товарними операціями повинно йти від форми до змісту, що дозволяє аудитору встановити зв'язки і розходження з іншими об'єктами і прийти до відповідного висновку. Результатом структурно-системного підходу до вивчення властивостей і ознак об'єктів аудиторської перевірки стала побудова їхньої класифікації. На нашу думку, виходячи зі ступеня значущості інформації, що міститься в об'єктах, вони можуть бути структуровані як основні, допоміжні і додаткові.

На нашу думку, найбільш ефективним є застосування методів документальної і фактичної перевірки, у числі яких можна виділити прийоми дослідження окремого облікового документа, а також групи документів, що відображають одну чи кілька взаємозалежних операцій або рух однорідного майна, контрольну перевірку поточних розрахунків і зобов'язань, одержання письмових довідок фахівців, тестування осіб, що мають пряме чи непряме відношення до досліджуваного факту господарської діяльності.

В основу аудиту розрахунків за товарними операціями повинні бути покладені дані про стан заборгованості на відповідну календарну дату по рахунках 63 «Розрахунки з постачальниками і підрядчиками», 36 «Розрахунки з покупцями і замовниками», 37 «Розрахунки з різними дебіторами» субрахунок «Розрахунки по авансах виданим», субрахунок «Розрахунки по претензіях», 68 «Розрахунки з різними кредиторами» субрахунок «Розрахунки по авансах отриманим» і іншим рахунках обліку.

Оскільки весь спектр розрахункових операцій з контрагентами так чи інакше сполучений з умовами договору, нам представляється, що господарський договір варто розглядати як безпосередній об'єкт аудиту (табл. 7).

Таблиця 7 – Основні напрямки аудиту господарських договорів

Напрямки аудита	Експертні задачі
1	2
Правовий	Перевірка відповідності договору вимогам діючого законодавства і звичаям ділового обороту
Бухгалтерський	Дослідження бухгалтерського супроводу договору (документообігу, кореспонденції рахунків, облікової оцінки об'єктів, відображення стану майна і зобов'язань у бухгалтерській звітності)
Податковий	Оцінка податкових наслідків реалізації договору (об'єкти оподаткування, податкові ставки, можливість використання податкових пільг)
Економічний	Аналіз економічних вигод, що отримуються, ризиків за договором, цінової політики, схем і форм розрахунків
Технологічний	Оцінка технічних параметрів відчужуваних або тих що складаються

З метою підвищення контролю за порядком складання та виконання договорів, керівникам підприємств рекомендовано видавати розпорядження щодо обов’язкового узгодження змісту договору з головним бухгалтером та надання одного примірника договору до бухгалтерії, що дозволить проконтролювати законність господарської операції і застерегти підприємство від штрафних санкцій.

Висновки та перспективи подальших досліджень. В обліку розрахунків за товарними операціями у сучасних умовах господарювання існує чимало проблемних моментів. Стосовно такого важливого аспекту товарної дебіторської заборгованості, як її оцінка, то основним проблемним моментом є методика розрахунку резерву сумнівних боргів.

З метою вдосконалення обліку розрахунків за товарними операціями ми пропонуємо ввести додаткові реєстри та аналітичні таблиці щодо контролю термінів розрахунків та запобіганню фактів виникнення простроченої заборгованості.

Список літератури

1. Аудит розрахунків з постачальниками і підрядниками. Бібліотека економіста. URL: http://library.if.ua/book/78/5603.html. (дата звернення: 12.05.2021).
2. Бондаренко О. М. Облік розрахунків з постачальниками і підрядниками. Економіка. Фінанси. Право. 2018. № 4. - С. 26-29. URL: http://nbuv.gov.ua/UJRN/ecfipr_2018_4_8 (дата звернення: 13.05.2021).
3. Бурак І. О. Облікова політика як складова організації обліку заборгованості за розрахунками. Науковий вісник Мукачівського державного університету. Сер. : Економіка. 2015. Вип. 2(1). С. 214-217.
4. Кононенко, Л. В., Сисоліна, Н. П., & Юрченко, О. В. (2021). Управління дебіторською заборгованістю: сучасний стан, проблеми, перспективи, інформаційне забезпечення. Економічний простір, (166), 104-109. https://doi.org/10.32782/2224-6282/166-18
5. Облікова політика: навч. посіб. / Г.М. Давидов та ін.; за заг. ред. Г.М. Давидова. 2-ге вид., перер. і доп. Кропивницький: ПП «Ексклюзив-Систем», 2017. 364 с
6. Пальчук О.В. Розвиток бухгалтерського обліку в умовах глобалізації та інформатизації суспільства: монографія / О.В. Пальчук, В.М. Савченко, І.В. Рузмайкіна та ін; за ред. Г.М. Давидова. Кропивницький: ПП «Ексклюзив-Систем», 2017. 248 с. URL: http://dspace.kntu.kr.ua/jspui/handle/123456789/7356 (дата звернення: 23.05.2021).
7. Положення (стандарт) бухгалтерського обліку 10 «Дебіторська заборгованість», затверджено наказом Міністерства фінансів України № 273 від 08. 10.1999 р. URL: http://zakon.rada.gov.ua. (дата звернення: 13.05.2021).
8. Потапова Н. О. Проблемні аспекти обліку розрахунків з покупцями та замовниками // Економіка. Фінанси. Право. - 2017. - № 10(1). - С. 46-47. URL: http://nbuv.gov.ua/UJRN/ecfipr_2017_10(1)__14 (дата звернення: 21.05.2021).
9. Савченко В. М. Система бухгалтерського обліку як складова системи управління. Наукові праці Кіровоградського національного технічного університету. Економічні науки. 2010. Вип. 18 (2). С. 27-33. URL: http://nbuv.gov.ua/UJRN/Npkntu_e_2010_18%282%29__7 (дата звернення: 22.05.2021).
10. Соболєва-Терещенко О. А. Особливості бухгалтерського обліку розрахунків з покупцями в умовах застосування программ лояльності // Науковий вісник Ужгородського університету. Серія: Економіка. - 2017. - Вип. 2. - С. 325-332. URL: http://nbuv.gov.ua/UJRN/ Nvuuec_2017_ 2_49 (дата звернення: 12.05.2021).
11. Спіцина Н.В. Обліково-аналітичне забезпечення системи управління розрахунками за товарними операціями: монографія / Н.В. Спіцина, Т.В. Момот, Н.С. Акімова. – Х.: Видавництво Іванченка І. С., 2019. – 281 с.

ЗМІСТ