МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЦЕНТРАЛЬНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
НАУКОВА АСОЦІАЦІЯ КІБЕРБЕЗПЕКИ УКРАЇНИ

УДК 004.4

Тези доповідей

**VII Міжнародної науково-практичної конференції
до 30-ти річчя кафедри кібербезпеки та програмного забезпечення**

"Інформаційна безпека та комп’ютерні технології"

1 листопада 2023 року

Кропивницький 2023

УДК 004.4

Матеріали VII Міжнародної науково-практичної конференції "Інформаційна безпека та комп'ютерні технології" до 30-ти річчя кафедри кібербезпеки та програмного забезпечення: тези доповідей, 1 листопада 2023 р. – Кропивницький: ЦНТУ, 2023. – 135 с.

Наведені тези пленарних та секційних доповідей за теоретичними та практичними результатами наукових досліджень і розробок. Представлені результати теоретичних досліджень в галузях проектування інформаційних систем, технологій захисту інформації, використання сучасних інформаційних технологій в управлінні системами за різними галузями народного господарства.

Матеріали публікуються в авторській редакції.

За достовірність викладених фактів, цитат та інших відомостей відповідальність несуть автори.

СЕКЦІЯ 1. ІНФОРМАЦІЙНА БЕЗПЕКА ДЕРЖАВИ, СУСПІЛЬСТВА ТА ОСОБИСТОСТІ

УДК 004.056

Д.С. Білик[1], Ю.П.Кльоц[1], Н.С.Петляк[1]
bilykds@khmnu.edu.ua, klots@khmnu.edu.ua, npetlyak@khmnu.edu.ua
[1]Хмельницький національний університет, м. Хмельницький

МЕТОД ВИЯВЛЕННЯ БОТІВ В ПУБЛІЧНІЙ МЕРЕЖІ НА ОСНОВІ МУЛЬТИАГЕНТНОГО ПІДХОДУ

Ботнет – це мережа, що складається з скомпрометованих хостів, керованих деяким шкідливим програмним забезпеченням (бот). Бот є частково автономною частиною шкідливого програмного забезпечення, яке контролюється віддалено.

Традиційні антивірусні інструменти засновані на пошуку сигнатур, таким чином вимагають об'ємної, точної бази сигнатур, яка має регулярно оновлюватися [1]. Ботнети можуть легко уникнути сигнатурного виявлення, оновлюючи себе частіше, ніж користувачі оновлюють антивірусні бази. Деякі боти можуть відключити антивірусні засоби системи або використовувати руткіт-технології, щоб захистити себе від виявлення на локальному вузлі мережі. Саме тому частота виявлення ботів відносно низька в порівнянні з іншими шкідливими програмами.

Мультиагентний підхід фактично позбавляє проблем масштабування при зростанні системи ідентифікації [2]. Виявлення набору однакових ознак взаємодії ботів із контролерами ботнетів можуть вирішити проблему автоматизації виявлення ботів. Як загальні ознаки ботів можна виділити:

– IP-адреса або доменне ім'я контролюючого центру ботнету;

– характеристики HTTP або IRC пакетів із певними командами управління;

– розмірність мережних пакетів;

– часові інтервали мережевих взаємодій;

– трафік зловмисної активності, наприклад, сканування, розсилка спаму, завантаження бінарних файлів; інформацію про протоколи DNS, SMTP;

– протокол обміну даними та порти транспортного рівня.

За основу при побудові методу ідентифікації ботнетів було взято типову структуру мережі Інтернет, засновану на взаємодії між автономними системами. Пропонований метод ідентифікації ботів базується на засобі захисту від розподілених атак типу «відмова в обслуговуванні» з можливістю виявлення атаки в мережі жертви та запобігання генерації атаки в мережі джерела. Отримані у процесі декомпозиції завдання можна віднести до різних класів функціональності: {Виявлення, Блокування, Дослідження, Ідентифікація, Координація, Інтерфейс}. Кожному класу може відповідати свій тип агента, який вирішує завдання класу. Таким чином, мультиагентна система ідентифікації ботнета має вигляд

$$MAS = \left\{A_{\text{det}ection}, A_{blocking}, A_{discrovery}, A_{identificaion}, A_{coordination}, A_{\text{int}erface}\right\},$$

де $A_{\text{det}ection} = \left\{A^1_{\text{det}ction}, ..., A^n_{\text{det}ection}\right\}$ – множина агентів виявлення атаки типу «розподілена відмова в обслуговуванні». Агенти даного класу вирішують завдання виявлення атак і реагують на неї певним у сценарії реагуванні чином. У кожній автономній системі мережі Інтернет розташовується щонайменше один агент даного класу, $A^i_{blocking}$ де i=1..n - номер автономної системи Інтернету.

$A_{blocking} = \left\{A^1_{blocking}, ..., A^n_{blocking}\right\}$ - множина агентів, що вирішують завдання блокування виявленої атаки. У кожній автономній системі мережі Інтернет розташовується щонайменше один агент даного класу $A^i_{blocking}$ де i=1..n - номер автономної системи Інтернету.

$A_{discovery} = \left\{A^1_{discovery}, ..., A^n_{discovery}\right\}$ – множина агентів виявлення ознак робота. Клас агентів вирішує завдання визначення характерних ознак роботи робота. У кожній автономній системі мережі Інтернет розташовується щонайменше один агент даного класу $A^i_{discovery}$ де i=1..n - номер автономної системи Інтернету.

$A_{identificaion} = \left\{A^1_{identificaion}, ..., A^n_{identificaion}\right\}$ - множина агентів ідентифікації роботи робота в рамках автономної системи. Агенти цього класу аналізують трафік мережі наявність ознак функціонування ботів. У кожній автономній системі мережі Інтернет розташовується щонайменше один агент даного класу $A^i_{identificaion}$ де i=1..n – номер автономної системи Інтернету.

$A_{coordination}$ - множина агентів мережі вирішують завдання поширення інформації про активних агентів.

$A_{interface}$ - множина агентів мережі вирішують такі завдання: контроль та моніторинг роботи мережі агентів, візуалізація атак, зберігання інформації.

Таким чином, структура мультиагентної системи ідентифікації ботів складається з наступних елементів:

1. Агент виявлення атаки типу «розподілена відмова в обслуговуванні»
2. Агент виявлення ознак робота
3. Агент ідентифікації роботів
4. Агент блокування атак. Функціонує, коли його розташування є мережею джерела атаки. Зокрема, здійснює реагування на основі інформації отриманої від агентів виявлення атак згідно з профілем мережевої безпеки (блокування систем задіяних у реалізації атаки, оповіщення відповідальних осіб по електронній пошті, SMS).
5. Агент координації. Поширює інформацію про місцезнаходження різних агентів з метою взаємодії між ними.
6. Інтерфейсний агент. Встановлюється у будь-якій точці глобальної мережі Інтернет. Призначений для контролю та моніторингу роботи мережі агентів, надання графічного інтерфейсу візуалізації виявлених атак, зберігання та забезпечення доступу до історії виявлених атак.

Концептуальний алгоритм функціонування системи полягає у наступному:

1. Агент виявлення атаки типу «розподілена відмова в обслуговуванні» виявляє атаку на підконтрольну йому мережу.
2. Агент виявлення атаки повідомляє агенту координації інформацію про мережі джерела виявленої атаки.
3. Агент координації передає агентам блокування, що знаходяться у відповідних джерелах атаки автономних системах, інформацію про вузол, що атакує.
4. Агент координації передає агенту виявлення ознак бота, що контролює мережу джерела атаки, інформацію про атакуючий вузол.
5. Агент координації передає інтерфейсному агенту інформацію про атаку.
6. Агент блокування припиняє зловмисну активність вузлів, що знаходяться в контрольованій мережі.
7. Агент виявлення ознак бота аналізує активність вузлів помічених в атаці. Внаслідок чого виявляє характерні ознаки роботи бота.
8. Агент виявлення ознак бота повідомляє характерні ознаки роботи агенту координації.
9. Агент координації розсилає інформацію про роботу ботів агентам ідентифікації ботів.
10. Агенти ідентифікації аналізують трафік своєї мережі, пробуючи виявити отримані ознаки роботи бота. У разі вдалої ідентифікації передають інформацію про бота агенту координації, який направляє її інтерфейсному агенту для подальшого прийняття рішення.

Запропонований метод (рис.1) дозволяє виявити ботнетів на основі аналізу функціонування ботів, що беруть участь у конкретній атаці. Особливість методу полягає у можливості ідентифікувати ботів, які не брали участі в атаці за рахунок роботи розподіленої мережі інтелектуальних агентів.

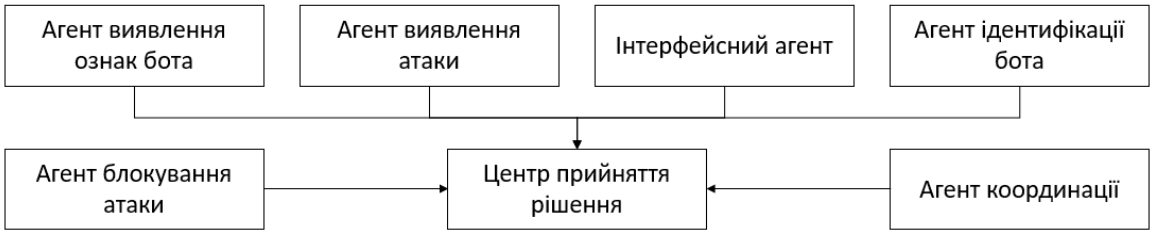


Рис. 1. Мультиагентий метод виявлення ботів

Список літератури

1. Козюра В. Д., Хорошко В. О., Шелест М. Є., Ткач Ю. М., Балюнов О.О. Захист інформації в комп'ютерних системах: підручник. – Ніжин: ФОП Лук'яненко В.В., ТПК «Орхідея», 2020. – 236с.

2. Lysenko, S.; Bobrovnikova, K.; Kharchenko, V.; Savenko, O. IoT Multi-Vector Cyberattack Detection Based on Machine Learning Algorithms: Traffic Features Analysis, Experiments, and Efficiency. Algorithms 2022, 15, 239.

УДК 004.056, 004.75

М.М. Сабов, *магістр 2 курсу*
msabov_@polissiauniver.edu.ua
Науковий керівник: К.В.Молодецька
професор кафедри комп'ютерних технологій і моделювання систем, доктор технічних наук
Поліський національний університет, м. Житомир

АНАЛІЗ ТЕХНОЛОГІЙ ВИЯВЛЕННЯ БОТІВ У СОЦІАЛЬНИХ МЕРЕЖАХ

В рамкам диверсифікації каналів комунікації, соціальні мережі перетворилися на середовище поширення дезінформації та пропаганди для впливу на масову суспільну свідомість. Для поширення деструктивного контенту в соціальних мережах використовують додаткові інструменти ампліфікації інформаційного впливу – соціальних ботів і тролів. Боти в соціальних мережах – це автоматизовані акаунти, які можуть виконувати різноманітні завдання, від автоматичного постингу контенту до імітації людської взаємодії. Хоча деякі боти використовуються для позитивних цілей, таких як автоматизація рутинних завдань та надання корисної інформації, інші можуть бути використані для маніпулювання думкою громадськості, спаму та інших шкідливих дій. Тому виявлення та блокування шкідливих ботів є важливим для забезпечення інформаційної безпеки та прозорості інформаційного простору соціальних мереж.

1. Аналіз поведінки користувачів та використання машинного навчання для виявлення ботів

Аналіз поведінки користувачів та використання методів машинного навчання в соціальних мережах відіграє вирішальну роль у виявленні ботів. Боти, як правило, демонструють аномальну або нелюдську поведінку, включаючи надмірну активність, автоматизовані відповіді та стандартні шаблони комунікації. Основні параметри для аналізу включають час та динаміку публікацій, мережеві характеристики, такі як структура друзів, та інші специфічні особливості поведінки, що допомагають ідентифікувати потенційних ботів. Машинне навчання, включаючи алгоритми, такі як Decision Tree, Random Forest та нейронні мережі, може бути застосоване для класифікації аккаунтів як ботів або людей, використовуючи набори даних із відомими прикладами ботів та людських аккаунтів.

Текстові дані та метадані, такі як нехарактерні шаблони мови та аномальні часові мітки публікацій, можуть служити важливими індикаторами аномальної поведінки акаунтів. Використання глибоких нейронних мереж для аналізу цих даних може сприяти ідентифікації складних шаблонів та аномалій, які можуть бути неочевидними для традиційних методів.

2. Використання метаданих та глибинного навчання для виявлення ботів

Метадані, такі як IP-адреси, часові мітки, та інформація про використані пристрої, можуть бути використані для виявлення ботів. Боти можуть використовувати специфічні IP-адреси або показувати аномальні шаблони в часових мітках своїх дій, що може слугувати індикатором їхньої присутності.

Глибинне навчання, зокрема конволюційні та рекурентні нейронні мережі, може бути використано для аналізу більш складних шаблонів у даних, які можуть бути недоступні для традиційних методів машинного навчання. Це може включати аналіз тексту, зображень, поведінкових характеристик або часових рядів для виявлення складних шаблонів поведінки ботів [5].

Отже, виявлення ботів у соціальних мережах залишається важливим науковим завданням, що вимагає постійного дослідження та розробки нових методів, моделей та технологій детектування. З урахуванням швидкого розвитку інформаційних технологій та змін у тактиках, які використовують суб'єкти ведення інформаційної боротьби, неперервне оновлення та адаптація методів виявлення є ключовими для забезпечення ефективності та актуальності в майбутньому.

Список літератури

1. Молодецька-Гринчук К. В. Метод оцінювання ознак загроз інформаційній безпеці держави у соціальних інтернет-сервісах. Автоматизація технологічних і бізнес-процесів. 2017. Vol. 9, Iss. 2/2017. С. 36–42.
2. Phenomenological model of information operation in social networking services. Molodetska K., Tymonin Y., Markovets O., Melnychyn A. Indonesian Journal of Electrical Engineering and Computer Science. 2020. Vol. 19, No. 2. PP. 1171–1180.
3. Hayawi K., Saha S., Masud M.M. et al. Social media bot detection with deep learning methods: a systematic review. Neural Comput & Applic, 2023, 35, P. 8903–8918.
4. Maksim Kalameyets. Algorithms and techniques for bot detection in social networks. Library and information sciences. Université Paul Sabatier - Toulouse III; ITMO University, 2021.

УДК 004.056.53

Улічев О.С
askin79@gmail.com
Центральноукраїнський національний технічний університет, м. Кропивницький

ФАКТОРНИЙ ПІДХІД ОЦІНКИ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Захист інформації є задачею нескінченного циклу. Тобто задача захисту інформації ніколи не може бути вирішена остаточно. Ця ситуація виникає в силу ряду причин: умови функціонування систем захисту, що постійно змінюються, нові підходи до атак і зламів, результати аудитів ІБ, розвиток комп'ютерної техніки і технологій (зокрема розвиток квантових комп'ютерів).

Одне з перших трактувань підходу до виміру ризику запропонував Мільтон Фрідмен [7]. Він розглядав проблему розрахунку (оцінки) рівня ризику крізь призму теорії корисності. Фрідмен зазначав, що в умовах спадної корисності та наявності ризику звичайні принципи максимізації не можуть бути використані, оскільки потрібна певна податкова плата у вигляді компенсації за фактор ризику.

При дослідженні складних систем часто немає можливості безпосередньо вимірювати величини, що визначають їх властивості (чинники). Більше того, нерідко є невідомими кількість та зміст цих факторів. Але можуть вимірюватися інші величини, які від них залежать. Якщо невідомий чинник впливає на кілька вимірюваних ознак, останні виявляють певний зв'язок, наприклад корелюють між собою. Тому загальна кількість факторів може бути значно меншою, ніж кількість вимірюваних ознак. Для виявлення таких факторів використовують факторний аналіз. Зменшення кількості факторів може знадобитися також для забезпечення збіжності алгоритмів подальшого аналізу даних, скорочення ресурсів пам'яті ЕОМ та часу, необхідного для їх обробки, бажання візуалізувати отримані результати тощо. В основу оцінки ризику може бути покладено метод факторного аналізу, який є найбільш адекватним в умовах невизначеності, конфліктності та нечіткої оцінки впливу окремих факторів, і дозволяє поєднати якісну та кількісну складову аналізу.

Факторний підхід є універсальним і може бути використаний для оцінки ризику на різних стадіях розвитку підприємства та етапах вибору та обґрунтування напрямків мінімізації ризиків інформаційної безпеки. Обов'язковими умовами факторного аналізу є:

- всі досліджувані ознаки мають бути кількісними;
- кількість ознак має бути принаймні вдвічі більшою, ніж кількість змінних;
- вибірка має бути однорідною.

Розглянемо конкретний приклад моделі.

Нехай на підприємстві для оцінки інформаційної безпеки виділено N експертів. Кожен із яких проставляє значення K ризикам, і на виході отримуємо значення випадкових багатовимірних нормально розподілених величин:

$$X_t = (X_{1t}, X_{2t}, \ldots\ldots X_{kt}), \quad (1)$$

де t = 1,2, ..., N.

Значення випадкових багатовимірних величин обумовлені якимись об'єктивними причинами, які називатимемо факторами. Передбачається, що кількість цих чинників завжди менше, ніж число K вимірюваних ризиків інформаційної безпеки. Ці фактори є прихованими, їх не можна безпосередньо виміряти і тому вони є гіпотетичними. Однак є методи їх виявлення, які становлять сутність факторного аналізу. Далі для конкретизації введемо припущення. Нехай в інформаційній безпеці було виділено чотири ризики, які обумовлені дією двох факторів (факторів) F1 та F2. Фактор F1 пояснює вплив всіх ризиків на інформаційну безпеку, своєю чергою F2 описує вплив лише X2 та X3.

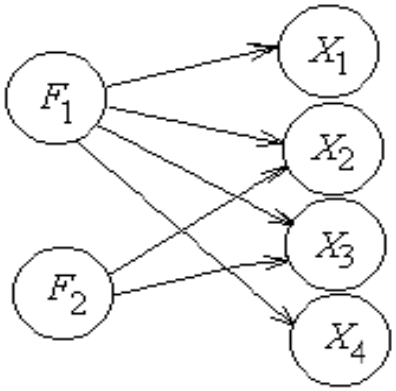


Рис. 1. Взаємозв'язок факторів та ризиків інформаційної безпеки

Отже, значення ризиків X1 та X4 визначаються лише фактором F1, а ризики X2 та X3 визначаються сукупною дією факторів F1 та F2. Але все це, поки що нам невідомо, і перед експертами стоїть завдання оцінити інтенсивність впливу факторів F1 і F2 на ризики X_i і виділити в X_i ті частини, які обумовлені дією кожного з F1 і F2 окремо.

Для вирішення цього завдання висувається припущення про залежність, нехай висунуто припущення, що X_i лінійно залежить від F_m (m = 1,2). Для нашого випадку маємо:

$$X_i = a_{i1} * F_1 + a_{i2} * F_2 \quad (2)$$

де i = 1,2,3,4;

a_{i1}, a_{i2} - факторні навантаження.

За цією гіпотезою, можемо отримати дві моделі факторного аналізу:

1) метод головних компонентів (МГК), у якому значення оцінки кожного з ризиків представляються у вигляді лінійних комбінацій факторних навантажень a_{ij} та факторів Z_j, де j = 1,2, ..., m.

$$R_F = \sum_{j=1}^{m} a_{ij} * Z_j, \quad (3)$$

де m – число факторів.

2) модель власне факторного аналізу (ФА), коли ризики, що спостерігаються, визначаються не тільки факторами, а й дією локальних випадкових причин.

$$R_F = \sum_{j=1}^{m} a_{ij} * Z_j + e_i, \quad (4)$$

Висновки

Дослідження публікацій та літератури на тему дозволяють зробити висновок, що сьогодні задача теоретичного обґрунтування повноти та ефективності інформаційного захисту залишається відкритою, насамперед це пов'язано з високою динамікою як систем захисту, так і методик та інструментів інформаційних атак. Дослідження можливості застосування математичних методів з метою оцінки захисту є актуальним питанням у сучасних умовах розвитку.

Дослідники питання оцінки якості (ефективності) систем захисту пропоную два різні напрями:

- моделі оцінки стійкості реалізованої системи захисту до атак та різних загроз;
- моделі оцінки ризиків інформаційної безпеки.

Один з простих підходів отримання моделі оцінки ризиків представлено в роботі.

Список літератури

1. BS 7799-3:2006 Information security management systems. Guidelines for information security risk management.

2. ISO / IEC 27000: 2009, Information security manage-ment systems. Overview and vocabulary. [Электронный ресурс]. Режим доступа: https: //www.iso. org / standard / 41933.html.

3. RiskWatch International. Global Leader in Risk Assessment Solutions [Электронный ресурс]. – Режим доступа: www.riskwatch.com

4. A Qualitative Risk Analysis and Management Tool – CRAMM. – Bethesda, Maryland: SANS Institute, 2012.

5. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу [Текст]: НД ТЗІ 2.5-004-99. – 1999. – Чин. 1999.07.01. – К. : ДСТСЗІ СБ України, 1999. – 57 с.

6. Національний стандарт України ДСТУ IEC/ISO 31010:2013 «Керування ризиком. Методи загального оцінювання ризику» / Офіційне видання. Київ. Мінекономрозвитку України. 2015 – с. 73.

7. Фрідмен М., Севідж Л. Дж. Аналіз корисності при виборі серед альтернатив, що передбачають ризик (переклад, документ pdf)

8. Хорошко В.О. «Проєктування комплексних систем захисту інформації», 2020. – 317с.

УДК 004 + 614.8

К.М. Марченко, О.В. Оришака
k_marchenko@i.ua, oryhsaka@gmail.com
Центральноукраїнський національний технічний університет, м. Кропивницький

ІНФОРМАЦІЙНИЙ ПРОСТІР ЯК ПОЛЕ БИТВИ – ЯК ВЦІЛІТИ

В інформаційному суспільстві високими темпами зростає вплив інформації на свідомість та благополуччя як людини, суспільства, держави. Інформація суттєво впливає на вибір, що здійснюється людиною, та на стан її здоров'я на всіх рівнях – духовному, ментальному, емоційному та фізичному [1]. Добре знаючи цей факт, різні геополітичні сили все більш широко й активно використовують інформацію в якості зброї для досягнення своїх цілей [2 - 4]. Використовуються інформаційні маніпуляції, фейки, брехня, спотворення та викривлення інформації, вибіркова вигідна інформація, а також спрямована на певні спільноти потужна агітація, пропаганда, втілення штучних ідеологій та хибних картин світу.

Потрапляючи в потік такого деструктивного інформаційного впливу, людина часто втрачає зв'язок з реальністю та природний здоровий стан. Світ починає сприйматися крізь призму тієї інформації, якою наповнена свідомість людини. Подаючи у щільному, спрямованому потоці вигідну, штучно підготовлену інформацію, політичні сили впливають на вибір людини, активно спонукаючи її до певних вчинків. Для підсилення впливу інформації надається емоційне забарвлення, враховуються інтереси, схильності та ментальні установки цільової аудиторії. Такий щільний інформаційний потік має досить велику гравітацію, аби утримувати увагу та свідомість адресантів у присутності та напрузі.

Агресивними формами використання інформації є інформаційний тиск, інформаційні атаки, інформаційні війни. Головною ціллю спрямованого інформаційного впливу є масова свідомість, яка використовується як інструмент реалізації певних деструктивних ідей та планів. Боротьба ведеться за домінуюче місце ідей та інтересів різних геополітичних сил у масовій свідомості, і захоплюється це місце за аналогією з територіальною інтервенцією за допомогою відповідної інформації.

Агресивні форми впровадження деструктивної, токсичної інформації, які призводять до деградації суспільства, ворожнечі, масової депресії, психічних розладів, погіршення стану здоров'я населення і навіть масової загибелі людей, можна розглядати як особливу форму геноциду – інформаційний геноцид.

В останні роки в інформаційному просторі суттєво порушено баланс позитивної та негативної інформації з явною перевагою останньої. Через інформаційний простір у свідомість людей вливається все більш низькоякісна, низько моральна інформація, яка має за мету деградацію кінцевих користувачів та деградацію суспільства. Не можна не відзначити, що майже всі події, які висвітлюються у новинах, торкаються вбивств, насильства, звірств, руйнування та масового знищення людей, а ці новини не можна характеризувати інакше, ніж «новини смерті». Суспільство, змальоване у таких новинах, постає як вкрай деградоване та приречене. Таку інформацію можна кваліфікувати як злочинну та зрадницьку.

Очевидно, що приймаючи участь у сучасному суспільному житті та виробництві, повністю ізолюватися від інформації не можливо. Відповідаючи ж на питання, як вціліти на інформаційному полі бою, можна надати користувачам інформації наступні рекомендації:

- звузьте свій потік інформації до мінімально необхідного;
- звільняйтеся від вже прийнятої інформації, яка не служить вашому благові та розвитку;
- уникайте емоційно забарвленої інформації, адже вона у значній мірі суб'єктивна та провокаційна;
- зосереджуйтесь більше на реаліях, які вас оточують та відносьтеся до них об'єктивно;
- шукайте навколо себе ознаки добробуту та процеси розвитку;
- стикаючись з інформацією, визначте, кому вона вигідна і чи вигідна саме вам;
- вивчить глобальні та стабільні інформаційні потоки, що панують в інформаційному просторі, і уникайте входити до них, адже на сьогодні вони токсичні та руйнівні.

Список літератури

1. Марченко К.М., Пестунов В.М., Святська Л.П., Марченко Т.К. Вплив інформації на стан здоров'я людини. Наукові записки, вип.10, ч. 2, Кіровоград: КНТУ, 2010. - С. 224-229.

2. Гібридна війна і журналістика. Проблеми інформаційної безпеки : навчальний посібник / О. І. Харитоненко, Ю. С. Полтавець. – Київ : Вид-во НПУ імені М. П. Драгоманова, 2018. – 356 с.

3. Бабенко Ю. Інформаційна війна – зброя масового знищення! URL: https://www.pravda.com.ua/rus/articles/2006/04/20/4399050/

4. Курбан О.В. Сучасні інформаційні війни в мережевому он-лайн просторі [Текст]: навчальний посібник / О.В. Курбан. – Київ: ВІКНУ, 2016. - 286 с.

УДК 004.057

О. Ю. Тішура
penoneq@gmail.com
Науковий керівник: Ю.В. Білявська
доцент кафедри менеджменту, кандидат економічних наук, доцент
y.biliavska@knute.edu.ua
Державний торговельно-економічний університет, м. Київ

ПОТОЧНИЙ СТАН ТА ЗАКОНОТВОРЧІ ТЕНДЕНЦІЇ У СФЕРІ КІБЕРБЕЗПЕКИ

Цифрові технології нині є ключовим фактором розвитку підприємств, отже, кібербезпека стає дедалі актуальнішим напрямом наукових досліджень. Основними нормативно-правовими документами, що формують політику України в галузі кіберпезпеки є Стратегія кібербезпеки України, затверджена Указом Президента України від 15 березня 2016 року № 96/2016 та Закон України «Про основні засади забезпечення кібербезпеки України» № 2163-VIII. Саме цими документами визначаються основні суб'єкти прийняття рішень у сфері кібербезпеки.

Для координації та контролю діяльності суб'єктів сектору безпеки і оборони, які забезпечують кібербезпеку у відповідних сферах, у 2016 році Указом президента України було створено Національний координаційний центр кібербезпеки (НКЦК) – робочий орган Ради національної безпеки і оборони України. Указом Президента України від 28.01.2020 №27 було посилено спроможності НКЦК та змінено формат його діяльності, зокрема, до роботи залучено фахівців з приватного сектору, які спеціалізуються на кіберзахисті. Посилений НКЦК став «хабом», цифровою платформою, аналітичним центром з моніторингу, виявлення, нейтралізації, прогнозування потенційних кіберзагроз та запобігання ним у майбутньому як у державному, так і у приватному секторі.

В той же час наразі в Україні розпочалися дискусії щодо необхідності оптимізації роботи Державної служби спеціального зв'язку та захисту інформації України з метою посилення кіберзахисту об'єктів критичної інфраструктури. Наразі також готуються пропозиції щодо реорганізації Державного центру кіберзахисту Держспецзв'язку. Додатково прийняті рішення КМУ щодо затвердження порядків формування переліку об'єктів критичної інформаційної інфраструктури, а також щодо забезпечення функціонування системи кіберзахисту державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури.

Міжсекторна співпраця у сфері кібербезпеки в Україні представлена у вигляді створеного на початку 2020 року Глобального центру взаємодії в кіберпросторі - інтеграційної платформи для держави, бізнесу і навчальних інститутів як українського, так і міжнародного формату. Мета центру - розробити нові правила взаємодії в цифровому світі. Завданням організації є створення майданчику для змістовного співробітництва стейкхолдерів кіберпростору - державних, ділових, навчальних і наукових інститутів, як українських, так і міжнародних гравців цієї сфери. Центр створений за сприяння Міністерства внутрішніх справ і НАК «Нафтогаз України».

Організація має запропонувати компаніям-учасникам:

- інсайти від міжнародних партнерів про стан та тенденції кібербезпеки у світі;
- оперативну комунікацію з державними органами, такими як МВС та Кіберполіція, Міністерство цифрової трансформації;
- можливість запропонувати нові законодавчі рішення для держави у сфері протидії кіберзагрозам;
- ефективну співпрацю при розслідуванні кібератак на компанію [1].

Також, за кількістю нормативно-правових документів і числом практичних заходів, що сьогодні вживаються в нашій країні у сфері захисту цифрової трансформації, навряд чи якась країна пострадянського простору випереджає Україну. Так, на теперішній час прийнято і діє (або діяло) чимало важливих документів концептуально-стратегічного характеру, в яких інформаційній безпеці відведено чільне місце. Протягом останніх п'ятнадцяти років в Україні змінили один одного чотири документи стратегічного характеру, в яких особливим чином наголошується на інформаційній сфері як об'єкті національної безпеки. Йдеться про Стратегії 2007, 2012, 2015 та 2020 рр. [2].

Ще у 2007 р. зазначалося, що безпека інформаційно-комп'ютерних систем в галузі державного управління, фінансової і банківської сфери, енергетики, транспорту, внутрішніх та міжнародних комунікацій тощо наближається до критичного стану [3].

У документі 2012 р. прямо наголошено на нездатності України протистояти новітнім викликам національній безпеці, пов'язаним із застосуванням інформаційних технологій в умовах глобалізації, насамперед кіберзагрозам. Тому серед першочергових засобів нейтралізації цих загроз робився акцент принаймні на забезпеченні безпеки інформаційно-телекомунікаційних систем, що функціонують в інтересах управління державою, забезпечують потреби оборони та безпеки держави, кредитно-банківської та інших сфер економіки, систем управління об'єктами критичної інфраструктури, а так само на розробці та впровадженні національних стандартів і технічних регламентів застосування інформаційно-комунікаційних технологій, гармонізованих із

відповідними стандартами держав-членів ЄС, у тому числі згідно з вимогами Конвенції про кіберзлочинність [4].

У Стратегії 2015 р. серед актуальних загроз національній безпеці України окремо виділено загрози інформаційній безпеці, зумовлені веденням інформаційної війни проти України, відсутністю цілісної комунікативної політики держави, недостатнім рівнем медіа-культури суспільства, та загрози кібербезпеці і безпеці інформаційних ресурсів, проявом яких є уразливість об'єктів критичної інфраструктури, державних інформаційних ресурсів до кібератак, фізична і моральна застарілість системи охорони державної таємниці та інших видів інформації з обмеженим доступом [5].

Стратегія 2020 р. уперше згадує про те, що Україна має намір здійснити цифрову трансформацію, забезпечуючи надання адміністративних послуг через безпечне " єдине вікно " з використанням сучасних інформаційних технологій, та поширювати цифрову грамотність [6].

Не можна не згадати і про Стратегію розвитку інформаційного суспільства в Україні 2013 р., в якій на той час наголошувалося, що національна інформаційна сфера перебуває у стані активного становлення, гармонійного включення у глобальний світовий інформаційний простір та є основою розвитку інформаційного суспільства в Україні [7].

Наприкінці 2021 р. в Україні прийнято нову Стратегію здійснення цифрового розвитку, цифрових трансформацій і цифровізації системи управління державними фінансами на період до 2025 року та План заходів з її реалізації. Зазначені документи прийняті для забезпечення якісної цифрової трансформації у певних сферах господарювання, пов'язаних з обігом матеріальних цінностей: як-от управління державними фінансами, діяльність із державного внутрішнього фінансового контролю, моніторингу та оцінки фіскальних ризиків, максимальна автоматизація бізнес-процесів та ін. У Стратегії як на окрему мету вказано на інформаційну безпеку в Єдиній інформаційно-телекомунікаційній системі Системи управління державними фінансами від сучасних кіберзагроз в умовах цифровізації управлінських процесів та необхідності обміну даними [8].

Отже, сучасний світ давно зробив перший крок до принципово нової технологічної, економічної та соціальної реальності – епохи цифрової глобалізації. Забезпечення кібербезпеки є одним із вагомих пріоритетів у загальній системі національної безпеки України. Впроваджуючи новітні технології, цивілізація у XXI ст. сприяє активному формуванню супутніх ризиків [9, с. 50]. Також спостерігаємо зростання питомої ваги кіберзагроз, і ця тенденція в міру розвитку цифрових технологій у поєднанні зі штучним інтелектом лише посилиться, а зростання такого впливу визначатиме формування нової безпекової ситуації

Список літератури

1. Цифрові трансформації в Україні - http://eap-csf.org.ua/wp-content/uploads/2021/04/Research_DT_PF_WG2_ua-1.pdf

2. Правова платформа для забезпечення в Україні ефективного захисту цифрових трансформацій суспільства - http://il.ippi.org.ua/article/view/254339

3. Про стратегію національної безпеки України - https://zakon.rada.gov.ua/laws/show/105/2007#Text

4. Про рішення Ради національної безпеки і оборони України від 8 червня 2012 року «Про нову редакцію Стратегії національної безпеки України» - https://zakon.rada.gov.ua/laws/show/389/2012#n6

5. Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року "Про Стратегію національної безпеки України" - https://zakon.rada.gov.ua/laws/show/287/2015#Text

6. Про схвалення Стратегії цифрової трансформації соціальної сфери - https://zakon.rada.gov.ua/laws/show/1353-2020-%D1%80#Text

7. Про схвалення Стратегії розвитку інформаційного суспільства в Україні - https://zakon.rada.gov.ua/laws/show/386-2013-%D1%80#Text

8. Про схвалення Стратегії здійснення цифрового розвитку, цифрових трансформацій і цифровізації системи управління державними фінансами на період до 2025 року та затвердження плану заходів щодо її реалізації - https://zakon.rada.gov.ua/laws/show/1467-2021-%D1%80#Text

9. Білявська Ю.В., Шестак Я.І. стаття: Кібербезпека та кібергігієна: нова ера цифрових технологій, ДТЕУ, Міжнародний науково-практичний журнал "Товари і ринки". №3-2022, м. Київ, 2022, С 47-59.

УДК 004.056

Д.О. Душко[1], Н.С.Петляк[1]
ddushko@khmnu.edu.ua, npetlyak@khmnu.edu.ua
[1]*Хмельницький національний університет, м. Хмельницький*

МЕТОД ТА СИСТЕМА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВА

Корпоративна інформаційна система - це комплекс апаратних засобів (сервера та серверне обладнання, робочі станції, канали зв'язку та ін.), каналів зв'язку та програмного забезпечення даної системи [1].

Задля створення ефективної системи захисту інформації важливо під час розробки дотримуватися низки ключових принципів, а саме:

– комплексність та узгодженість – побудова системи захисту інформації передбачає застосування досить широкого спектру інструментів та методів захисту, при цьому важливо підтримувати цілісність системи та уникати вразливостей у взаємодії окремих компонентів системи;

– диференціація – кожен рівень захисту має розроблятися з урахуванням рівня важливості та критичності інформації, оцінки потенційних атак;

– достатність механізмів захисту - передбачає оцінку співвідношення витрат на створення та підтримку системи захисту інформації та можливої шкоди.

Проаналізувавши можливі шляхи здійснення несанкціонованого доступу до інформаційного середовища [2] та ґрунтуючись на вищезазначених принципах організації системи інформаційної безпеки, запропоновано модель системи захисту інформації (СЗІ), що буде складатися із трьох основних компонентів: захист від зовнішніх загроз та руйнівних дій зловмисників, захист від віддалених та міжсегментних атак, захист інформаційного середовища від окремих ПК та серверів у мережі. Таким чином, розроблена модель СЗІ включатиме три компоненти: модель захисту від зовнішніх загроз, модель захисту від віддалених та міжсегментних атак та модель захисту у внутрішньому сегменті мережі.

З метою аналізу процесу прийняття рішень щодо протидії загрозам, представимо кілька типів атак: міжсегментну атаку, зовнішню атаку через точку бездротового доступу, зовнішню атаку через інтернет.

Пропонуємо модель протидії у формі зв'язного графа (рис.1а), де U_n – це варіанти реагування, а V_n – варіанти результатів під час реалізації протидії загроз.

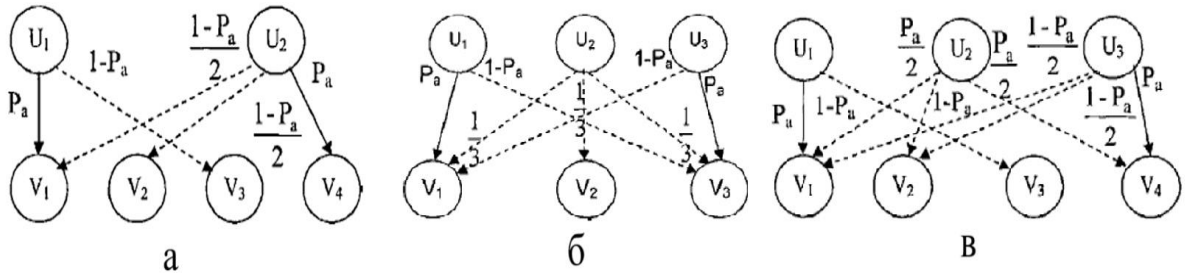


Рис. 1. Граф зв'язків варіантів реагування та результатів:
а) при прийнятті рішень при міжсегментній атаці, б) рішень при зовнішній атаці через Wi-Fi мережу, в) при зовнішній атаці через провайдера

При виборі варіанту реагування U_1 з ймовірністю $1\text{-}P_a$ буде отримано середні втрати, оскільки в якості атаки прийнято при стандартному режимі роботи мережі ненавмисні шкідливі впливи від користувача або помилкове розпізнавання як атаки сигналів із сенсорів.

Реалізація варіанту реагування U_2, може мати три різні варіанти результату. Якщо події, розпізнані як аномальні, дійсно є атакою, то з ймовірністю P_a буде реалізовано максимальні збитки за відсутності блокування атакуючого впливу. У разі якщо розпізнана аномальна дія була причиною помилкових дій користувача, то шкоди не буде (тобто дорівнює нулю). Якщо керуючий вплив буде реалізовано внаслідок помилкового розпізнавання сигналів як атаки, то користувачеві буде відправлено попередження та знижено його пріоритет – буде нанесено незначні збитки користувачеві. У останніх двох варіантах ймовірності результатів складати одну й ту саму величину $(1\text{-}P_a)/2$.

Для реалізації зовнішнього вторгнення зловмиснику потрібен доступ до бездротового адаптера і необхідно, щоб він знаходився в радіусі дії бездротової мережі. На відміну від атаки за допомогою провідної лінії, маємо більш високу ступінь погрози та можливість нанесення максимальної шкоди. Об'єктом атаки в даному випадку є точка доступу.

Для забезпечення захисту використовуються системи виявлення бездротових атак, основою роботи яких є сигнатурний аналіз та аналіз поведінки. Події безпеки генеруються при виявленні відхилення параметрів точки доступу від заданих. Для реалізації захисту інформації процедури реагування повинні бути сформовані

таким чином, щоб були максимально знижені можливі збитки як від реалізації вторгнення, так і від можливого збою взаємодії через точку доступу. Модель протидії у графічному вигляді представлена на рис.1б.

Якщо система реалізує вплив U_1, то з ймовірністю P шкоди системі не буде завдано. Ймовірність P_a, у разі рівна ймовірності атаки. Якщо за реалізацію атаки були помилково розпізнані сигнали сенсорів чи відбулася помилка в діях користувача, то шкода при виборі варіанта реагування впливу U_1 буде. Імовірність $1–P_a$ такого результату відповідає ймовірності помилкової інтерпретації сигналів системою чи помилки користувача. Якщо обраний варіант реагування U_3, то в разі реалізації атаки максимальну шкоду буде отримано з ймовірністю P_a – атаку не відстежено системою. Якщо даний варіант реагування обраний у ситуації помилкового розпізнавання сигналів сенсорів як атаки, то шкода буде нульовою – система захисту не втручається у роботу та продовжується робота в штатному режимі (ймовірність складе $1-P_a$ для даного результату). Якщо системою обраний варіант реагування U_2 (здійснення DOS -атаки), то можливі три варіанти результату (нульовий - запобігання дії зловмисника, середній – заблокований користувач за помилкові дії або максимальний – порушено працездатність мережі, завдано збитки), ймовірності яких дорівнюють 1/3.

Для прийняття рішень з реагування в разі можливого зовнішнього вторгнення через провайдера запропоновано модель протидії, що зображено на рис.1в.

Якщо система вибирає варіант реагування U_1, то з ймовірністю P_a, яка дорівнює ймовірності реалізації атаки, збитки інформаційної системи дорівнює нулю, оскільки система захисту нейтралізувала атаку. Якщо здійснено U_1, але відбулося хибне спрацювання сенсорів або було зроблено помилку користувачем, то шкода буде середнього значення. Ймовірність даного результату становитиме $1-P_a$. Реалізація рішення U_2 може призвести або для завдання шкоди віддаленому користувачеві з ймовірністю $1-P_a$, або у разі реалізованої атаки можливі два рівноймовірні $P_a/2$ результати. Коли U_3 атака здійснена, то результатом буде максимальний збиток (реалізована атака не буде зупинена системою захисту з ймовірністю P_a, що дорівнює ймовірність атаки. У разі помилкового спрацьовування датчиків або помилки користувача, з рівною ймовірністю $(1-P_a)/2$ кінцевому користувачеві буде завдано незначної шкоди, інакше не буде ніякої шкоди як системі, так і користувачеві.

Для реалізації системи управління інформаційною безпекою підприємства, що зображена на рис.2, використано наступні елементи: засоби управління (ЗУ); модулі управління (МУ); система підтримки прийняття рішень керування захистом інформації (СППР); зовнішні загрози (Uзовн); доступна в СППР інформація про стан навколишнього середовища (U'зовн); інформація про команду на виході СППР (U); контрольна дія (Uкд); інформація про стан оперативного керування (X); інформація про контрольовані параметри, що доступні в системі підтримки прийняття рішень керування захистом (X').

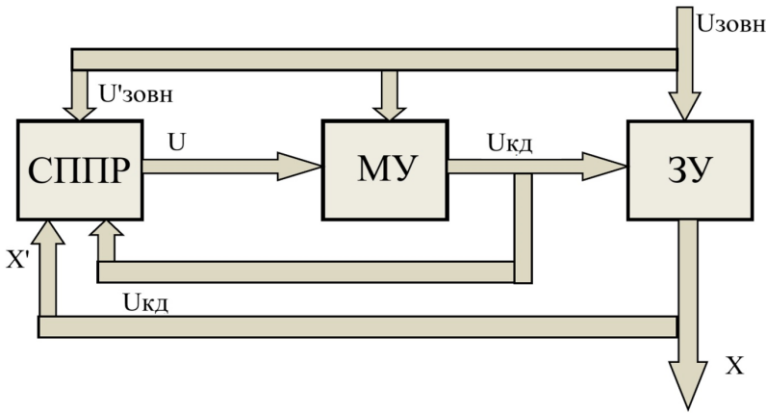


Рис.2. Система управління інформаційною безпекою підприємства

Список літератури

1. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.1994 р. № 80/94. Дата оновлення: 01.07.2022. URL: https://zakon.rada.gov.ua/laws/show/80 /94-вр (дата звернення: 28.09.2023)

2. Козюра В. Д., Хорошко В. О., Шелест М. Є., Ткач Ю. М., Балюнов О.О. Захист інформації в комп'ютерних системах: підручник. – Ніжин: ФОП Лук'яненко В.В., ТПК «Орхідея», 2020. – 236с.

УДК 004.056.51

І.В.Сафонов
safonov.igor.2005@gmail.com
Науковий керівник: Ю.В. Білявська,
доцент кафедри менеджменту, кандидат економічних наук, доцент
y.biliavska@knute.edu.ua
Державний торговельно-економічний університет, м. Київ

МЕНЕДЖМЕНТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Інформаційна безпека є однією з найважливіших складових загальної безпеки організації. Вона забезпечує захист інформаційних активів організації від несанкціонованого доступу, використання, розкриття, модифікації або знищення.

Менеджмент інформаційної безпеки (МІБ) - це процес управління та контролю за інформаційними активами організації з метою їх захисту від загроз. Мета його- забезпечити захист інформаційних активів організації від усіх можливих загроз та забезпечити їхню доступність, цілісність та конфіденційність.

МІБ повинен враховувати загальні принципи, такі як комплексність (МІБ повинен враховувати всі можливі загрози інформаційній безпеці, як внутрішні, так і зовнішні), проактивність (МІБ повинен бути спрямований на попередження загроз, а не на їх ліквідацію), відповідність (МІБ повинен відповідати вимогам законодавства та внутрішніх політик організації). МІБ виконує такі функції: планування (розробка та впровадження політики та процедур МІБ), організація (створення та забезпечення функціонування системи МІБ), контроль (моніторинг та оцінка ефективності системи МІБ). МІБ включає в себе такі заходи: технологічні заходи (використання засобів захисту інформації, таких як антивіруси, фаєрволи та системи виявлення вторгнень), адміністративні заходи (розробка та впровадження політики та процедур безпеки, навчання користувачів), фізичні заходи (захист фізичного доступу до інформації).

Ефективний МІБ може допомогти організації захистити свої інформаційні активи від загроз та забезпечити їхню доступність, цілісність та конфіденційність , в умовах повномасштабної війни в Україні ефективний менеджмент інформаційної безпеки є особливо важливим для організацій, які продовжують свою діяльність. Військові дії та інші фактори створюють додаткові загрози інформаційній безпеці, тому організаціям необхідно вжити додаткових заходів для захисту своїх інформаційних активів.

Найефективнішими рішеннями для захисту інформації системи (ІС) організації є : навчання персоналу ІБ, сучасне ПЗ для моніторингу та управління ІБ, розробка плану реагування на інциденти, це можна побачити у таблиці 1 - Загрози ІС та їх рішення [1].

Таблиця 1

Загрози інформаційних систем та їх рішення

Загроза для інформаційної безпеки	Рішення загрози
Фішинг і смішинг	Навчання користувачів, системи виявлення вторгнень і спам-фільтри, надійні інструменти автентифікації, плани реагування на інциденти
Зловмисне програмне забезпечення	Програмне забезпечення безпеки, оновлення системи ІБ, безпека мережі, навчання з безпеки для співробітників, плани реагування на інциденти
Програми-вимагачі	Сучасні системи ІБ, окремі системи резервного копіювання, належна кібергігієна, плани реагування на інциденти
Внутрішні загрози	Зміни в культурі, захист критично важлицвих активів, відстеження поведінки, плани реагування на інциденти
Ненавмисне розголошення	Обмежений доступ, програмне забезпечення для запобігання витоку інформації та моніторингу активності, плани реагування на інциденти
Загроза для інформаційної безпеки	Рішення загрози
Розвідка сховища	Шифрування, надійні засоби автентифікації, вибір інформації, плани реагування на інциденти
Атаки нульового дня	Брандмауери, ефективне програмне забезпечення для запобігання вторгненням, плани реагування на інциденти
Соціальна інженерія	Навчання персоналу, використання VPN, процедури моніторингу, плани реагування на інциденти
Витік даних	Управління загрозами, моніторинг активності користувачів, плани реагування на інциденти

Для захисту інформаційної системи організації та її менеджменту є багато напрямків:

- CRM системи

- Email Security
- Web Application Firewall (WAF)
- User and Entity Behavioral Analytics (UBA / UEBA)
- Backup and Recovery
- File Storage Optimization
- eDiscovery& Compliance
- Endpoint Security

Цифрова економіка, як породження Концепції «Індустрія 4.0», стає сьогодні новим рушієм розвиту економіки України [1]. З поглядом на цю новітню потребу, стає актуальною проблема створення відповідної методології цифровізації сучасних підприємств, яка є визначальним базисом практичної реалізації цифрової економіки у всіх її масштабних проявах (регіональному, загальносвітовому). Це, в свою чергу, породжує нову проблему - забезпечення інформаційної безпеки цифрових підприємств. В контексті цього висновку можна стверджувати, що необхідні ґрунтовні дослідження щодо розробки структурної моделі забезпечення інформаційної безпеки процесноорієнтованого цифрового підприємства.За неможливості самостійно створити сучасну та стабільну систему інформаційної безпеки (СІБ) організація може скористатися послугами зовнішніх організацій у сфері інформаційної безпеки - Managed Security Service Providers (MSSP). Наприклад, організація може звернутися до зовнішніх експертів з питань інформаційної безпеки за допомогою у розробці або впровадженні програми управління інформаційною безпекою. В Україні це такі компанії, як TechExpert, MO Group, IT Specialist LLC, BDO Україна, Winncom Technologies, H-X Technologies.

Персонал організації є одним з найважливіших активів у сфері інформаційної безпеки. Тому для забезпечення ефективного захисту інформаційних активів організація повинна проводити регулярне навчання персоналу з питань інформаційної безпеки. В Україні це такі компанії, як Ernst & Young, H-X Technologies.

Підсумовуючи можна зазначити, що моніторинг ІС організації, її менеджмент, швидке реагування на порушення цілісності ІС, наявність кваліфікованого та обізнаного персоналу у сфері ІБ є важливими в інформаційну еру суспільства. Організаціям можна надати такі рекомендації: розробка та впровадження ефективної системи МІБ, ПЗ для моніторингу , захисту МІБ , навчання персоналу основам ІБ, впровадження посади менеджера ІБ та планів реагування на інциденти.

Інформаційна безпека є однією із важливих складових глобальної безпеки, невід'ємною умовою глобалізації та одним із факторів впливу глобальних процесів на всі сфери діяльності. Дедалі більше посилюється роль інформаційної безпеки у процесі глобалізації і, навпаки, вплив глобальних процесів на інформаційну безпеку та взаємопов'язану з нею економічну, національну та глобальну безпеку в умовах побудови інформаційного суспільства – нового ступеня розвитку людства. Глобальний процес інформатизації суспільства, який є відображенням загальних закономірностей генезису цивілізації, сьогодні охопив усі сфери соціокультурної діяльності людини. Стрімкий розвиток і розповсюдження нових інформаційно-комунікаційних технологій обумовлює кардинальні зміни в управлінні господарськими системами різних рівнів. Формування та рівень розвитку інформації, інформаційних ресурсів та всього інформаційного простору є головною характеристикою розвитку будь-якої соціальноекономічної системи на макро- та мікрорівнях [2, с. 102].

Таким чином, засоби забезпечення збереження та захисту інформації в державній організації, на підприємстві або фірмі відрізняються за своїми масштабами і формами. Вони залежать від виробничих, фінансових та інших можливостей підприємства, від кількості секретів, які вона охороняє та їхньої значимості. При цьому вибір таких заходів необхідно здійснювати за принципом економічної доцільності, дотримуючись у фінансових розрахунках „золотої середини‖, оскільки надмірне закриття інформації, так само як і халатне відношення до її збереження, можуть викликати втрату певної частки прибутку або призвести до непоправних збитків. Відсутність у керівників підприємств чіткого уявлення про умови, що сприяють витоку конфіденційної інформації, приводять до її несанкціонованого поширення.

Список літератури

1. Мартчан Е. Індустрія 4.0 як інноваційний тренд України.URL: https://interfax.com.ua/news/blog /799334.html

2. Тупкало В.М.Бізнес – інжиніринг сучасних процесно – орієнтованих підприємств: монографія / В.М. Тупкало. Київ.: ДУТ, 2016. 281 с.

УДК 65.012.83

В.С. Варава
v.varava_fmtp_8_21_b_d@knute.edu.ua
Науковий керівник: Ю.В. Білявська,
доцент кафедри менеджменту, кандидат економічних наук, доцент
y.biliavska@knute.edu.ua
Державний торговельно-економічний університет, м. Київ

РОЛЬ ISO/IEC 27001 В СИСТЕМІ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

Система управління інформаційною безпекою (від англ. «ISMS», «Information Security Management System») – це система політики, процедур і засобів контролю, які допомагають організації захистити свої інформаційні активи від різних загроз і ризиків. Вона узгоджується з цілями організації, відповідає відповідним стандартам і нормам, а також забезпечує цінність і переваги для зацікавлених сторін, зокрема організації та її споживачів [1].

Міжнародна організація зі стандартизації (від англ. «ISO», «International Organization for Standardization») є незалежною неурядовою організацією та найбільшим у світі розробником добровільних міжнародних стандартів. В свою чергу Міжнародна електротехнічна комісія (від англ. «IEC», «International Electrotechnical Commission») є провідною світовою організацією з підготовки та публікації міжнародних стандартів для електричних, електронних та суміжних технологій.

ISO/IEC 27001 – це стандарт безпеки, який офіційно визначає систему управління інформаційною безпекою та є формальною специфікацією, що передбачає вимоги щодо впровадження, контролю, підтримки та постійного вдосконалення системи управління інформаційною безпекою [2].

Починаючи з 1995 року даний стандарт постійно модифікується, розвивається та акцентує увагу на актуальних викликах, але навіть при внесенні останнього оновлення в жовтні 2022 року він продовжує ґрунтуватись на трьох головних принципах (рис.1).

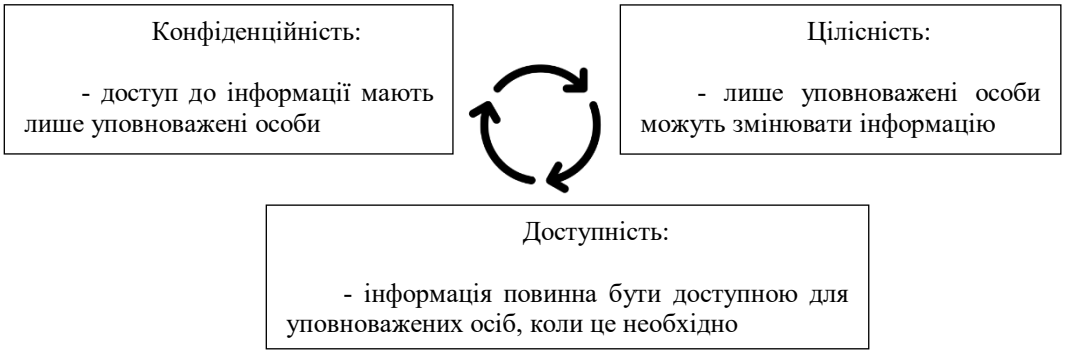


Рис.1 Принципи ISO/IEC 27001

Джерело: сформовано автором за [3]

Оскільки управління інформаційною безпекою тісно пов'язана з управлінням ризиками, то варто наголосити, що управління ризиками є фокусом ISO/IEC 27001 та здійснюється за рахунок певних запобіжних засобів або засобів контролю.

Засоби контролю за стандартом ISO/IEC 27001 – це методи, які слід застосовувати для зниження ризиків до прийнятного рівня. У додатку А до стандарту ISO/IEC 27001 у редакції 2022 року перераховано 93 засоби контролю, поділені за чотирма секціями:

1) Організаційний контроль.

Реалізується шляхом визначення правил, яких слід дотримуватися, а також очікуваної поведінки користувачів, обладнання, програмного забезпечення та систем.

2) Контроль людей.

Впроваджується шляхом надання знань, освіти, навичок або досвіду особам, щоб вони могли виконувати свою діяльність у безпечний спосіб.

3) Фізичні засоби контролю.

Здійснюються за допомогою обладнання або пристроїв, які фізично взаємодіють з людьми та об'єктами.

4) Технологічні засоби контролю.

Впроваджуються в інформаційних системах з використанням програмних, апаратних і мікропрограмних компонентів, доданих до системи.

Багато організацій вирішують прийняти структуру ISO/IECIEC 27001, щоб продемонструвати свою відданість інформаційній безпеці та надати впевненість клієнтам, партнерам і регуляторним органам, що їхні засоби контролю є ефективними. Але повинні зазначити як плюси, так і мінуси даного рішення.

Таблиця 1

Переваги та недоліки впровадження ISO/IEC 27001

Переваги	Недоліки
1	
Міжнародне визнання: - всесвітнє визнання, повага, лояльність; - приваблення клієнтів, партнерів і схвальна оцінка регуляторних органів шляхом наявності необхідних заходів для захисту конфіденційної інформації	Вартість: - потреба великої кількості часу та ресурсів; - витрати на навчання персоналу, проведення оцінок і впровадження нових засобів контролю
2	
Всебічне охоплення: - широкий спектр засобів контролю; - можливість швидко виявити й усунути потенційні вразливості у системі і процесах	Складність: - комплексність може ускладнити розуміння та впровадження; - складно для невеликих організацій з обмеженими ресурсами та досвідом у сфері інформаційної безпеки
3	
Постійне вдосконалення: - регулярний перегляд та вдосконалення засобів контролю; - підтримка ефективності системи з часом; - оптимізація процесів безпеки; - усунення дублювання.	Потребує постійного обслуговування: постійне оновлення засобів контролю, щоб переконатися, що вони ефективні та відповідають останнім найкращим практикам; постійне обслуговування
4	
Міцна основа для інформаційної безпеки: - повний набір засобів контролю, які охоплюють усі аспекти інформаційної безпеки, від оцінки ризиків і управління до контролю доступу та реагування на інциденти	
5	
Покращення рівня безпеки: - зменшення ризику витоку даних, кібератак та інших інцидентів безпеки	

Джерело: сформовано автором за [4]

Отже, система управління інформаційною безпекою зберігає конфіденційність, цілісність і доступність інформації, застосовуючи процес управління ризиками належним чином, і дає зацікавленим сторонам впевненість у ньому. Стандарт ISO/IEC 27001 – це міжнародно визнаний стандарт, який надає набір найкращих практик для створення, впровадження, підтримки та постійного вдосконалення системи управління інформаційною безпекою організації через особливі засоби контролю. Методика впровадження стандарту має певні переваги та недоліки, які слід враховувати індивідуально.

Список літератури

1. Information Security Management System (ISMS). What are the key roles and responsibilities for ISMS governance and leadership?. LinkedIn: Log In or Sign Up. URL: https://www.linkedin.com/advice/0/what-key-roles-responsibilities-isms (дата звернення: 09.10.2023).

2. ISO/IEC 27001:2013 Information Security Management Standards - Microsoft Compliance. Microsoft Learn: Build skills that open doors in your career. URL: https://learn.microsoft.com/en-us/compliance/regulatory/offering-iso-27001 (дата звернення: 09.10.2023).

3. What is ISO 27001? A detailed and straightforward guide. 27001Academy. URL: https://advisera.com/27001academy/what-is-iso-27001/ (дата звернення: 09.10.2023).

4. Songer A. ISO 27001: Pros and Cons. Austin Songer. URL: https://www.songer.pro/iso-27001-pros-and-cons/(date of access: 09.10.2023).

УДК 004.056, 004.75

С.В. Науменко[1,2], І.О. Розломій[1], П.В. Михайловський[1,2]
naumenko.serhii1122@vu.cdu.edu.ua, inna-roz@ukr.net, tatiana_ami@vu.cdu.edu.ua
[1]Черкаський національний університет ім. Б. Хмельницького,м. Черкаси
[2]Active Bridge, м. Черкаси

ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В SMART-ІМПЛАНТАХ: РОЛЬ ПОЛЕГШЕНОЇ КРИПТОГРАФІЇ

Сучасний динамічний ландшафт медичних технологій поклавши початок революції в медичних практиках і концепції «Smart-здоров'я». Однією з ключових складових цієї революції є смарт-імпланти – інноваційні медичні пристрої, які вбудовуються в організм пацієнта для моніторингу стану здоров'я та здійснення медичних втручань. Медичні smart-імпланти мають вбудовані електронні компоненти, які дозволяють здійснювати різноманітні функції [1].

Зазвичай smart-імпланти мають вбудовані сенсори, що дозволяють збирати дані про фізіологічні показники пацієнта або інші параметри здоров'я. Ці дані можуть передаватися безпосередньо до лікарів або медичних систем за допомогою бездротових технологій для моніторингу та аналізу [2].

Проте разом з великими можливостями, що відкриваються завдяки smart-імплантам, виникають і нові виклики, серед яких одним з основних є проблема забезпечення кібербезпеки цих інноваційних медичних пристроїв. Завдяки підключенню до мереж Інтернету речей (IoT), smart-імпланти стають об'єктами можливих кібератак, а це може мати серйозні наслідки для здоров'я і навіть життя пацієнтів.

Актуальність даного дослідження визначається контекстом зростаючої ролі smart-імплантів у медичних технологіях та зростаючою загрозою кібербезпеці в цій області.

Smart -імпланти стають необхідними для вдосконалення діагностики, лікування та моніторингу стану пацієнтів, і їх застосування широко впроваджується в медичну практику. Однак разом з перевагами smart-імплантів з'являються нові виклики у сфері кібербезпеки, зокрема в ризику доступу до медичних даних зловмисниками.

Забезпечення безпеки smart-імплантів має вирішальне значення для захисту особистої інформації пацієнтів та запобігання можливим кібератакам, які можуть призвести до серйозних наслідків для життя та здоров'я. Тому дослідження ролі полегшеної криптографії в забезпеченні кібербезпеки smart-імплантів є актуальним і важливим завданням, оскільки воно визначає можливість подолання цих викликів та зроблення smart-імплантів більш захищеними і надійними для користувачів та медичних фахівців.

Роль полегшеної криптографії в процесі захисту інформації в smart-імплантах є визначальною для забезпечення конфіденційності, цілісності та доступності даних, зберіганих та передаваних через ці медичні пристрої [3].

У порівнянні зі складними алгоритмами шифрування, які вимагають значних обчислювальних ресурсів, полегшені криптоалгоритми, такі як легкі блочні шифри або потокові шифри, використовують менше ресурсів і можуть бути більш практичними для smart-імплантів. Для забезпечення безпеки інформації на IoT smart-імплантах, особливо в умовах обмежених обчислювальних ресурсів, використовуються полегшені алгоритми шифрування. Ці алгоритми забезпечують високий рівень конфіденційності та дозволяють захищати дані від несанкціонованого доступу. Зокрема для захисту даних імплантованих медичних пристроїв використовуються такі полегшені алгоритми шифрування:

1. AES-CCM (Advanced Encryption Standard with Counter with CBC-MAC) – популярний полегшений алгоритмом шифрування, який використовує блок шифрування Advanced Encryption Standard (AES) разом з режимом рахівника (Counter) і аутентифікацією на основі коду перевірки цілісності (CBC-MAC). Він надає надійний захист і є ефективним для застосування в обмежених ресурсах [4].
2. ChaCha20-Poly1305 – це сучасний асиметричний потоковий шифр та метод аутентифікації на основі пароля (AEAD), який базується на двох основних операціях. Одна з операцій – ChaCha20. Цей потоковий шифр використовується для шифрування та розшифрування даних. Він базується на операціях зведення в роботу та виключення і забезпечує високу швидкість обробки даних (1).

$$\text{ChaCha20(key, nonce, counter, block)} \rightarrow \text{keystream} \quad (1)$$

Інша операція – Poly1305. Ця аутентифікаційна функція використовується для забезпечення цілісності даних та аутентифікації повідомлень. Вона використовує ключ і повідомлення для генерації коду аутентифікації (MAC), який додається до шифрованого повідомлення (2).

$$\text{Poly1305(key, message)} \rightarrow \text{MAC} \quad (2)$$

3. Serpent – це симетричний блок-шифр, який був створений з метою забезпечення високого рівня безпеки при шифруванні інформації. Цей алгоритм шифрування відомий своєю надійністю і високим ступенем стійкості до різних видів атак [5].

Роль алгоритму Serpent для інформаційної безпеки IoT смарт-імплантів полягає в тому, щоб забезпечити конфіденційність даних, які передаються між смарт-імплантами та зовнішніми системами. У зв'язку з обмеженими обчислювальними ресурсами смарт-імплантів, важливо використовувати шифри, які можуть

забезпечити надійний захист даних, не створюючи занадто великого обчислювального навантаження. Алгоритм Serpent відповідає цим вимогам завдяки своїй надійності та можливості працювати на різних обчислювальних платформах. Він забезпечує дуже високий рівень безпеки, що робить його привабливим вибором для захисту інформації в смарт-імплантах.

4. Blowfish – є симетричним блок-шифром, який був розроблений для шифрування та дешифрування інформації. Він базується на мережі Фейстеля, яка включає в себе послідовні раунди операцій перестановки та заміни даних [3]. Основні обчислення в алгоритмі Blowfish включають в себе такі операції: розширення ключа (Key Expansion), заміна байта (Substitution), перестановка байтів (Permutation). Для початкового ключа генерується велика кількість раундових ключів. Цей процес базується на перетвореннях ключа та функціях заміни, що виконуються послідовно та ітеративно. В алгоритмі Blowfish використовується таблиця заміни для заміни байтів відкритого тексту на шифрований текст та навпаки. Дані розбиваються на підблоки, які потім переставляються та обробляються певними логічними операціями.

Алгоритм Blowfish відомий своєю ефективністю та відмінною швидкістю обробки даних. Він також володіє досить високим рівнем безпеки та застосовується для шифрування даних в різних сферах, включаючи інформаційну безпеку IoT пристроїв. Він володіє гнучкістю щодо розміру ключа і блоку, що робить його практичним для різних застосувань.

5. Elliptic Curve Cryptography (ECC) – це сучасний криптографічний метод, який використовується для забезпечення конфіденційності, цілісності та аутентифікації даних в різних областях інформаційної безпеки, включаючи криптовалютні системи, безпеку мережі та комунікацій, а також інші області.

Нижче наведена порівняльна таблиця полегшених алгоритмів шифрування для забезпечення конфіденційності даних smart-імплантів системи IoT.

Таблиця 1

Порівняльна таблиця полегшених алгоритмів шифрування

Алгоритм	Тип	Довжина ключа	Рівень безпеки	Ефективність
AES-CCM	Блочний	128 бітів	Високий	Висока
ChaCha20-Poly1305	Потоковий	256 бітів	Високий	Висока
Serpent	Блочний	128, 192 або 256 бітів	Дуже високий	Середня
Blowfish	Блочний	32-448 бітів	Високий	Висока
ECC	Еліптична крива	Залежить від ключа	Дуже високий	Висока

З цієї таблиці видно, що алгоритм ECC (Еліптична крива) має дуже високий рівень безпеки, що робить його відмінним вибором для захисту інформації в IoT, включаючи медичні смарт-імпланти. Його ефективність також висока, і він може працювати на різних апаратних платформах, що робить його популярним вибором для пристроїв з обмеженими ресурсами.

Рростаюча кількість смарт-імплантів в сучасній медицині створює важливу необхідність забезпечення захисту від потенційних кібератак, які можуть негативно вплинути на здоров'я та безпеку пацієнтів. Застосування криптографічних методів при проектуванні смарт-імплантів може значно знизити ризик несанкціонованого доступу та зловживання, забезпечуючи високий рівень захисту та конфіденційності для пацієнтів, що використовують такі медичні технології.

Список літератури

1. Sametinger, J., Rozenblit, J., Lysecky, R., & Ott, P. (2015). Security challenges for medical devices. Communications of the ACM, 58(4), 74-82.

2. Camara, C., Peris-Lopez, P., & Tapiador, J. E. (2015). Security and privacy issues in implantable medical devices: A comprehensive survey. Journal of biomedical informatics, 55, 272-289

3. Naru, E. R., Saini, H., & Sharma, M. (2017, February). A recent review on lightweight cryptography in IoT. In 2017 international conference on I-SMAC (IoT in social, mobile, analytics and cloud)(I-SMAC) (pp. 887-890). IEEE

4. Rana, M., Mamun, Q., & Islam, R. (2022). Lightweight cryptography in IoT networks: A survey. Future Generation Computer Systems, 129, 77-89.

5. Thakor, V. A., Razzaque, M. A., & Khandaker, M. R. (2021). Lightweight cryptography algorithms for resource-constrained IoT devices: A review, comparison and research opportunities. IEEE Access, 9, 28177-28193.

УДК 004.056

М.О. Ємець[1], Н.С.Петляк[1]
m.iemets@khmnu.edu.ua, npetlyak@khmnu.edu.ua
[1]*Хмельницький національний університет, м. Хмельницький*

ВИЯВЛЕННЯ ЗЛОВМИСНИКА В ПУБЛІЧНІЙ МЕРЕЖІ НА ОСНОВІ АНАЛІЗУ ВИХІДНИХ DNS-ЗАПИТІВ НЕЙРОННОЮ МЕРЕЖЕЮ

Однією з основних причин зростання кібератак є доступність технологій та інтернет-з'єднання для широкого кола людей і організацій. Загальнодоступні комп'ютерні мережі дозволяють користувачам легко підключатися до мережі Internet без обмежень. Але це також означає, що кіберзлочинці можуть використовувати анонімність і прихованість для виконання атак. Тому актуальним є питання аналізу дій користувачів у відкритих сегментах комп'ютерних мереж [1-2].

Статистичні дані різних організацій свідчать про те, що кількість атак які реалізуються за допомогою DNS-запитів суттєво зросла у 2022 році. Тому варто приділити особливу увагу аналізу саме DNS-запитів у публічних мережах [3].

Проведений аналіз наявних систем виявлення та запобігання вторгненням ефективно працює щодо різного роду загроз, проте вони націлені на захист системи від стороннього несанкціонованого впливу та не орієнтовані на аналіз роботи в середині мережі. А розгортання таких систем є дорогим та потребує наявності фахівця, що не доцільно для публічних мереж [4].

З метою виявлення зловмисних дій користувачами в публічній мережі стосовно ресурсів, що знаходяться поза мережею розроблено метод виявлення зловмисника на основі аналізу вихідних DNS-запитів. Послідовність роботи методу наступна:

1. отримання маршрутизатором DNS-запиту;
2. передача DNS-запиту на аналізатор;
3. аналіз DNS-запиту CNN-мережею;
4. передача отриманих результатів на LSTM шар;
5. формування висновку про пропуск/блокування пакету з DNS-запитом;
6. модифікація налаштувань маршрутизатора для дозволу або блокування запитів від користувача.

Вищеописаний метод реалізується за допомогою системи аналізу трафіку, яка у мережі буде знаходитися на одному рівні із DNS-сервером, щоб маршрутизатор зміг одночасно транслювати запити до сервера та системи. Схематично комп'ютерну мережу зображено на рис.1.

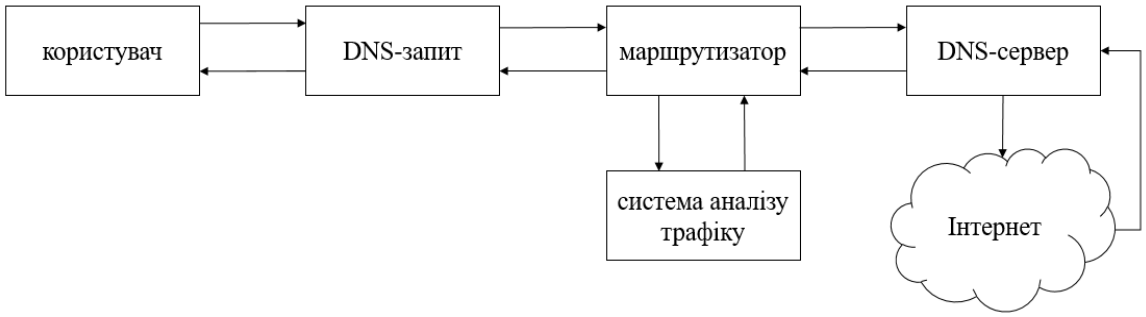


Рис. 1. Комп'ютерна мережа із під'єднаною системою аналізу трафіку

З метою дослідження ефективності запропонованого методу було розгорнуто локальне тестове середовище, що відокремлене від інших мереж та не становить небезпеки при запуску атак чи інших зловмисних дій. До проведення дослідження всі нейромережі були навчені та протестовані за допомогою набору даних KDD Kup 99, що широко використовується в дослідженнях і експериментах для розробки та оцінки систем виявлення вторгнень, а також для тестування алгоритмів машинного навчання. Вхідні дані одночасно надходили на три нейронні мережі: CNN, LSTM, CNN-LSTM. Схематично реалізацію підключення нейромереж зображено на рис.2. Далі відбувався аналіз запитів та виведення результатів роботи.

Під час експерименту було запущено 10 000 пакетів: 6 000 – безпечні, 4 000 – небезпечні. Дані експериментальних досліджень представлено у таблиці 1, де: TP – кількість пакетів, що визначено як зловмисні і вони дійсно такими є; TN – кількість пакетів, що визначено як нормальні і вони таким є; FP – кількість пакетів, що визначено як зловмисні, але вони не є такими; FN – кількість пакетів, що визначено як дозволені, але є зловмисними.

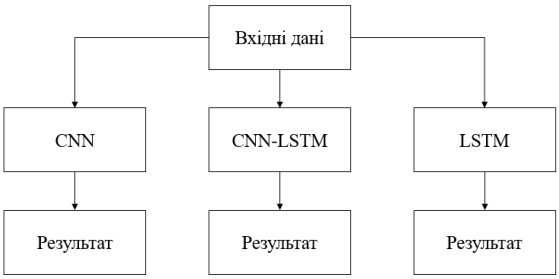


Рис. 2. Схема підключення нейромереж у системі

Таблиця 1
Дані експериментальних досліджень

	TP	TN	FP	FN
CNN	5640	3630	370	360
LSTM	5720	3580	420	280
CNN-LSTM	5840	3740	260	160

На основі даних із таблиці 1 було проведено розрахунки щодо метрик ефективності за трьома нейронними мережами. Точність дозволяє визначити, наскільки система правильно класифікує об'єкти або події як зловмисні без зайвих помилок та обчислюється як TP/(TP+FP). Акуратність вказує на загальну точність системи виявлення та рахується за формулою (TP+TN)/(TP+FP+FN+TN). Помилка вказує на здатність системи уникати хибних спрацьовувань, обчислюється як (FP+FN)/(TP+FP+TN+FN). F-метрика дозволяє врахувати FP та FN, обчислюється як середнє значення між точністю і повнотою. Результати відображено на рис.3.

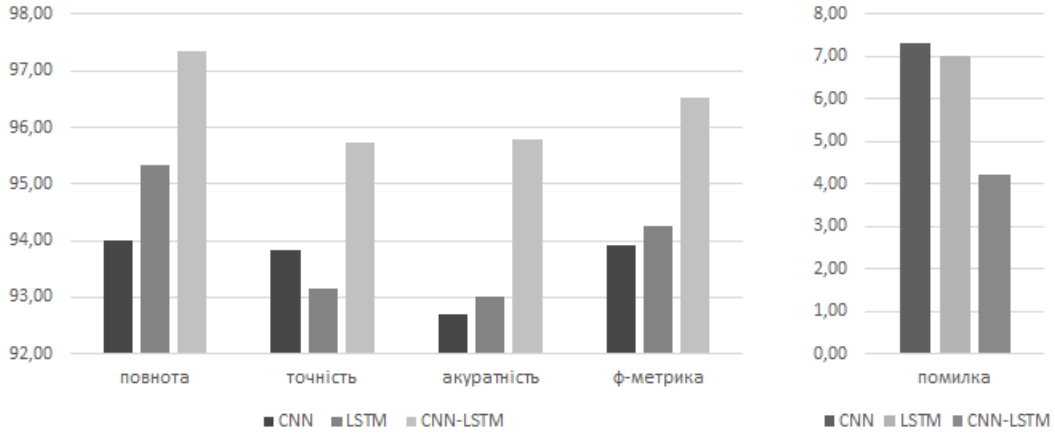


Рис. 3. Порівняння результатів метрик ефективності під час експерименту роботи нейронних мереж CNN, LSTM та CNN-LSTM

На основі отриманих даних можна зробити висновок, що поєднання CNN та LSTM мереж призвело до суттєвого покращення при роботі з DNS-запитами задля виявлення зловмисних дій у публічному сегменті мережі в порівнянні з роботою лише CNN чи лише LSTM мереж. Показник точності сягає 95,74% при F-метриці 96,54% та 4,2% помилок.

Список літератури

1. Козюра В. Д., Хорошко В. О., Шелест М. Є., Ткач Ю. М., Балюнов О.О. Захист інформації в комп'ютерних системах: підручник. – Ніжин: ФОП Лук'яненко В.В., ТПК «Орхідея», 2020. – 236с.

2. Шматок О.С, Фіненко Ю.І, Єлізаров А.Б, Телющенко В.А. Класифікація загроз і ризиків сучасних інфокомунікаційних систем. Вісник Університету «Україна». Серія: інформатика, обчислювальна техніка та кібернетика, № 2 (23), 2019, 221-229

3. T. Radivilova, L. Kirichenko, D. Ageiev and V. Bulakh, "Classification Methods of Machine Learning to Detect DDoS Attacks," 2019 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), Metz, France, 2019, pp. 207-210, doi: 10.1109/IDAACS.2019.8924406.

4. А. Шевченко, Г. Застело, Є. Шпачинський, Аналіз застосування методів машинного навчання на основі штучних нейронних мереж для виявлення кіберзагроз, Information Technology and Security. January-June 2019. Vol. 7. Iss. 1 (12) DOI 10.20535/2411-1031.2019.7.1.184327

УДК 004.056

Н.В. Дженюк[1], М.Ю. Толкачов[1]
natalidzh16@gmail.com, maksymtolkachov@gmail.com
[1]Національний технічний університет «Харківський політехнічний інститут»,м. Харків

ФОРМУВАННЯ КЛАСИФІКАТОРА ЗАГРОЗ НА ОСНОВІ КОМПЛЕКСУВАННЯ ІЗ ЗАГРОЗАМИ МЕТОДІВ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ

розвитком Інтернету речей і соціальних мереж генерується великий обсяг даних. Методи соціальної інженерії об'єднуються з кібератаками, зі змішаними та цільовими атаками. У зв'язку з цим з'являється гібридність цільових атак. Потрібен комплексний, багаторівневий підхід, який, крім того, розв'язує завдання захисту від впливу цільових атак, пов'язаних із різними соціальними групами в суспільстві. Необхідна композиційна структура захисту. Цей захист має об'єднувати функціональні елементи систем для реалізації властивостей системного рівня, які не можуть бути досягнуті шляхом інтеграції локальних властивостей компонентів системи [1].

Метою роботи є створення багатоконтурної системи безпеки в соціокіберфізичних системах з урахуванням комплексування кіберзагроз із загрозами на основі соціальної інженерії, а також моделі безпеки інформаційних взаємодій. Такий підхід дає змогу забезпечити синергію систем безпеки між функціональними елементами систем безпеки та забезпечити реалізацію властивостей системного рівня, що не можуть бути досягнуті шляхом інтеграції локальних властивостей компонентів системи захисту.

Для формування загрози необхідно розуміти, які шаблони процесів впливу слід застосовувати для тих чи інших агентів для аналізу та виділення загрози. Це положення можна розглядати як базовий принцип побудови моделі багатоаспектної структури в SCPS.

Одне із завдань, яке необхідно розв'язати для досягнення мети роботи, є формування класифікатора загроз з урахуванням загроз на основі методів соціальної інженерії та багатоконтурності систем захисту інформації. Запроваджено класифікацію загроз на основі соціальної інженерії, що дасть змогу підвищити рівень об'єктивності можливих соціальних загроз і забезпечити синергію при формуванні динамічної моделі формування систем безпеки та сформувати основні фази їх комплексування з цільовими атаками та сформувати уніфікований класифікатор загроз. При цьому враховуються аспекти багатоконтурності соціокіберфізичних систем, їх багатоплатформеність і синтез різних технологій.

Для формального опису математичного апарату кібернетичної моделі загроз використовується підхід, що дасть змогу сформувати об'єктивну оцінку загроз з ознаками синергізму та гібридності в багатоконтурних системах – соціокіберфізичних системах [2].

Для забезпечення безпеки всієї системи захисту необхідно враховувати загрози внутрішнього та зовнішнього контурів за кожною з платформ з урахуванням їхнього комплексування із загрозами на основі методів соціальної інженерії:

– загрози внутрішнього контуру з урахуванням гібридності та синергізму загроз для 1 платформи – соціальні мережі, для 2 платформи – кіберпростір, для 3 платформи – кіберфізичні системи;

– загрози зовнішнього контуру з урахуванням гібридності та синергізму для 1 платформи – соціальні мережі, для 2 платформи – кіберпростір, для 3 платформи – кіберфізичні системи.

Крім цього, враховується багатоконтурність соціокіберфізичних систем, їх багатоплатформеність та інтегрованість її складових елементів. Такий підхід дає змогу уніфікувати не тільки побудову класифікатора загроз, а й забезпечити комплексну оцінку цільових атак на основі емерджентних властивостей комплексованого формування атак.

Запропоновано класифікацію загроз на основі методів соціальної інженерії, яка дає змогу сформувати уніфікований, об'єктивний класифікатор загроз з урахуванням ознак їхньої гібридності та синергізму. Такий підхід дозволяє забезпечити формування комплексної оцінки цільових (змішаних) атак на соціокіберфізичні системи з урахуванням побудови багатоконтурних систем захисту інформації.

Список літератури

1. Horváth, I., Rusák, Z., & Li, Y. (2017). Order beyond chaos: introducing the notion of generation to characterize the continuously evolving implementations of cyberphysical systems. In Volume 1: 37th computers and information in engineering conference (p. V001T02A015). ASME. 10.1115/DETC2017-67082.

2. O. Korol, and other. DEVELOPMENT OF METHODOLOGICAL FOUNDATIONS FOR A CLASSIFIER OF THREATS TO CYBERPHYSICAL SYSTEMS DESIGN. Eastern-European Journal of Enterprise Technologies – 3/9 (105) – 2020, – P. 6–19.

УДК 004.056, 004.75

В.О. Дюльдєв[2], М.Г. Пожидаєв[1], Є.А. Просветов[1]
fludit1@gmail.com, maxim.pozhidaev23@gmail.com, aboutlight41@gmail.com
[1]*Національний технічний університет «Харківський політехнічний інститут», м. Харків*

ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ В БЕЗДРОТОВИХ ПРОТОКОЛАХ НА ПРИКЛАДІ LORAWAN

Забезпечення базового рівня безпеки даних в бездротових мережах, що використовуються в IoT-пристроях, можна розглядати на прикладі протоколу LoRaWAN.

LoRaWAN обрано для аналізу з кількох причин. По-перше, цей стандарт відзначається докладною документацією та широким сприйняттям в галузі. Це робить його важливим джерелом для визначення найкращих практик, якщо ви розробляєте власний бездротовий протокол. По-друге, LoRaWAN є типовим рішенням для IoT та має специфіку, яка важлива для більшості розробників. Вивчення захисту даних у контексті Wi-Fi або LTE може бути корисним, але, ймовірно, не варто витрачати ресурси на розробку власних реалізацій цих протоколів. По-третє, слабопотужні IoT-пристрої, які мають обмежені ресурси, часто вразливі, і LoRaWAN надає приклад того, як економити байти та захищатися від можливих атак (Рис. 1).

Рис. 1 Обмін повідомленнями в мережі LoRaWAN між сервером і пристроєм

Незважаючи на те, що схема обміну повідомленнями в мережі LoRaWAN на зображенні виглядає досить простою, простота обманлива, оскільки за нею стоїть значна кількість роботи, де кожен елемент цієї схеми має своє важливе призначення.

Розглянемо це на прикладі LoRaWAN 1.0.2, будемо аналізувати можливі загрози.

Перша основна загроза, яку варто розглянути, - це перехоплення користувацьких даних. Завдяки тому, що радіохвилі поширюються неконтрольовано, будь-яка особа може взяти приймач, налаштований на відповідний діапазон і тип модуляції, і прослуховувати всі передавані дані. Однак простий спосіб захисту від цієї загрози - це шифрування даних.

У LoRaWAN користувацькі дані шифруються за допомогою алгоритму AES-128 з ключем довжиною 128 бітів (16 байтів). AES є надійним алгоритмом, і навіть на мікроконтролерах з обмеженими обчислювальними ресурсами його використання не вимагає значних накладних витрат. Навіть на таких мікроконтролерах, як Cortex-M3 з частотою 48 МГц, один 16-байтовий блок шифрується приблизно за 100 мікросекунд "з нуля".

Друга загроза, яку варто розглянути, - це повторення даних. Іноді зловмиснику навіть не потрібно знати конкретний вміст передаваних даних. Наприклад, якщо у вас є датчик закритого вікна, який передає однакові дані, коли вікно відкрите, і інші дані, коли воно закрите, то зловмиснику можна просто записати і повторити "закрите" повідомлення, не глибоко аналізуючи їх вміст. У LoRaWAN до кожного пакету додається лічильник. Якщо на сервер мережі надходить пакет з лічильником, рівним або меншим за попередній, то цей пакет просто відкидається. Завдяки двом байтам на лічильник і типовому для систем IoT темпу передачі повідомлень, лічильник вистачить на дуже тривалий час.

ВІДСТЕЖЕННЯ ПОСТІЙНИХ ДАНИХ

Відстеження даних є завданням важливим для збереження безпеки та конфіденційності інформації. У багатьох ситуаціях небажано, щоб незаконні користувачі мали можливість зрозуміти або відтворити дані. Один із способів досягнення цього полягає в тому, щоб незаконний користувач міг розпізнати, що дані залишаються незмінними, але не міг отримати доступ до самого вмісту.

Для досягнення цієї мети використовується шифрування даних. Отже, однакові дані, зашифровані одним і тим же ключем, завжди виглядають однаково. Якщо ми отримуємо зашифровані дані від джерела, де дані не змінюються, ми можемо визначити цей факт, не розшифровуючи самі дані.

У LoRaWAN застосовується ускладнена схема. Реалізовується вона шляхом шифрування лічильника пакетів та інформацію про пристрій та пакет по алгоритму AES. Результат шифрування XORиться разом із пакетом даних користувача. Перевагою є те, що байти корисного навантаження не губляться марно, а кожне повідомлення виглядає інакше незалежно від того, чи змінювалася навантаження.

IoT характеризується застосуванням великої кількості пристроїв , та в такому випадку доволі складно мати достатній контроль, і тому якщо всі пристрої будуть мати один і той самий ключ шифрування, то власник будь-якого з них може вільно відслідковувати трафік іншого пристрою. Через це зловмисникам можна набагато легше отримати ключ шифрування.

У LoRaWAN реалізовано дві схеми використання ключів, які є унікальними для кожного пристрою:

• Over The Air Activation, OTAA — ключі генеруються сервером мережі щоразу, коли пристрій у ній реєструється

• Activation By Personalization — ключі, задані виробником і зберігаються на пристрої, ніколи не змінюючись

Зазвичай використовуються мінімум два ключі, а саме — AppSKey, яким шифруються дані користувача, і NwkSKey, яким підписується повідомлення.

ПЕРЕХОПЛЕННЯ ЗГЕНЕРОВАНИХ КЛЮЧІВ

При реєстрації в мережі генеруються нові ключі. Їх щоразу необхідно синхронизовувати між пристроєм і сервером, що само собою означає потенційну загрозу перехоплення їх зловмисником. Тому пристрої LoRaWAN мають третій ключ — AppKey, зашитий у пристрій і використовується в один-єдиний момент: при реєстрації в мережі. З його допомогою підписується обмін сесійними ключами між пристроєм та сервером. У зв'язку із обмеженою кількістю використань, це може бути визнано допустимим.

AppKey перед підключенням пристрою заноситься до його налаштування на сервері мережі. Отже, пристрій формує запит на реєстрацію (JoinRequest), не шифруючи його, але підписуючи його ключем AppKey. Сервер мережі, отримавши цей пакет і перевіривши адресу відправника та підпис, відповідає пакетом JoinAccept, в якому передає налаштування мережі – підтвердженням реєстрації. Ключи до AppSKey та NwkSKey формуються шляхом шифрування AES-128 із ключем AppKey з переданого сервером у відповіді випадкового числа AppNonce, номера ключа (1 або 2), ID мережі та ще одного випадкового числа DevNonce:

NwkSKey = aes128_encrypt(AppKey, 0x01 | AppNonce | NetID | DevNonce)
AppSKey = aes128_encrypt(AppKey, 0x02 | AppNonce | NetID | DevNonce)

Оскільки і пристрій, і сервер після обміну пакетами реєстрації знають ці параметри, всі вони згенерують однакові ключі. Таким чином, жодні ключі передаватися не будуть, але при цьому пристрій і сервер отримають унікальні ключі шифрування та підписи пакетів.

ПЕРЕХОПЛЕННЯ ПОТОКУ ДАНИХ НА СЕБЕ

У доволі рідкісних випадках стається подія реєстрації в мережі, ініційована та перехоплена зловмисником. Якщо ним буде надісланий записаний пакет JoinRequest, нічого в ньому не змінюючи, сервер відповість на нього пакетом JoinAccept, згенерувавши нові ключі. Після цього атакований пристрій перестане спілкуватися з сервером, адже він JoinRequest не ініціював, і жодних підстав оновлювати ключі не бачить. Зловмисник не зможе підробити дані, тому що для цього потрібно знати ключі, а для їх отримання потрібно знати AppKey, який він не знає. Але вибити пристрій із мережі зможе. Щоб уникнути цього, при реєстрації пристрій передає на сервер випадкове число DevNonce. Крім того, що на його базі генеруються ключі, воно є ще однією метою - сервер LoRaWAN зберігає архів DevNonce. Якщо від пристрою надійшов повторний запит реєстрації з уже використаним DevNonce, сервер просто проігнорує. У свою чергу, пристрій зобов'язаний при кожній реєстрації генерувати новий DevNonce.

Висновок: У підсумку, важливо розуміти, що бездротові мережі, такі як LoRaWAN, можуть бути піддані різним загрозам, і вирішення питань безпеки вимагає обережності і врахування всіх можливих ризиків.

УДК 004.05

В.В.Кіш, Н.І.Йовбак
kish.viktor@student.uzhnu.edu.ua, yovbak.nika@student.uzhnu.edu.ua
ДВНЗ »Ужгородський національний університет», м.Ужгород

ЗАХИСТ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ СИСТЕМАХ ТА МЕРЕЖАХ

Захист інформації в комп'ютерних системах та мережах є однією з найбільш важливих сфер сучасної інформаційної технології. Із зростанням кількості даних, що обробляються та передаються в цифровому середовищі, зростає і загроза їх незаконному доступу та зловмисному використанню. Тому забезпечення безпеки інформації стає ключовим завданням для організацій, користувачів та розробників.

Однією з основних складових захисту інформації є **криптографія.** Вона використовується для шифрування даних, забезпечуючи їх конфіденційність та цілісність. Сучасні алгоритми шифрування, такі як AES, RSA та інші, забезпечують надійний захист від несанкціонованого доступу до даних.

Файрволи та системи виявлення вторгнень (IDS) грають важливу роль у захисті мережевого трафіку. Файрволи фільтрують та контролюють трафік, дозволяючи лише дійсним користувачам отримувати доступ до мережі, тоді як IDS виявляють незвичайну активність або потенційні загрози.

Іншою важливою аспект захисту є аутентифікація та авторизація. Системи паролів, біометричні методи та двофакторна аутентифікація допомагають підтвердити ідентичність користувачів та надати їм доступ лише до необхідних ресурсів.

Серед інших важливих практик варто відзначити регулярне оновлення програмного забезпечення та вчасну реакцію на виявлені уразливості, а також навчання користувачів правилам кібербезпеки.

Загалом, захист інформації в комп'ютерних системах та мережах вимагає комплексного підходу та постійного моніторингу, оскільки загрози постійно змінюються та розвиваються. Тільки завдяки цим заходам можна забезпечити надійний захист важливих даних та зберегти конфіденційність у цифровому світі.

Розглянемо більш детально загрози, з якими стикаються комп'ютерні системи та мережі. Однією з основних загроз є атаки на мережевий рівень, такі як DDoS (розподілений деніальний сервіс) атаки, які спрямовані на перевантаження мережі та заваду нормальному функціонуванню. Важливим є вчасне виявлення таких атак і розробка заходів для їх запобігання.

Соціальна інженерія є ще однією загрозою, коли зловмисники намагаються отримати доступ до інформації, використовуючи маніпуляцію та обман користувачів. Освіта та свідомість користувачів грають ключову роль у захисті від таких атак.

У світі віртуальних атак не менш важливим є резервне копіювання даних та планування для відновлення в разі втрати інформації через кіберінциденти. Регулярні резерви, а також тестування планів відновлення, гарантують, що організація може швидко відновити доступ до даних у разі потреби.

Завершуючи, захист інформації в комп'ютерних системах та мережах є постійним завданням, яке вимагає узгодженого підходу, інноваційних рішень та уваги до нових загроз. Тільки так можна забезпечити надійну інформаційну безпеку в світі, де обмін даними стає все більш важливим для розвитку суспільства та господарства.

Загрози та методи атак на інформацію в комп'ютерних системах та мережах постійно змінюються та розвиваються. Ось кілька додаткових аспектів, які важливо враховувати в контексті захисту інформації:

- **Малвар та віруси:**

Шкідливе програмне забезпечення, таке як троянці, віруси та шпигунське ПЗ, може ширитися через інтернет, електронну пошту чи навіть під час завантаження програм. Важливо мати актуальний антивірус та антишпигунське ПЗ для виявлення та блокування цих загроз. Обмеження прав доступу: Встановлення обмежень щодо того, хто має доступ до конфіденційних даних і ресурсів, є ключовим аспектом захисту інформації. Правильна управління доступом та ролева модель допомагають зменшити ризик несанкціонованого доступу.

- **Моніторинг та журналювання:**

Ведення журналів подій та постійний моніторинг дозволяють виявити незвичайну активність та вразливості у реальному часі, що дає можливість реагувати швидко на потенційні загрози.

- **Захист фізичного доступу:**

Фізичний доступ до серверів та комп'ютерів також важливо захищати. Це може включати в себе застосування біометричних систем, контроль доступу і системи відеоспостереження.

- **Захист від внутрішніх загроз:**

Іноді загрози можуть виникнути внаслідок недбалості або зловмисних дій власних співробітників. Важливо мати політики та процедури для внутрішнього контролю та моніторингу діяльності персоналу.

Загалом, захист інформації вимагає поєднання технічних заходів, правильних політик та освіти користувачів. Сучасна кібербезпека є постійною боротьбою, і розуміння актуальних загроз та використання найкращих практик є важливими кроками для забезпечення інформаційної безпеки.

Розглянемо додаткові аспекти захисту інформації:

- **Захист від внутрішніх загроз:**

Загрози можуть виникати не тільки ззовні, але і всередині організації. Інсайдерські загрози включають в себе дії власних співробітників, які можуть бути недбалими або намагатися завдати шкоду. Важливо мати політики та технічні рішення для виявлення та запобігання цим загрозам.

- **Захист від атак на програмне забезпечення:**

Вразливості в програмному забезпеченні можуть використовуватися зловмисниками для атак. Регулярне оновлення програмного забезпечення та виявлення вразливостей є важливими кроками для захисту.

- **Безпека Інтернету речей (IoT):**

За поширенням підключених пристроїв до мережі виникають нові загрози. Важливо забезпечити безпеку IoT-пристроїв, оскільки вони можуть стати точкою входу для атак.

- **Забезпечення безпеки мобільних пристроїв:**

Мобільні пристрої, такі як смартфони і планшети, стали невід'ємною частиною робочого процесу. Важливо застосовувати політики безпеки для мобільних пристроїв та даних, що на них зберігаються.

- **Навчання та свідомість користувачів:**

Освіта користувачів про правила кібербезпеки та небезпеки, пов'язані з соціальною інженерією, може допомогти запобігти багатьом атакам. Важливо надавати інструкції та навчати персонал користуватися технологією безпеки.

Ці аспекти разом утворюють повний спектр заходів, які можуть бути використані для ефективного захисту інформації в комп'ютерних системах та мережах.

Зважаючи на швидкий розвиток технологій і зростаючу складність загроз, розглянемо кілька нішевих аспектів захисту інформації:

- **Блокчейн і кібербезпека:**

Технологія блокчейн використовується для забезпечення безпеки та цілісності даних, зокрема в фінансовому секторі. Вона може застосовуватися для підтримки безпеки транзакцій та уникнення подій, які можуть вплинути на конфіденційність інформації.

- **Стійкість до відмов і відновлення:**

Побудова систем, які можуть продовжувати функціонувати під час відмов та відновлювати роботу після інцидентів, є важливим аспектом бізнес-контингентності та безпеки.

- **Кваліфіковані кадри в галузі кібербезпеки:**

Зростаючий попит на професіоналів у галузі кібербезпеки створює нові можливості для спеціалізації та розвитку кар'єри в цій області. Важливо інвестувати в навчання та сертифікацію, щоб забезпечити наявність кваліфікованих кадрів для захисту інформації.

Ці нішеві аспекти відображають важливі тенденції у галузі кібербезпеки та вказують на постійну необхідність адаптації та вдосконалення стратегій захисту інформації.

Отже, захист інформації в комп'ютерних системах та мережах є справжнім викликом в сучасному світі, де обмін даними став невід'ємною частиною життя організацій та осіб. Інформація стала важливим активом, і захист від зловмисників та загроз стає ключовим завданням. Для досягнення найвищого рівня захисту інформації необхідно враховувати багато аспектів. Важливо застосовувати сучасні методи криптографії для забезпечення конфіденційності та цілісності даних. Файрволи, системи виявлення вторгнень і контроль доступу допомагають виявляти та блокувати небезпечну мережеву активність. Загрози включають в себе атаки ззовні, такі як DDoS і соціальна інженерія, а також внутрішні загрози від інсайдерів. Політики безпеки та навчання користувачів грають важливу роль у запобіганні цим загрозам. Додаткові нішеві аспекти, такі як застосування блокчейну, квантової криптографії та аналізу великих даних, допомагають вдосконалити заходи захисту інформації в умовах постійно змінюючихся технологій та загроз. Усі ці аспекти вказують на те, що захист інформації - це складний та постійний процес, який вимагає поєднання технологічних рішень, правильних політик, навчання та свідомості користувачів. Тільки комплексний підхід може забезпечити надійний захист цінної інформації в цифровому світі.

Список літератури:

1. Гапак О.М. Захист інформації в комп'ютерних системах: підручник / О.М. Гапак, С.І. Балога. – Ужгород: ДВНЗ «УжНУ», 2021. – 184 с. URL: https://www.uzhnu.edu.ua/uk/infocentre/get/42935
2. https://www.forcepoint.com/cyber-edu/firewall
3. https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security
4. https://www.upguard.com/blog/the-role-of-cybersecurity-in-blockchain-technology
5. https://www.techtarget.com/iotagenda/definition/Internet-of-Things-IoT

УДК 004

Я.О. Козлов, Т.В. Смірнова , О.А.Смірнов
kozlov.yan1@gmail.com, sm.tetyana@gmail.com, dr.SmirnovOA@gmail.com
Центральноукраїнський національний технічний університет, м. Кропивницький

ДОСЛІДЖЕННЯ SIEM-СИСТЕМ ДЛЯ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

За даними Державної служби спеціального зв'язку та захисту інформації України, в складі якої функціонує CERT (англ. Computer Emergency Response Team – команда реагування на комп'ютерні надзвичайні події), кількість ворожих кібератак на Україну зросла втричі у порівнянні з 2021 роком. Під атаки підпадають як медіаресурси, так і об'єкти критичної інфраструктури [1]. Така тенденція підтверджує необхідність запровадження систем забезпечення кібербезпеки на організаційному та технічному рівні в уразливих установах.

Існує багато принципово різних рішень для захисту інформаційно-комунікаційних систем: мережеві екрани, системи виявлення та запобігання вторгненням, антивіруси; але лише їх недостатньо для вчасного реагування на загрози або шкідливі дії. На момент, коли спеціаліст виявить джерело порушень та можливі протидії – розмір шкоди може бути занадто великим. Саме для пришвидшення процесів, необхідних для захисту системи, створюються спеціальні операційні центри безпеки (англ. Security Operation Center), основним компонентом котрих є SIEM [1-5].

SIEM-системи стають зв'язуючою ланкою між іншими рішенням захисту, що дозволяє не просто зберігати усю безпекову інформацію в одному місці, але й тим самим збагачувати аналітику, контролювати стан усіх елементів системи та виявляти несанкціоновані дії у реальному часі.

Зі збільшенням кількості інформації, що оброблюється та передається між різноманітними інформаційно-комунікаційними системами, користувачі все більше покладаються на безперервність на надійність виконання відповідних процесів. Відповідно, зростає і кількість загроз у сфері кібербезпеки, починаючи від витоку конфіденційних даних закінчуючи атаками на критичну інфраструктуру. Незалежно від типу організації, вона потребує впровадження системи захисту інформаційно-комунікаційних систем, тож з'являється потреба аналізувати величезну кількість журналів аудиту безпеки та інших даних безпекового характеру. Ядром такої системи є SIEM-система (англ. Security Information and Event Management) – централізований хаб для обробки, аналізу безпекових даних та реагування на загрози до того як вони нанесуть певну шкоду. Сучасні SIEM-системи дуже гнучкі в аспекті інтеграції з іншими безпековими рішеннями: журнали безпекового аудиту робочих станцій, мережевого обладнання, IDS/IPS, мережеві екрани, хмарні середовища та ін. Централізація безпекових повідомлень та даних значно пришвидшує процес виявлення, аналізу та протидії загрозам, які мають місце у підконтрольній інформаційно-комунікаційній інфраструктурі. Більшість SIEM-систем надають можливість налаштовувати сценарії дій у випадках появи певних підозрілих записів, автоматично повідомляти про це спеціалістів, якщо певна налаштована умова виконалася, а деякі комерційні рішення навіть запроваджують машинне навчання для виявлення аномалій. непередбачених спеціалістами. Вбачаючи можливості та роль таких систем у забезпеченні та підтримці безпеки в інформаційно-комунікаційних системах, автори статті вважають доцільним порівняти основні рішення SIEM-систем та їхні перспективи запровадження в різноманітних організаціях.

Список літератури

1. Кількість кібератак під час війни зросла втричі. [Електронний ресурс]. Доступно: https://cip.gov.ua/ua/news/kilkist-kiberatak-pid-chas-viini-zrosla-vtrichi. Дата звернення: Вер. 27, 2023.

2. Billy K Leung, "Security Information and Event Management (SIEM) Evaluation Report", May 2021. [Online]. Available: https://scholarworks.calstate.edu/downloads/41687p49q. Accessed on: Sep. 28, 2023.

3. Gustavo González-Granadillo, Susana González-Zarzosa, Rodrigo Diaz. "Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures", July 12, 2021. [Online]. Available: https://www.mdpi.com/1424-8220/21/14/4759. Accessed on: October 3, 2023.

4. Muhammad Sheeraz, Muhammad Arsalan Paracha, Mansoor Ul Haque, Muhammad Hanif Durad, Syed Muhammad Mohsin, Shahab S. Band, Amir Mosavi. "Effective Security Monitoring Using Efficient SIEM Architecture", April 30, 2023. [Online]. Available on: http://hcisj.com/data/file/article/2023040003/13-17.pdf. Accessed on: October 3, 2023.

5. NIST. "Guide for Security-Focused Configuration Management of Information Systems", August, 2011. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-128.pdf. Accessed on: October 5, 2023.

УДК 004.056

М.М.Федух[1], Ю.П.Кльоц[1], Н.С.Петляк[1]
mfedukh@khmnu.edu.ua, klots@khmnu.edu.ua, npetlyak@khmnu.edu.ua
[1]Хмельницький національний університет, м. Хмельницький

ПІДХОДИ ДО КЕРУВАННЯ БЕЗПЕКОЮ МОБІЛЬНИХ ПРИСТРОЇВ В ЗАХИЩЕНИХ ПРИМІЩЕННЯХ

Використання сучасних мобільних пристроїв для обробки конфіденційної інформації обмежено через ряд суттєвих особливостей їх функціонування, таких як розміри, мобільність користувачів і багатофункціональність.

Ці характеристики визначають великий спектр потенційних загроз інформаційній безпеці, які відрізняються від тих, які існують при використанні стаціонарних обчислювальних засобів. Постійна зміна місцезнаходження користувачів мобільних пристроїв (МП), бездротовий дистанційний доступ до мереж з різними вимогами до захищеності, обмежені обчислювальні можливості з одного боку та високошвидкісні комунікаційні можливості з іншого створюють велику кількість загроз інформаційній безпеці, зокрема загрози порушення конфіденційності інформації.

Необхідно розробити універсальну систему захисту інформації, що забезпечуватиме конфіденційність при використанні МП. Основною метою цієї системи буде забезпечення безпеки інформації, коли користувачі отримують доступ до різних мереж з різними вимогами до захищеності за допомогою МП. Це досягатиметься за допомогою адаптивного управління безпекою МП через зміну його програмно-апаратної конфігурації, що дозволить адаптувати стан МП до параметрів доступу, вимог щодо безпеки корпоративної мережі та вимог до якості послуг, які надаються.

До основних принципів, які лежать в основі всіх методів визначення розташування, включаються:

– тріангуляція та трилатерація - методи оцінювання місцезнаходження на основі геометричних характеристик кутів, що вказують на об'єкт (тріангуляція), або відстаней від трьох або більше об'єктів з відомим місцезнаходженням (трилатерація);

– аналіз карти вимірів - метод базується на оцінці розташування, виходячи з карти точок вимірювань параметрів сигналу, що називається "картою сигнального простору";

– аналіз близькості здійснює визначення місця розташування на підставі того, наскільки близько об'єкт знаходиться до приймача сигналу в порівнянні з іншими об'єктами;

– аналіз динаміки руху: цей метод залежить від вивчення і врахування динаміки руху об'єкта, що допомагає визначити його розташування на основі змін в часі.

Ці принципи визначення розташування використовуються для різноманітних завдань і додатків, де точність і надійність визначення місцезнаходження є критичними факторами.

На рисунку 1 представлено порівняльний огляд технологій визначення розташування з урахуванням їх точності та застосування.

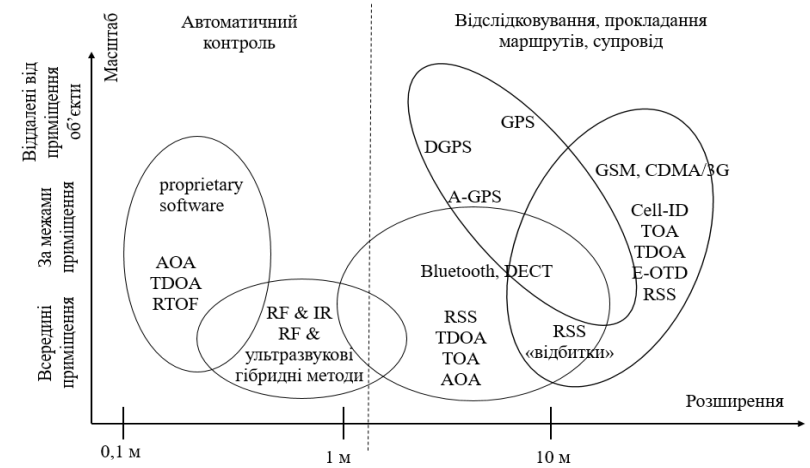


Рис. 1. Порівняння технологій визначення розташування

Технології супутникової навігації не можна використовувати всередині приміщень через значне пригнічення сигналу від супутників. Методи, що базуються на сигналах GSM/CDMA/3G/LTE, мають обмежену точність для вирішення завдань визначення місця розташування мобільних пристроїв (МП). Ультразвукові методи, радіочастотна ідентифікація (RFID), технології на основі волоконно-оптичних ліній зв'язку не дозволяють створити захищений канал управління для МП і, крім того, деякі з них не надають можливість ідентифікувати МП.

Для системи визначення розташування мобільних пристроїв встановлюються ряд вимог, виконання яких впливає на збереження конфіденційності інформації:

– точність визначення місця розташування повинна бути настільки високою, щоб можна було ідентифікувати конкретне приміщення, в якому перебуває користувач мобільного пристрою, і при цьому з мінімальною похибкою 2-го роду;

– ідентифікація користувача мобільного пристрою в системі визначення розташування повинна забезпечити можливість однозначно встановити особу, яка використовує мобільний пристрій, в контексті системи визначення розташування.

Завдання визначення місцезнаходження та завдання захищеної інформаційної взаємодії можуть бути вирішені за допомогою одного бездротового модуля стандарту 802.11, або можуть бути розділені на технологічно незалежні бездротові модулі. Для сигналів стандарту 802.11, розв'язання задачі визначення розташування може бути досягнуто за допомогою методів тріангуляції (трилатерації) та аналізу карти сигнального простору. Слід зауважити, що метод трилатерації не потребує попередніх вимірювань рівня сигналів мережі, що різко спрощує розробку, експлуатацію та підтримку системи. Проте, в той же час підсистеми розташування, побудовані на основі методу трилатерації, мають помітно меншу точність порівняно з системами, що використовують аналіз карти сигнального простору.

Як основні технології, які використовують бездротові мережі передачі даних для визначення місця розташування та для обґрунтування алгоритмічної складності запропонованого підходу до розрахунку ймовірності знаходження мобільного пристрою (МП) у спеціальному приміщенні, незалежно від обраного методу, запропоновано використовувати наступні технології:

– метод трилатерації сигналу МП: цей метод передбачає використання кількох точок доступу бездротових мереж для визначення місця розташування МП;

– метод k-найближчих сусідів: цей метод базується на аналізі найближчих сусідів для визначення місця розташування МП;

– метод, що використовує байєсівський підхід: цей метод використовує байєсівську ймовірність для визначення місця розташування МП;

– розв'язання задачі обчислення площі приміщень кожного рівня захищеності: це вимагає врахування наступних умов: конфігурація та розташування приміщень відомі заздалегідь; координати місця розташування МП та розташування кола, в межах якого може знаходитися МП, обчислюються відомими методами; конфігурація та розташування приміщень усередині даного кола мають геометричну форму довільної природи; максимальний радіус кола, в межах якого може знаходитися МП, залежить від використовуваної технології розташування і визначається максимальною помилкою розташування для даної технології, яку отримано емпірично.

У вищезазначених умовах застосування традиційного геометричного підходу для розрахунку площі фігур не є прийнятним. Це пояснюється, передусім, необхідністю визначення площі фігур довільної конфігурації в будь-який момент часу та урахуванням великої кількості можливих варіантів. Найбільш відповідним методом для визначення площі довільних фігур є статистичний метод, відомий як метод Монте-Карло. Цей метод дозволяє визначити площу довільної фігури, яка знаходиться всередині кола, що визначає ймовірне місцезнаходження мобільного пристрою, хоча може вимагати попереднього навчання. Попереднє навчання означає процес збору статистики помилок визначення місця розташування для конкретної технології. Ця статистика представляє собою розподіл значень помилок розташування і становить основу для проведення статистичних експериментів. Важливою частиною цього процесу є врахування помилки розташування як випадкової величини.

Застосування методу Монте-Карло для розрахунку ймовірності знаходження мобільного пристрою (МП) в спеціальному приміщенні у поєднанні з технологіями визначення розташування на базі бездротових мереж передачі даних дозволяє зменшити вплив нестійкості радіосигналів у бездротових мережах на похибку визначення місця розташування МП і підвищити надійність розрахунків ймовірності в спеціальному приміщенні в межах захищеної корпоративної мережі.

Тому обґрунтовано алгоритмічну реалізованість запропонованого підходу до обчислення ймовірності розташування мобільного пристрою (МП) в спеціальному приміщенні. Досліджено, що для підвищення точності визначення розташування МП цілком доцільно використовувати емпіричні дані щодо статистики помилок вимірювання місця розташування. При цьому межове значення критерію прийняття рішення про рівень захищеності приміщення, в якому знаходиться МП, повинно визначатися на основі вимог замовника і припустимих значень помилки другого роду. Для апробації моделі системи розташування було проведено імітаційне моделювання. Проведена комплексна оцінка якості цієї моделі, яка включала перевірку її адекватності, чутливості та стійкості. Також були отримані оцінки параметрів приватних моделей, що впливають на точність визначення розташування МП.

УДК 004.056, 004.75

М.І. Поломошнова,
кандидат економічних наук, студентка 5 курсу,
mariia.polomoshnova@gmail.com
науковий керівник: С.В. Мілевський
кандидат економічних наук, доцент кафедри кібербезпеки,
Національний технічний університет
«Харківський політехнічний інститут» м. Харків

ТЕОРЕТИКО-СУТНІСНА ХАРАКТЕРИСТИКА ПОНЯТТЯ "КІБЕРРИЗИК"

Кіберизики є реальною загрозою фінансовій системі країни, тому дослідження цих питань заслуговують на особливу увагу. Для ідентифікації теоретико-сутнісної характеристики поняття «Кіберризик» проаналізуємо особливості різних точок зору науковців та провідних міжнародних організацій, українських інституцій на цю проблему.

Слід звернути увагу на те, що в основних нормативно-правових документах чинного законодавства України правова дефініція поняття «Кіберризик» не визначена [1,2].

За результатами аналізу основних дефініцій поняття «Кіберризик», їх можна згрупувати за наступними ознаками (табл.1).

Таблиця 1.
Особливості визначення поняття «Кіберризик»

№ визначення	Вид ризику	Об'єкт ризику	Результат реалізації ризику	Вплив ризику
1 [3]	Операційний	Інформаційні та технологічні активи	Наслідки	Конфіденційність, доступність або цілісність інформації або інформаційних систем
2 [4]	Операційний	Інформаційні активи	Кіберзагрози	Збитки та/або додаткові втрати
3[5]	Операційний	Цифрові технології, що використовуються для інформаційних та/або операційних функцій, запроваджених у виробничу систему за допомогою електронних засобів	Несанкціонований доступ, використання, розголошення, збій, модифікація або руйнування виробничої системи	Фінансові втрати, збій у роботі чи збитки
4 [6]	Операційний	Кіберресурси	Кіберзагрози	Система або системні елементи, які існують у кіберпросторі або періодично присутні в ньому
5 [7, с.50]	Операційний	Інформаційні ресурси та/або інформаційна інфраструктура	Кіберзагрози	-
6 [8, с.82]	Операційний	Активи або інформація	Пошкодження, знищення або викрадення активів або інформації	Активи або інформація
7 [9]	Операційний	Інформаційні технології	Збій системи інформаційних технологій	Фінансові втрати, руйнування або шкоди репутації організації

Після об'єднання в групи за певними спільними ознаками наведених розрізнених дефініцій виникає необхідність проаналізувати розбіжності в кожній з цих груп задля окреслення особливостей кожної з них. В результаті здійснення відповідних процедур автором були сформульовані суттєві розбіжності концептуальних підходів щодо встановлення об'єктів ризику, його впливу та результатів реалізації ризиків. В свою чергу, за результатами аналізу виявлено спільні ознаки теоретико-сутнісної характеристики поняття «Кіберризик», а саме, щодо класифікації виду ризику. Слід також зазначити, що хоч думки авторів щодо об'єктів ризику суттєво різняться, проте в цілому всі автори вважають, що об'єкт кіберризику знаходиться в області інформаційних технологій. Слід також звернути увагу на те, що на думку більшості авторів результат реалізації кіберризику має завжди негативний вплив, що не в повній мірі корелює з загальною теорією управління ризиками про те, що ризику можуть мати різні наслідки (як негативні, так і позитивні). Деякі автори дещо звузили спектр можливих видів впливу кіберризику, наприклад, у визначенні №2 йде мова про збитки та/або додаткові втрати, хоча збитки є по суті однією з форм фінансових втрат; у визначенні №3 йде мова про фінансові втрати чи збитки, хоча збитки і є частиною фінансових втрат.

Щодо авторської точки зору, то всі вище зазначені визначення більш сконцентровані на фінансових втратах, проте більший вплив в сьогоднішніх реаліях мають саме нефінансові чинники (збій в роботі, шкода репутації, регуляторні санкції тощо).

Таким чином, за результатами проведеного аналізу автором сформульовано власне визначення поняття «Кіберризик» як будь-який ризик фінансових та/або нефінансових втрат, порушення безперервності діяльності організації, шкоди її репутації внаслідок некоректної роботи та/або збоїв в роботі інформаційної інфраструктури. Такий підхід до трактування даного феномену, на думку автора, більш точно розкриває особливості теоретико-сутнісної характеристики поняття «Кіберризик».

Список літератури

1. Про основні засади забезпечення кібербезпеки України: Закон України від 21 черв. 2018 р. №2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 19.10.2023).

2. Стратегія кібербезпеки України: затв. Указом Президента України від 26 серп. 2021 р. № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#n12 (дата звернення: 19.10.2023).

3. Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment: International Monetary Fund Working Paper, June 2018. URL: https://www.imf.org/-/media/Files/Publications/WP/2018/wp18143.ashx (дата звернення: 19.10.2023).

4. Положення про здійснення контролю за дотриманням банками вимог законодавства з питань інформаційної безпеки, кіберзахисту та електронних довірчих послуг: затв. постановою Правління Національного банку України від 16 січ. 2021 р. № 4. URL: https://zakon.rada.gov.ua/laws/show/v0004500-21#n11 (дата звернення: 19.10.2023).

5. Cybersecurity Framework Manufacturing Profile: National Institute of Standards and Technology, September 2017. URL: https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8183.pdf (дата звернення: 19.10.2023).

6. Developing Cyber-Resilient Systems: A Systems Security Engineering Approach: U.S. Department of Commerce, December 2021. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2r1.pdf (дата звернення: 19.10.2023).

7. Квасницька Р., Форкун І., Гордєєва Т. Сучасні підходи забезпечення інформаційної безпеки платіжних систем та їх кіберзахисту. Вісник Хмельницького національного університету. 2022. № 5, т.1. С.47-52.

8. Міщенко, В., Науменкова, С., & Міщенко, С. Управління операційними ризиками в платіжних системах. Економічний простір, 2023. №183. С.79-87.

9. Абрамова А. С. Трансформаційна природа операційних ризиків комерційних банків. Проблеми сучасних трансформацій. Серія: економіка та управління. 2022. №3. URL: https://reicst.com.ua/pmt/issue/view/issue_3_2022%20 (дата звернення: 19.10.2023).

УДК 004.056.55, 003.27

В. Д. Корнєва
viktoria.kornyeva@gmail.com
Науковий керівник: Ю.В. Білявська
доцент кафедри менеджменту, кандидат економічних наук, доцент
y.biliavska@knute.edu.ua
Державний торговельно-економічний університет, м. Київ

СПОСОБИ ЗАХИСТУ ІТ-ІНДУСТРІЇ ВІД ВИТОКУ ІНФОРМАЦІЇ

Зазвичай, будь-який витік конфіденційної інформації приносить збитки, яку б сферу ми не розглядали. ІТ-індустрія не є винятком. Великим компаніям і ще маленьким студіям потрібно діяти на випередження, тобто зробити все, щоб мінімізувати ризик розповсюдження інформації та можливі шкідливі наслідки. Історії про кіберзлочинців, що зламують бази даних та розповсюджують їх або вимагають за них гроші вже не є чимось дивним, але нерідко це роблять самі робітники. Вони допомагають конкурентам чи просто замовникам отримати секретні відомості за винагороду або ж вчиняють так з власних причин, наприклад, через звільнення. Тому компаніям потрібно захищатись не лише ззовні, а й слідкувати за процесами всередині.

Робота менеджерів в ІТ-галузі надзвичайно складна, адже для цього потрібно вміти керувати всіма процесами у компанії. Тенденції постійно змінюються і за ними не слід відставати, а цифровізація лише прискорює ці зміни. Та на шляху навіть у висококваліфікованих менеджерів виникають труднощі.

У міжнародній доктрині поняттями "кіберзлочини" і "кіберзлочинність" можна назвати різні види правопорушень. У п. 14 Доповіді Комітету II Десятого Конгресу ООН 2000 року по попередженню злочинності і поводженню з правопорушниками було зазначено, що існує дві категорії кіберзлочинів:

- кіберзлочини у вузькому розумінні («комп'ютерні злочини»): будь-яке протиправне діяння, здійснюване шляхом електронних операцій, метою якого є подолання захисту комп'ютерних систем і оброблюваних ними даних;
- кіберзлочини в широкому розумінні («злочини, пов'язані з використанням комп'ютерів»): будь-яке протиправне діяння, яке вчиняється шляхом або в зв'язку з комп'ютерною системою або мережею, включаючи такі злочини, як незаконне зберігання, пропонування або розповсюдження інформації через комп'ютерні системи або мережі [1].

Найбільш поширена класифікація кіберзлочинів в даний час ґрунтується на структурі Конвенції Ради Європи про кіберзлочинність від 23.11.2001 року. За конвенцією Ради Європи про кіберзлочинність існує чотири основних групи кіберзлочинів. До першої групи належать правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем: незаконний доступ, нелегальне перехоплення, втручання у дані, втручання у систему, зловживання пристроями. До четвертої групи увійшли правопорушення, пов'язані з порушенням авторських та суміжних прав [1].

За результатами досліджень Infosecurity Europe 2014, які ініціював Британський інститут стандартизації (BSI), 37 % опитуваних заявили, що, на їх думку, основну небезпеку для бізнесу працедавця створюють внутрішні загрози, а саме нелояльна, а часом і злочинна поведінка працівників організації [2].

Згідно з результатами досліджень компанії "SearchInform", більше 55 % персоналу у так званому пострадянському просторі готові передати важливу для компанії інформацію конкурентам, журналістам або контролюючим органам. При цьому майже 20 % з них зможуть це зробити абсолютно безкоштовно [2].

Можна виділити такі види порушників, що сприяли витоку інформації: недбалий інсайдер; маніпульований інсайдер; ображений інсайдер; нелояльний інсайдер; підробляючий інсайдер; впроваджений інсайдер [3].

Ще нещодавно на ринку праці була нестача висококваліфікованих ІТ-фахівців, і навіть великі компанії наймали новачків, яких почали масово звільняти з кінця 2022 [4]. Підприємствам потрібно зосереджувати свою увагу на персоналі та формувати команду, яка зможе адаптуватися до неочікуваних ситуацій, що виникають на ринку праці. Проте незалежно від галузі, знайти правильних людей - небияка проблема.

Не потрібно недооцінювати усю важливість персоналу. Бо чим цінніший працівник з відповідними характеристиками, тим більший шанс досягнення поставлених цілей компанії. Часта заміна працівників не призводить до бажаного результату, оскільки порушується внутрішній спокій в організації, виникає високий ризик витоку конфіденційної інформації, зростають фінансові витрати у сфері розвитку та навчання персоналу, зменшується можливість формування професійного персоналу, зростає вразливість організації до зовнішнього мінливого середовища та збільшується кількість надання неякісних послуг [5].

Ні вітчизняне законодавство, ні наявна практика не виробили на сьогоднішній день ефективних превентивних заходів щодо попередження витоку інформації або способів захисту правовласників після того, як інформацію було розголошено. Труднощі виникають вже на етапі визначення кола відомостей, які підлягають охороні, та й довести факт незаконного поширення таких відомостей під час судового розгляду часом буває неможливо, так само як і чітко розрахувати і обґрунтувати розмір завданих збитків та упущеної вигоди [6]. Хоча чітких способів уникнути цього ніде не вказано, проте можна виділити деякі дієві способи, що разом зменшать ризики.

Договір про нерозголошення конфіденційної інформації (NDA) та судовий захист. Обов'язковим повинно бути підписання співробітниками, розробниками, постачальниками угод про нерозголошення конфіденційної інформації та контракти про відповідальність за витік інформації.

Перевірка нових робітників. У деяких випадках компанія надсилає новачкам фейкові фішингові листи, щоб виявити, чи попадеться людина в таку пастку. Такий метод потрібен для безпеки організації, адже шахраї можуть надіслати вже справжні листи.

Шифрування даних, контроль та обмеження доступу. Впровадження нових програмних рішень, які дозволяють застосовувати політики безпеки і надають додатковий захист від втрати даних. Це може бути контроль додатків і контроль пристроїв, антивірусні рішення для мобільних пристроїв, програмні рішення для управління мобільними пристроями та їх захисту, надання доступу лише певним робітникам або шифрування коду та даних на знімних носіях [7].

Санкції, покарання та штрафи. За даними GlobalCorporateITSecurityRisks чіткі санкції та дисциплінарні заходи в разі порушення діючих в компанії політик безпеки застосовуються менш ніж у 32% в Східній Європі (46% у світі). І тільки 33% респондентів (48% у світі) заявили, що в їх компаніях співробітники розуміють всю важливість дотримання політик безпеки [7].

Освіта співробітників. Найбільшу складність викликають проблеми, що виникають внаслідок «людського» фактора. До найзначніших відносяться вразливості або помилки у встановленому програмному забезпеченні й випадкові витоки даних з вини працівників. Тому навчання основам безпеки та конфіденційності, дотримання правил та постійне підвищення кваліфікації є надзвичайно важливим [7].

IT-аудит. Це може бути спеціальна перевірка персоналу чи документів, анкетування, інтерв'ю чи тестування систем контролю. Здійснення IT-аудиту з метою профілактики дозволить систематизувати інформаційну структуру підприємства, визначити основні тенденції її розвитку, виявити місця можливого зниження витрат на IT та захистити підприємство від можливих витоків інформації [8].

Фізична безпека. Охорона приміщень, де зберігаються обладнання, джерела та носії даних.

Моніторинг. Використання камер відеоспостереження та різних датчиків для виявлення порушників.

Кібербезпека. Система кібербезпеки складається із декількох елементів: безпеки додатків; безпеки даних; безпеки критично важливої інфраструктури; мережевої і операційнлї безпеки; хмарної безпеки; планування аварійного відновлення. Це захист всього, що вразливе для злому, кібератаки та несанкціонованого доступу, тобто комп'ютерів, пристроїв, мереж, серверів та програм. При цьому розглянуте відноситься виключно до захисту даних, які існують у цифровій формі [9].

Отже, кібератаки та недоброчинність робітників - дві глобальні проблеми IT-індустрії. Підбір правильного персоналу й захист даних не такі прості завдання, як здається. Щоб уникнути небезпеки для бізнесу компаніям потрібно прийняти певні заходи, а краще одразу ж комплекс заходів. Крім того, в нашій країні варто покращити судовий захист авторських прав у законодавстві.

Список літератури

1. Кундеус В. Г. Поняття та види кіберзлочині — URL: в https://dspace.univd.edu.ua/server/api/core/bitstreams/6e42bc23-7a3f-41b5-b4cf-9a5a737e8184/content

2. Криловецький Б. С., Кухарська Н. П. Персонал - джерело внутрішніх загроз інформаційній безпеці підприємствам— URL: https://sci.ldubgd.edu.ua/bitstream/123456789/752/1/5.pdf

3. Інсайдер — URL: https://uk.wikipedia.org /wiki/Інсайдер

4. Казарян С. Що спричинило масові звільнення в IT? — URL: https://telegraf.design/shho-sprychynylo-masovi-zvilnennya-v-it/

5. Кобеля З. І. Особливості IT-рекрутингу на сучасному ринку праці — URL: http://surl.li/llvzv

6. Мадрик А. Договори про уникнення розголошення та неконкуренцію: аналіз зарубіжної практики та дійсність за чинним законодавством України — URL: http://nbuv.gov.ua/UJRN/ipch_2019_1_26

7. Шеховцова В. І., Ключко Г. Г. Чинники впливу на ефективність функціонування іт-інфраструктури підприємства — URL: https://openarchive.nure.ua/server/api/core/bitstreams/22f8101a-7561-44eb-aaf4-0bacc7d8a63f/content

8. Дегтяренко В. І. IT-аудит як перспективний напрямок розвитку бізнесу — URL: https://evnuir.vnu.edu.ua/bitstream/123456789/16761/1/Degtyarenko%20168-171.pdf

9. Сопілко І. М. Інформаційна безпека та кібербезпека: порівняльно-правовий аспект — URL: https://dspace.nau.edu.ua/bitstream/NAU/53733/1/%d0%86.%20%d0%9c.%20%d0%a1%d0%be%d0%bf%d1%96%d0%bb%d0%ba%d0%be.pdf

УДК 004.056, 004.75

П.С. Мірошніков, М.М. Тімчинко
Miroshnikov_PS@gmail.com , Tim_M25@gmail.com
Центральноукраїнський Національний технічний університет, м. Кропивницький

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ ЗАХИСТУ В ІНФОРМАЦІЙНІЙ СИСТЕМІ

Інтернет речей(IoT) є одним із найбільш перспективних напрямків розвитку інформаційно-комунікаційних технологій. Кількість підключених до мережі Інтернет пристроїв бурхливо зростає, і це вимагає сучасних підходів до побудови високонавантажених серверних систем. Платформи Інтернету речей мають забезпечувати можливість аналізувати різні аспекти даних, що потрібно для оптимізації різноманітних виробничих та інших процесів. Проблеми та задачі у сфері побудови серверних систем для Інтернету речей можна поділити на загальні, які притаманні багатьом іншим системам обробки великих даних, та специфічні, що виникають лише в цій області. Загальними задачами є побудова та використання ефективних, відмовостійких, масштабованих і розподілених систем роботи з даними. Специфічними для Інтернету речей проблемами є забезпечення надійного керування та моніторингу пристроїв.

У цій роботі визначаються вимоги до побудови хмарних платформ для Інтернету речей, досліджуються існуючі платформи та виокремлюються шляхи їх покращення. Вивчаються й описуються архітектурні рішення в галузі обробки великих обсягів даних та підходи до розробки програмного забезпечення, які дозволяють реалізувати платформу таким чином, аби вона задовольняла означеним функціональним і нефункціональним вимогам.

Рис. 1. Структурна схема систем IoT

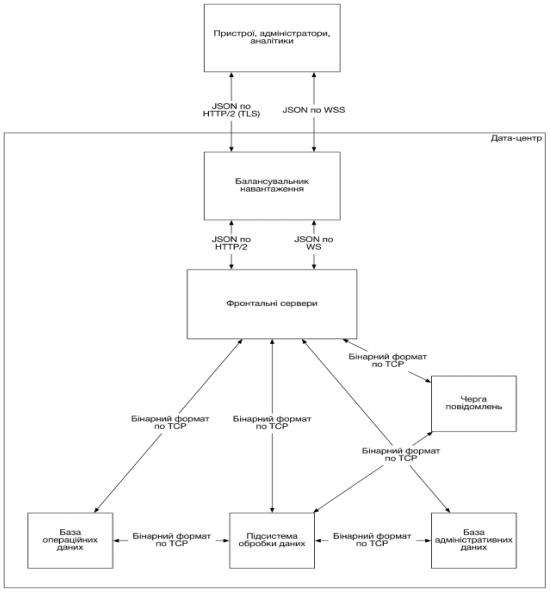


Рис. 2. Запропоновані формати даних і їх протоколи передачі

На рис.1 наведено класичну схему реалізації систем IoT а на рис.2 запропоновані протоколи передачі.

У процесі рішення завдань, обумовлених цілями дослідження, отримані наступні результати:

– удосконалено серверне рішення хмарної платформи Інтернету речей з впровадженням підсистеми безпеки передачі даних;

– проведено огляд технологій зв'язку в системах IoT;

– розроблено вітчизняний продукт управління хмарною платформою з підсистемою безпеки передачі даних, який має більш широкі можливості, на відміну від існуючих аналогів.

УДК 004.7

О.А. Якименко, Є.В. Мелешко, Р.О. Ткачук, С.В. Шимко
elismeleshko@gmail.com
Центральноукраїнський національний технічний університет, м. Кропивницький

МЕТОД ВИЯВЛЕННЯ ІНФОРМАЦІЙНИХ АТАК НА КОМП'ЮТЕРНУ СИСТЕМУ НА ОСНОВІ R/S-АНАЛІЗУ ТРАФІКУ

Мережеві інформаційні атаки на комп'ютерні системи є серйозною загрозою для безпеки інформаційного суспільства. Зловмисники використовують різні методи та техніки для злому та заволодіння конфіденційною інформацією, завдання шкоди, або перешкоди нормальному функціонуванню комп'ютерних систем. Однією з найпоширеніших та найнебезпечніших форм мережевих атак є DDoS-атаки (розподілені атаки з відмовою в обслуговуванні).

Актуальність дослідження та розробки методів захисту від мережевих атак та особливо DDoS-атак базується на наступних ключових факторах:

– Зростання залежності від цифрових технологій у різних сферах діяльності. Все більше аспектів нашого життя та бізнесу стають цифровими та підключеними до мережі Інтернет. Робота компаній, фінансові операції, комунікація, медицина, транспорт, енергетика – усе це переходить у мережу Інтернет, і DDoS-атаки можуть спричинити серйозні збої у роботі та втрати.

– Зростання обсягів мережевого трафіку. Обсяги мережевого трафіку зростають величезними темпами, особливо з розвитком стримінгу відео, хмарних служб та Інтернету речей. Це робить DDoS-атаки ще більш ефективними і руйнівними.

DDoS-атаки становлять велику загрозу, оскільки вони можуть перевантажувати мережеві ресурси, призводячи до відмови в обслуговуванні, втрати прибутку та порушенні доступності важливих онлайн-систем, пристроїв в Інтернеті речей тощо. Різновиди DDoS-атак включають атаки з використанням ботнетів, ампліфікації, SYN/ACK-атаки та інші, і вони можуть бути спрямовані на веб-сервери, мережеві інфраструктури та інші цільові об'єкти.

Розвиток нових методів та інструментів для виявлення і захисту від DDoS-атак стає важливим завданням у сфері кіберзахисту, оскільки спрямований на забезпечення стабільності та безпеки мереж і онлайн-систем у сучасному цифровому світі.

Метою даної роботи була розробка та реалізація методу виявлення мережевих інформаційних атак на комп'ютерну або комп'ютерно-інтегровану систему, зокрема, атак типу Ddos, на основі R/S-аналізу вхідного трафіку.

Для визначення наявності Ddos-атаки було вирішено аналізувати вхідний трафік, що надходить на комп'ютерну систему, методом R/S-аналізу. Це дозволить виявляти тренди у трафіку, зокрема, тенденцію до продовження його збільшення. R/S-аналіз часових рядів трафіку дозволяє отримати показник Херста. Інтерпретація одержаних значень показника Херста може здійснюватися наступним чином:

– $H = 0.5$ – певного тренду у мережевого трафіку немає, вважаємо його повністю випадковим.

– $H > 0.5$ – мережевий трафік характеризується персистентністю – має тенденцію до збереження тренду; чим більше число, тим більш проявлене збереження тренду.

– $H < 0.5$ – мережевий трафік характеризується антиперсистентністю – будь-яку тенденцію прагне змінити протилежна; чим менше число, тим більш проявлене прагнення до зміни тренду.

Значення показника Херста природних процесів групуються поблизу значень 0,72-0,73.

Персистентний трафік (з показником $H \geq 0.74$) є зоною ризику, так як може свідчити про Ddos-атаку, або природнє (але сильне) підвищення інтересу до комп'ютерної системи (наприклад, серверу веб-сайту), що також може призвести до відмови в обслуговуванні при надто великих і тривалих об'ємах вхідного трафіку.

Показник Херста H треба розглядати разом з поточною інтенсивністю трафіку λ. Адже тільки сукупність високого індексу Херста та високої інтенсивності трафіку може свідчити про можливу небезпеку перевантаження комп'ютерної системи (наприклад, сервера) та ймовірність подальшої відмови в обслуговуванні.

Запропонований метод виявлення інформаційних атак типу Ddos на комп'ютерну або комп'ютерно-інтегровану систему на основі R/S-аналізу вхідного трафіку має наступні кроки:

Крок 1. Читання вхідного трафіку комп'ютерної системи у реальному часі та запис його зразків у вигляді часових рядів.

Крок 2. Визначення інтенсивності трафіку на основі зібраної статистики.

Крок 3. Визначення показника Херста на основі R/S-аналізу та зібраної статистики.

Крок 4. Визначення ймовірності інформаційної атаки на основі аналізу значень інтенсивності трафіку та показника Херста. Для визначення ймовірності атаки використовуються правила з бази знань розробленої системи, наприклад, IF $H > n$ AND $\lambda > m$ THEN $P_{attack} = q$.

Крок 5. Виведення звіту користувачу системи по запиту та виведення повідомлення про небезпеку інформаційної атаки при її високій ймовірності.

Було запропоновано наступну структурну схему для розробки програмного забезпечення (рис.1):

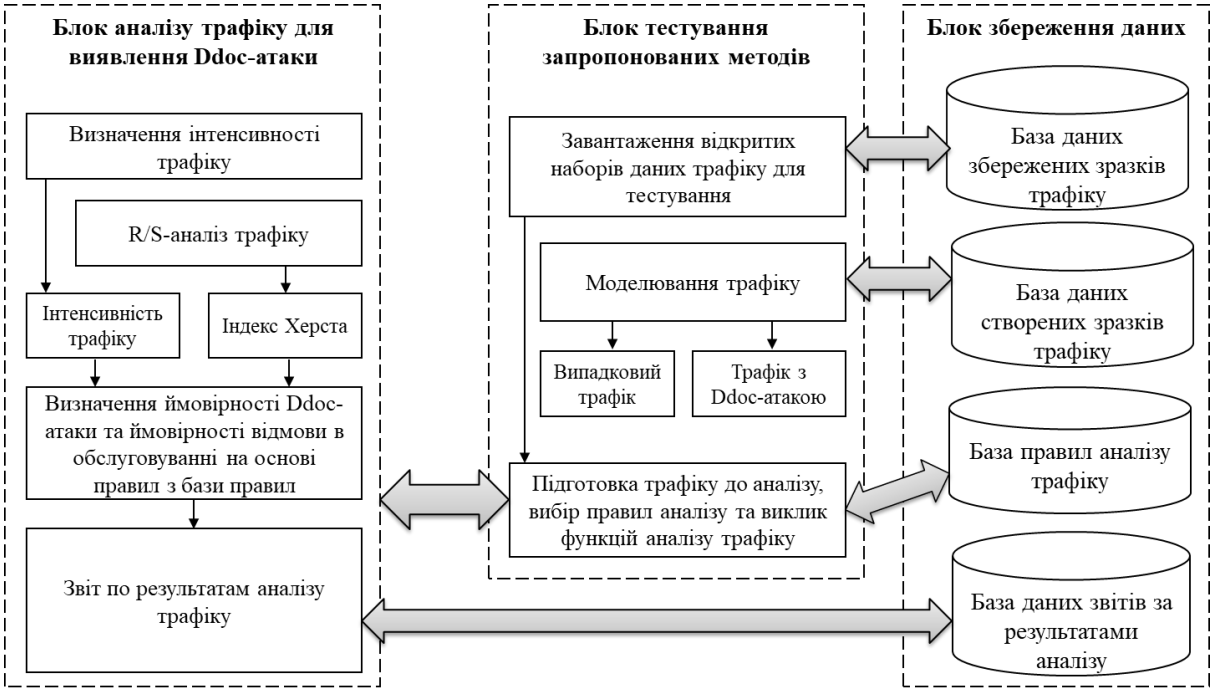


Рисунок 1. Структурна схема розроблюваного програмного забезпечення на основі запропонованого методу

Було розроблене відповідне програмне забезпечення на мові Python. Тестування розробленого програмного забезпечення проводилося на відкритому наборі даних CICEV2023 DDoS attack dataset та на наборах даних згенерованих у розробленій програмній моделі. Точність результатів розпізнавання інформаційних атак в середньому складала 75%. Запропонований метод доцільно поєднувати з іншими існуючими методами виявлення інформаційних атак для підвищення точності їх роботи.

Таким чином було розроблено метод виявлення мережевих інформаційних атак типу Ddos на комп'ютерну або комп'ютерно-інтегровану систему на основі R/S-аналізу вхідного трафіку, а також розроблене відповідне програмне забезпечення та проведено тестування якості його роботи.

Список літератури

1. Ali M. Time Series Forecasting Tutorial. 2022. URL: https://www.datacamp.com/tutorial/tutorial-time-series-forecasting#rdl

2. Lakhmi Priya Das, Sanjay Kumar Patra, Sarojananda Mishra. Impact of hurst parameter value in self-similarity behaviour of network traffic. International Journal of Research in Computer and Communication Technology. 2016. Vol. 5, no. 12. P. 631–633.

3. Millán G. Traffic flows analysis in high-speed computer networks using time series. arXiv preprint arXiv:2103.03984. 2021. DOI: 10.48550/arXiv.2103.03984. URL: https://arxiv.org/abs/2103.03984

4. Кучук Г. А., Можаєв О. О., Воробйов О. В. Прогнозування трафіка для управління перенавантаженнями інтегрованої телекомунікаційної мережі. Радіоелектронні та комп'ютерні системи. 2007. Вип. 8. С. 261–271. URL: http://nbuv.gov.ua/UJRN/recs_2007_8_48.

5. Моделі та процедури класифікації і прогнозування недетермінованих процесів за показниками хаотичної динаміки / В. В. Скалозуб, В. М. Горячкін, І. В. Клименко, Д. О Шаповал. System technologies. 2022. Vol. 3, no. 140. DOI: 10.34185/1562-9945-3-140-2022-10.

6. Canadian Institute for Cybersecurity. CICEV2023 DDoS attack dataset. URL: https://www.unb.ca/cic/datasets/cicev2023.html

УДК 004.62

Г.О. Молнар, д-р техн. наук, проф. С.П. Євсеєв
hanna.molnar@cit.khpi.edu.ua, serhii_yevseiev@khpi.edu.ua
Національний технічний університет «Харківський політехнічний інститут», м. Харків

ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНА БЕЗПЕКА

У сучасному світі інформація впливає на психіку, формуючи наше розуміння оточуючого світу. З розвитком інтернету та соціальних мереж вплив інформації став ще помітнішим. Інформаційна безпека та критичне сприймання інформації стали важливими для психологічного здоров'я та стійкості в умовах інформаційного перевантаження та маніпуляцій.

Свідомість щодо інформаційної безпеки полягає в дотриманні правил і регуляцій для захисту інформації в організації і є важливою частиною плану управління інформаційною безпекою .

Різна інформація викликає різні емоції. Психічне здоров'я залежить від соціальних зв'язків: сім'ї, друзів, роботи та інших. Впливи можуть бути позитивними або негативними .

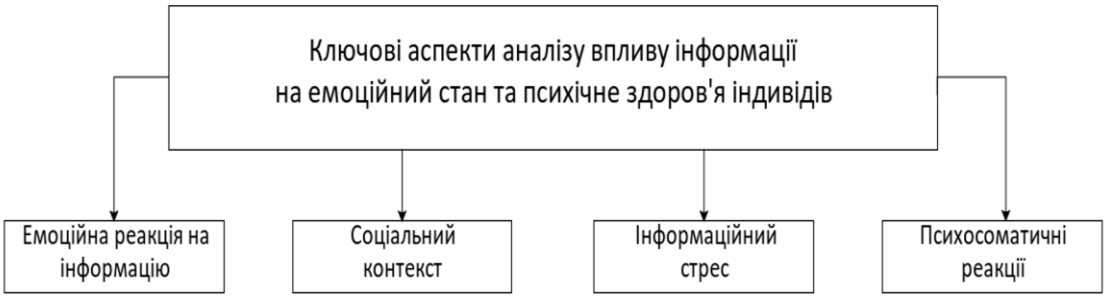


Рис. 1. Аналіз впливу інформації на емоційний стан та психічне здоров'я індивідів.

Аналіз впливу інформації на емоційний стан та психологічне здоров'я показав, що в ведення гібридних війн необхідне комплексування всіх складових аспектів, визначення їх синтезу та поєднання.

Таким чином, неможна недооцінювати важливість інформаційно-психологічної безпеки, особливо в умовах інформаційно-психологічної війни. В умовах гібридної та відкритої війнах вивчення загроз, пов'язаних із маніпуляцією та дезінформацією у цифровому середовищі є важливим для розробки стратегій протидії маніпуляції, дезінформації.

Досвід інформаційно-психологічної війни у виконанні рф проти України вже аналізується як у середині України так і за межами країни. Необхідно активно впроваджувати та популяризувати інформаційну грамотності та психологічний захист населення.

Інформаційно-психологічна безпека напряму пов'язана з інформаційно-психологічною війною, яка може мати серйозні наслідки для стабільності та безпеки суспільства та держави, і потребує комплексних заходів для захисту від неї, таких як підвищення інформаційної грамотності, зміцнення кібербезпеки, і розвинення ефективних стратегій з протидії дезінформації та психологічному впливу.

Для забезпечення інформаційно-психологічної безпеки, важливо розвивати навички медіаграмотності та емоційного інтелекту, щоб індивіди могли критично оцінювати інформацію та керувати своїми емоціями під час споживання контенту.

Також необхідно впроваджувати заходи самозахисту, включаючи кібербезпеку, а також надавати психологічну підтримку тим, хто стикається з психологічними труднощами через інформаційні загрози. Крім того, сприяти комунікації і співпраці між індивідами та організаціями для обміну досвідом і знаннями у сфері інформаційно-психологічної безпеки, регулювати інформаційні практики для забезпечення безпеки і прав індивідів.

Таким чином, в умовах гібридності та комплексування наведених аспектів інформаційно-психологічної безпеки необхідна гнучка система захисту на основі підвищення рівня медіаграмотності та емоційного інтелекту, що дозволяє протистояти як цільовим атакам, так й комплексованим з методами соціальної інженерії.

УДК 004.056, 004.75

І.О. Хоменко
unmindful_headache411@simplelogin.com
доцент О.Г. Король
Національний технічний університет «Харківський політехнічний інститут», м. Харків

ВАЖЛИВІСТЬ КІБЕР ГІГІЄНИ ТА ОБДУМАНОГО РОЗПОВСЮДЖЕННЯ ПЕРСОНАЛЬНИХ ДАНИХ

Кібер гігієна - це практика вжиття заходів для захисту себе та своєї організації від кібератак. Дотримуватися належної кібер гігієни важливо для всіх, незалежно від їхніх технічних знань. У світі, де майже кожен аспект нашого життя залежить від цифрових технологій, захист ваших даних стає надзвичайно актуальним завданням. Важливо пам'ятати, що кібератаки можуть наслідувати різні форми, включаючи віруси, фішинг, рейди, і інші. Ви не завжди зможете передбачити, коли і звідки може надійти загроза, але дотримання кібер гігієни може допомогти вам залишатися в безпеці.

Останніми роками сталася низка гучних витоків даних, які призвели до витоку персональних даних мільйонів людей. Ці витоки були спричинені різними факторами, в тому числі й поганими практиками кібер гігієни. Однак, слід відзначити, що багато з цих витоків могли б бути унеможливленні за наявності належної обізнаності та уважності. Важливо підкреслити, що інформація - це валюта сучасного світу, і несанкціонований доступ до неї може завдати значної шкоди. Тому, зберігання та обробка особистих даних повинні супроводжуватися відповідними заходами забезпечення кібербезпеки для захисту як особистих інтересів, так і інтересів організації. Використовуйте надійні паролі та вмикайте багатофакторну автентифікацію, де це можливо. Надійний пароль складається щонайменше з 12 символів і включає в себе поєднання великих і малих літер, цифр і символів. Також слід уникати використання загальних слів або фраз у своїх паролях. Багатофакторна автентифікація додає додатковий рівень безпеки до вашого облікового запису, вимагаючи ввести код з телефону на додаток до пароля під час входу. Оновлюйте своє програмне забезпечення. Оновлення програмного забезпечення часто включають виправлення безпеки, які можуть допомогти захистити ваші пристрої від кібератак. Важливо встановлювати оновлення програмного забезпечення, як тільки вони стають доступними.

Використовуючи надійні паролі та вмикайте багатофакторну автентифікацію, де це можливо, ви робите важливий крок у напрямку захисту своїх особистих даних. Створення сильного паролю – це більше, ніж просто комбінація символів. Важливо також не використовувати однаковий пароль для різних сервісів, оскільки це робить ваші дані вразливими в разі порушення безпеки одного з них. Багатофакторна автентифікація, в свою чергу, створює додатковий бар'єр для незаконних спроб доступу, оскільки для входу потрібно буде не лише пароль, але й інший елемент, який тільки вам відомий[1].

Будьте в курсі останніх шахрайств та фішингових атак. Фішингові атаки - це спроби обманом змусити вас розкрити особисту інформацію або перейти за шкідливими посиланнями. Фішингові електронні листи можуть виглядати так, ніби вони від легальних компаній, таких як банки або компанії, що надають кредитні картки. Однак такі листи, як правило, містять багато червоних прапорців, таких як погана граматика та орфографічні помилки. Якщо ви отримали листа від незнайомої вам компанії або якщо лист містить підозрілі посилання, не переходьте за ними. Замість цього зв'яжіться безпосередньо з компанією, щоб перевірити автентичність листа.

Повідомляйте про будь-яку підозрілу активність органам влади. Якщо ви підозрюєте, що ваші персональні дані були витоком, або якщо ви стали жертвою кібератаки, важливо повідомити про інцидент органам влади. Це допоможе відстежити зловмисників і запобігти тому, щоб інші не стали жертвами такої ж атаки.

Дотримуючись цих простих правил кібер гігієни, ви можете допомогти захистити себе і свою організацію від кібератак. Заходи, наведені вище, формують базовий каркас для забезпечення безпеки в цифровому світі. Проте важливо розуміти, що кіберзахист - це постійний процес, і ви повинні залишати свою обізнаність актуальною. Світ інформаційної безпеки постійно змінюється, і зловмисники розвивають нові методи атак. Тому навчання та самоосвіта в цій галузі є важливою складовою кібер гігієни. Поглиблене розуміння ризиків і сучасних загроз допоможе вам бути більш підготовленими до викликів, які можуть виникнути в цифровому середовищі.

На додаток до вищесказаного, я хотів би підкреслити, що поширення персональних даних викликає все більше занепокоєння. Ми бачили, як це відбувається в ряді нещодавніх випадків, включаючи витоки з українських державних органів[2], Facebook[3] та Google[4]. Ці випадки слугують нагадуванням про те, наскільки цінними і уразливими можуть бути ваші особисті дані. Поширення персональних даних може призвести до непередбачених наслідків, включаючи можливість крадіжки ідентичності, фінансових злочинів та шантажу.

Важливо розуміти, що після витоку ваших персональних даних дуже важко контролювати, як вони використовуються. Ці дані можуть бути використані в різних зловмисних цілях, таких як крадіжка особистих даних, шахрайство і навіть шантаж. Тому варто приділити особливу увагу заходам, спрямованим на запобігання несанкціонованому доступу до вашої особистої інформації та контролю над тим, кому і за якими умовами ви її надаєте.

- Єдиного рішення проблеми навмисного поширення персональних даних не існує. Однак є ряд речей, які можна зробити, щоб зменшити ризики. До них відносяться:
- Обережно ставитися до інформації, якою ви ділитеся в Інтернеті. Доцільно ретельно перевіряти сайти і сервіси, з якими ви спілкуєтеся.
- Використання надійних паролів та багатофакторної автентифікації. Не губіть бджілок з паролями та використовуйте парольні менеджери для збереження складних комбінацій символів.
- Постійно оновлювати програмне забезпечення, оскільки знову з'являються нові загрози. Регулярні оновлення - це ваша оборона від вразливостей.
- Бути в курсі останніх шахрайств і фішингових атак. Важливо навчитися розпізнавати потенційно шкідливі повідомлення та посилання.
- Повідомляти про будь-яку підозрілу активність органам влади, що спеціалізуються на кібербезпеці. Ваша реакція може допомогти припинити атаку та захистити інших користувачів мережі.

Вживаючи цих заходів, ви можете допомогти захистити себе від негативних наслідків навмисного поширення персональних даних. Дбайте про свою кібербезпеку та будьте уважними при обробці особистих даних, оскільки ваша захищеність і приватність є на вагу золота в цифровому світі.

Список літератури

1. bayshore, 6 Tips To Create A Password Policy For Your Organization
2. biz.nv.ua, Витік чи провокація? Що відомо про імовірний продаж персональних даних українців з Дії
3. Віталій Кузьмін, blog.liga.net, Витік даних Facebook: про що варто знати українцям
4. LILY HAY NEWMAN, wired.com, A New Google+ Blunder Exposed Data From 52.5 Million Users

СЕКЦІЯ 2. ПРОГРАМУВАННЯ ТА ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ

УДК 004.9

В.В. Міхав[1], С.Г. Семенов[2], Є.В. Мелешко[1], М.С. Якименко[1], Я.П. Шуліка[1]
mihaw.wolodymyr@gmail.com
[1]*Центральноукраїнський національний технічний університет, м. Кропивницький, Україна*
[2] *Краківський педагогічний університет, м. Краків, Польща*

МАТЕМАТИЧНА МОДЕЛЬ РЕКОМЕНДАЦІЙНОЇ СИСТЕМИ ДЛЯ ДЕЦЕНТРАЛІЗОВАНИХ ОДНОРАНГОВИХ КОМП'ЮТЕРНИХ МЕРЕЖ

Розроблена модель децентралізованої рекомендаційної системи, що дозволила оцінити ймовірнісно-технічні характеристики процесу обробки даних в рекомендаційній системі децентралізованої однорангової комп'ютерної мережі. В основі структури рекомендаційної системи, що розроблена, була використана парадигма функціонування багатоагентної однорангової мережі *CAN*. При цьому основною інноваційною складовою цієї розробки стала побудова структури, в якій множина моніторингових вузлів розглядається як багатоагентна та мультитригерна система. В цій структурі кожен вузол представлений агентом-об'єктом, що має функції, пов'язані з відслідковуванням та ідентифікацією зміни стану об'єктів моніторингу в межах свого поля зору. Для реалізації функції багатовузлового моніторингу об'єктів, розроблена структура рекомендаційної системи однорангової мережі (рис. 1).

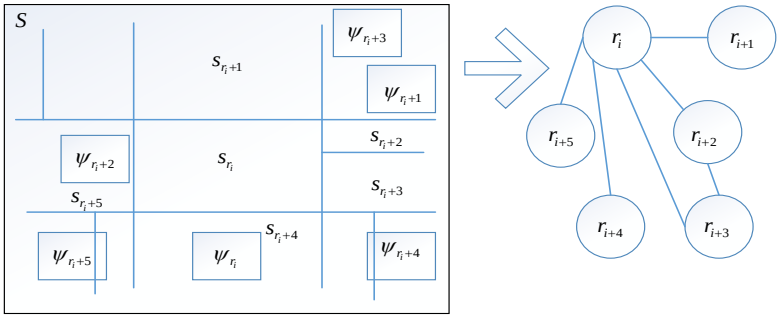
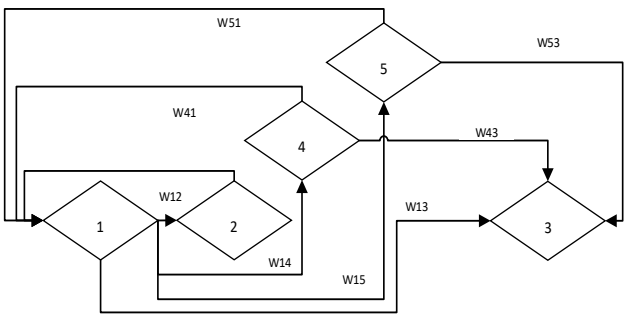


Рис. 1. Приклад структури рекомендаційної системи однорангової мережісформованої з урахуванням підвищених вимог до достовірності і безпеки даних шляхом зв'язування зон відповідальності «батьківських» та «дочірніх» вузлів

Дослідження проводилися з використанням системи комп'ютерної алгебри із класу систем автоматизованого проєктування MathCad. Для математичного моделювання було використано теорію GERT-мереж. Для оцінки точності розробленої моделі було використано наближені оцінки, засновані на обробці даних з відкритого датасету Netflix Prize data [1]. Точність результатів моделювання оцінювалася за допомогою показника довірчої ймовірності потрапляння в «усереднений» довірчий інтервал.

Було запропоновано GERT-схему представлену на рис. 2.



Стан 1. «Початковий», змін нема.

Стан 2. «Відбулись зміни». В якомусь з вузлів може змінитись рекомендаційний «портрет», тобто сформуватись нова ідеологія рекомендацій.

Стан 3. «Зафіксовано у всіх вузлах». Фіксується «портрет» «дочірнього» вузла в інших вузлах.

Стан 4. «Про зміни повідомлено». Вузол «батько» помічає зміни рекомендаційного «портрету» «дочірнього» вузла.

Стан 5. «Перевірено та зафіксовано про зміни стану». Фіксується «портрет» «дочірнього» вузла в «батьківському» вузлі.

Рис. 2. GERT-схема ідентифікації стану вузлів децентралізованої рекомендаційної системи

W-функції – це функції часу ідентифікації стану вузлів рекомендаційної системи в процесі формування та зміни рекомендацій. Для запропонованої схеми можна скласти наступне рівняння:

$$W_E(s)=\frac{W_{13}+W_{14}W_{43}+W_{15}W_{53}}{1-W_{15}W_{51}-W_{14}W_{41}-W_{12}W_{21}}=\frac{(\lambda_4-s)\times\left(\lambda_2\lambda_5 q_5(\lambda_3-s)+p_3\lambda_3(\lambda_2-s)(\lambda_5-s)\right)}{\left((\lambda_3-s)(\lambda_5-s)\times\right.}\Bigg/\left.\begin{matrix}\\ \times\left((\lambda_2-s)\left((\lambda_4-s)(\lambda_1-s)-p_1q_2\lambda_1\lambda_4\right)-\lambda_2\lambda_4q_6(\lambda_1-s)\right)\end{matrix}\right),$$

де s – час ідентифікації стану вузлів рекомендаційної системи в процесі формування та зміни рекомендацій, $л$ – інтенсивність переходів, p та q – ймовірності переходів між станами.

Одним з основних результатів формалізації процесів формування та змін рекомендацій, отриманими у цій роботі, є отримання аналітичного виразу (1):

$$\zeta(x)=\sum_{n=1}^{5}\operatorname{Re}s\left[e^{zx}\Im(z)\right]=\sum_{n=1}^{5}\frac{e^{z_n x}\left(z_n^3 b+z_n^2 a+z_n u+k\right)}{\left(5z_n^4+4g_4z_n^3+3g_3z_n^2+2g_2z_n+g_1\right)}, \quad (1)$$

де $a=q_5\lambda_5\lambda_2\left(\lambda_3+\lambda_4\right)+p_3\lambda_3\left(\lambda_4+\lambda_2+\lambda_5\right)$, $b=q_5\lambda_5\lambda_2+p_3\lambda_3$,

$u=q_5\lambda_5\lambda_2\left(\lambda_3\lambda_4+\lambda_4+\lambda_3\right)+p_3\lambda_3\left(\lambda_2\lambda_4+\lambda_5\lambda_4+\lambda_2\lambda_5\right)$,

$k=\lambda_2\lambda_3\lambda_4\lambda_5\left(q_5+p_3\right)$, $g_1=\lambda_5\lambda_3+r\left(\lambda_5+\lambda_3\right)$, $g_2=\lambda_5\lambda_3 w+d\left(\lambda_5+\lambda_3\right)+r$, $g_3=\lambda_5\lambda_3+w\left(\lambda_5+\lambda_3\right)+d$,

$g_4=\lambda_5+\lambda_3+w$,

x – межі математичного моделювання, n – кількість станів системи, e – експонента, z – випадкова величина часу формування рекомендацій, $z = –im$, де т є дійсною змінною.

За допомогою виразу (1) є можливість оцінити щільність розподілу ймовірностей часу ідентифікації стану вузлів рекомендаційної системи. А за допомогою неї можна існуючими методами та інструментами визначити математичне очікування як характеристику часу формування рекомендацій та дисперсію як точність прийнятої характеристики часу формування рекомендацій.

Однією з переваг отриманого виразу (1) є можливість його використання для різних датасетів рекомендаційних систем. Потрібно лише емпіричним шляхом отримати значення основних характеристик ($л$ та p) GERT-мережі. Використання багатоагентного та мультитригерного підходу дозволило підвищити точність результатів моделювання на 5%. Це доведено за допомогою порівняльного аналізу даних, згенерованих розробленою моделлю, отриманих після обробки датасету Netflix Prize data [1] та згенерованих з використанням відомих моделей [2, 3] (рис. 2).

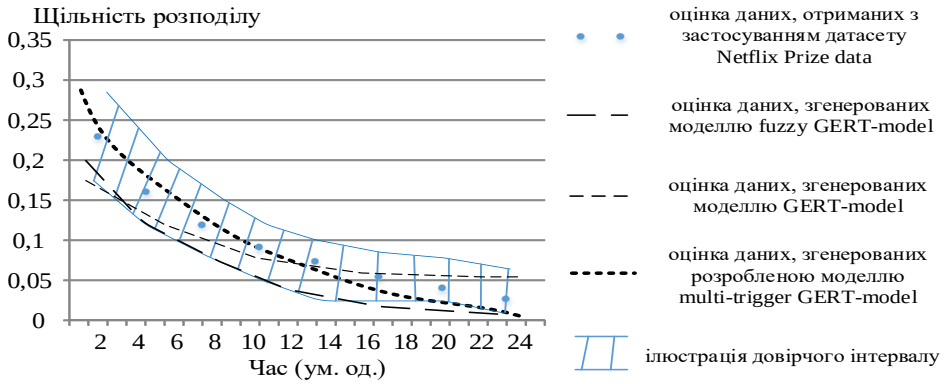


Рис. 2. Графіки залежності щільності розподілу ймовірностей часу ідентифікації стану вузлів рекомендаційної системи від часу передачі файлу для різних «датасетів»

Розроблена математична модель дозволяє проводити порівняльний аналіз різних методів роботи рекомендаційних систем та підбирати оптимальні параметри роботи системи. Запропонована модель може бути використана для прототипування рекомендаційних систем у різних сферах діяльності.

Список літератури

1. Netflix (2019) Netflix Prize data: Dataset from Netflix's competition to improve their reccommendation algorithm. Kaggle, data mining contest organization system. URL: https://www.kaggle.com/datasets/netflix-inc/netflix-prize-data?resource=download

2. Semenov S., Zhang L., Cao W., Bulba S., Babenko V., Davydov V. (2021) Development of a fuzzy GERT-model for investigating common software vulnerabilities. Eastern-European Journal of Enterprise Technologies, 6(2 (114), pp. 6–18. doi: https://doi.org/10.15587/1729-4061.2021.243715

3. Semenov S., Liqiang Z., Weiling C., Davydov V. (2021) Development a mathematical model for the software security testing first stage. Eastern-European Journal of Enterprise Technologies, 3(2 (111)), pp. 24–34. doi: https://doi.org/10.15587/1729-4061.2021.233417

УДК 004.056, 004.75

О.С. Пауков[1]
Paukov_OS@gmail.com
[1]*Центральноукраїнський Національний технічний університет, м. Кропивницький*

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ ЗАСТОСУВАННЯ NOSQL БАЗ ДАНИХ В ІНФОРМАЦІЙНИХ СИСТЕМАХ

NoSQL (Not Only SQL) - це широкий термін, який стосується нереляційних моделей баз даних, які використовують різні структури для зберігання даних: документи, ключ-значення, стовпцеві та графові бази даних. NoSQL-бази даних використовуються тоді, коли потрібно зберігати дані неструктурованого характеру, наприклад, великі обсяги текстових даних, зображень та відео.

NoSQL-бази даних можна порівняти із великою та складною грою в головоломки, в якій кожний елемент представляє окремий фрагмент інформації. Інформація може бути представлена не лише у вигляді тексту, але і у вигляді зображень, звукових файлів, відеоматеріалів і т.ін. Кожен фрагмент може мати різний розмір і форму, і для того, щоб отримати повну картину, необхідно зібрати та об'єднати всі фрагменти. Це схоже на роботу з NoSQL-базами даних, де кожен елемент може бути різних типів і форматів, і для отримання всієї необхідної інформації слід використовувати різні методи та інструменти запитів. В ході роботи було проведено тестування PostgreSQL, Cassandra, DinamoDB. Для тестування використана система Yahoo Cloud System Benchmark. Адаптація системи YCSB дозволяє проводити тестування на швидкість виконання операцій та складних запитів.

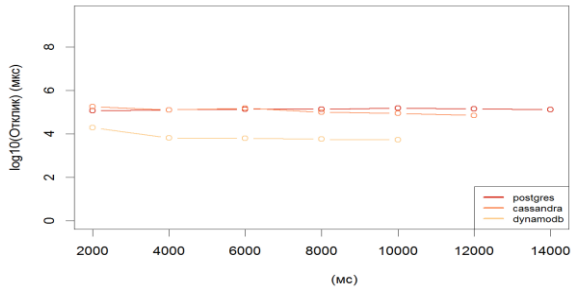


Рис. 1. Час відклику виконання JOIN при великих об'ємах даних

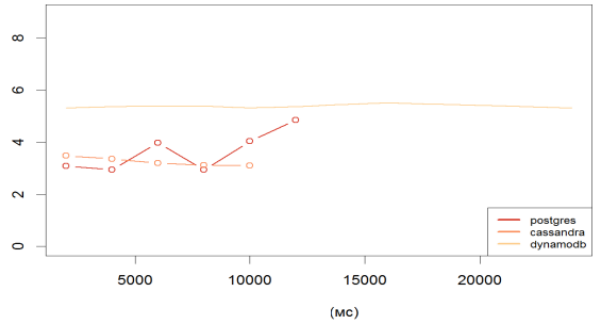


Рис. 2. Час відклику виконання update при середніх об'ємах даних

Були отримані дані про продуктивність представлених систем управління базами даних для набору різних запитів при описаній конфігурації. Отримані дані були проаналізовані, і за ним було зроблено висновок про продуктивність реляційної СУБД у порівнянні з NoSQL системами.

Список літератури

1. Apache HBase. [Електронний ресурс] - Режим доступу: - https://hbase.apache.org/

2.Amazon DynamoDB. [Електронний ресурс] - Режим доступу: - https://aws.amazon.com/documentation/dynamodb/

3. Apache Cassandra. [Електронний ресурс] - Режим доступу: - http://cassandra.apache.org/

4. MongoDB Atlas. [Електронний ресурс] - Режим доступу: - https://www.mongodb.com

5. Гайна Г.А. Організація баз даних і знань. Мови баз даних: Конспект лекцій.−К.:КНУБА, 2002. − 64 с.

УДК 621.397

В.І. Солодка, А.Ю. Чумак, Д.С. Ломенко
valyaonas@gmail.com, nastiachumak16@gmail.com, dima.lomenko@gmail.com
Державний університет інтелектуальних технологій та зв'язку, м. Одеса

ОЦІНКА ЯКОСТІ ЗОБРАЖЕНЬ, ЗАСНОВАНА НА ВИМІРЮВАННІ ВИДИМИХ СПОТВОРЕНЬ

Зображення широко використовуються в різних сферах, як повсякденному житті людини, так і в конкретних галузях науки. Очевидно, що якість зображень аналізованих користувачем грає не останню роль. Для зберігання зображень з високою якістю потрібні великі обсяги пам'яті, що може створювати неприйнятні ситуації при роботі з зображеннями. Залежно від вимог, що висуваються до зображення, існує можливість, варіюючи методи стиснення, отримувати прийнятні характеристики зображення. Кожен з алгоритмів і їх модернізації має ряд характеристик, аналізуючи які можна варіювати їх застосування в залежності від поставленого завдання.

В даний час існує достатня кількість напрямів поліпшення алгоритмів стиснення зображень з мінімальними похибками. В результаті виконання роботи ставиться завдання отримати порівняльний аналіз існуючих методів модифікації спектральних алгоритмів стиснення. Як критерій для порівняння пропонується аналізувати основні характеристики результату роботи методів і їх етапи роботи.

В даній роботі запропоновано метод візуальної оцінки якості, заснований на видимості похибки між початковим зображенням - оригіналом і спотвореним зображенням, використовуючи ледь помітну різницю при спектральному перетворені, а саме вейвлет-перетворенні (JND) [1]. Похибка, що перебуває нижче видимого порогу в кожній смузі частот ігнорується, у той час як деякі похибки, які перебувають у змістовній області, замасковані. За допомогою вимірювань видимих відмінностей двох входів і візуального маскування, була отримана формула оцінки зображень. Експерименти, проведені над випробувальними послідовностями групи VQEG, показали, що запропонований метод може досягти дуже гарної кореляції з суб'єктивними оцінками якості.

Середньоквадратична помилка (MSE) або пікове відношення сигнал/шум (PSNR) зазвичай використовується в області обробки сигналів як об'єктивна якісна метрика зображення. Одна з переваг, яка є важливої для швидкої роботи, це обчислювальна простота. Проте, відомо, що MSE або PSNR погано корелюють з якістю сприйняття в більшості додатків, тому що це засновано на вимірі точності відтворення в ЕЗ. Іншими словами, це не враховує властивостей зорової системи людини (HVS). Деякі спотворення, які знаходяться нижче порога або є замаскованим фоном, все ще вважаються як похибки в MSE або PSNR[2]. Ідея JND полягає в тому, що кожен сигнал кодується з граничним рівнем видимості похибки, нижче якого знаходяться невидимі похибки відновлення.

Розглянемо метрику якості зображення, яка вимірює сприйняту похибку між оригінальними і спотвореними зображеннями, використовуючи ледь помітну різницю при вейвлет-перетворенні JND. Вейвлет-перетворення було визнано одним з найбільш сильних методів для кодування зображення та аналізу з тих пір, як воно стало враховувати властивості зорової системи людини. Вимірюючи помітну різницю двох сигналів в вейвлет-підгрупах і локальне значення контрасту зображення, можна отримати кількісну оцінку якості зображення.

Розглянемо моделі зорової системи людини і ледь помітні спотворення (JND) при вейвлет-перетворенні. У зорової системи людини є багато фундаментальних властивостей, які включають чутливість яскравості, контрастну чутливість і маскування. Чутливість яскравості - нелінійна функція інтенсивності світла, що потрапляє в очі. Контрастна чутливість залежить від просторової і частотно-часової залежності подразника. Вона змінюється в залежності від рівня адаптації, пов'язаного з локальним середнім значенням яскравості. Контрастна чутливість зазвичай представлена функцією контрастної чутливості (CSF) [3], яка визначена як інверсія контрастного порогу, тобто мінімальний контраст, необхідний для спостерігача, щоб виявити мету. Маскування – дуже важливе явище в баченні. Видимість шуму може бути зменшена через виникнення іншого сигналу. Зазвичай обидва сигнали приблизно однакової частоти, в тому ж самому місці і тієї ж самої орієнтації. Маскування може відбутися в просторовій області або у часовій області.

Пороги ледь помітних спотворень при вейвлет-перетворенні. Основний поріг виявлення для дискретного вейвлет-перетворення виміряна, використовуючи примусову процедуру вибору з двома альтернативами. Відповідаючи даним результатів психофізичних експериментів математична модель порогового значення ледь помітної різниці (JND), сформульована як:

$$JND_{\lambda,\varphi}(r) = \frac{1}{M_{\lambda,\varphi}}\alpha 10^{\rho\left\{\log_{10}\left(g_\varphi f_0 2^{\lambda}/_{r}\right)\right\}^2} \quad (1)$$

де r– візуальний показник кількості екрану, який може бути визначений як:

$$r = dv\tan(\frac{\pi}{180}) \approx \frac{dv}{57.3} \quad (2)$$

v - відстань розглядання в см, d– показник роздільної здатності в ЕЗ/см. $M_{\lambda,\varphi}$– амплітуда дискретного вейвлет-перетворенні, основна функція, що відповідає рівню λі орієнтації φ; $\alpha, \rho, f_0 ig_{\varphi}$– константи.

Впершу чергу вкажемо основні позиції для базового алгоритму. Базовий алгоритм передбачає розбиття вихідного зображення на доменні і рангові блоки. Після чого для кожного рангу перебирають доменні блоки (для кожного варіанту орієнтації домен стискають до розмірів рангового блоку і визначають оптимальні значення коефіцієнтів перетворення методом найменших квадратів). Потім обчислюють нормоване значення параметра L, який характеризує відповідність отриманого стисненого доменного блоку в його орієнтації рангових блоку. Можливо два режими роботи алгоритму (з пошуком і без пошуку кращого домену). У режимі з пошуком кращого домену для кожного рангу перебираються всі домени, і вибирається з мінімальним L. У режимі без пошуку найкращого домену повний перебір доменів зупиняють, як тільки визначається такий *i*-й домен і його *j*-я орієнтація, що значення його параметра *L* не перевищує заданої допустимої похибки.

Тепер поетапно розглянемо існуючі методи для модифікації базового алгоритму. Найбільш поширеною модифікацією базового алгоритму є *FE*-алгоритм. З метою зниження обчислювальних витрат в *FE*-алгоритмі виділяють п'ять характеристик, які описують доменні і рангові блоки. І перш за все, проводиться саме їх порівняння[4]. Це значно скорочує обсяг обчислень. Ці характеристики: стандартне відхилення, асиметрія, між піксельна контрастність, коефіцієнт, що характеризує відмінності значень пікселів від значення центрального пікселя. При обробці рангового блоку обчислюють його вектор характеристик, потім обчислюють відстані між вектором характеристик даного рангу і вектором характеристик кожного домена. Процедура відбору доменів є своєрідним фільтром, який значно обмежує кількість доменів, які перебираються. Для прискорення процесу також є можливим в якості критерію оптимальності використовувати коефіцієнт кореляції Пірсона: *r'*(*R*, *D*). Чим краще реальна залежність *R* від *D* апроксимується лінійною, тим ближче за модулем до 1 буде їх коефіцієнт кореляції. Використання цього коефіцієнта дозволяє відразу оцінити оптимальність поточного домену для даного рангу, без розрахунку коефіцієнта перетворення контрасту і яскравості. Таким чином, ці коефіцієнти розраховуються один раз для кожного рангу. Виконується перетворення формул, що описують співвідношення для визначення коефіцієнтів яскравості та контрасту, через коефіцієнт кореляції.

Крім того, заздалегідь обчислюється середньоквадратичне відхилення яскравості пікселів рангів і доменів. Після цього стає можливим розглядати тільки ті домени, які задовольняють нерівності: тобто контрастність домену повинна бути вище контрастності рангу (пропонується підраховувати середнє значення яскравості пікселів для кожного рангу, а не коефіцієнт яскравості для кожного домена, що значно прискорює процес стиснення в середньому в 9,35 рази). Також існує можливість варіювати і інші характеристики: результат спектрального аналізу Фур'є, вейвлет аналізу, характеристики відтінку або текстури зображення. Крім того, алгоритм такого роду ефективно реалізований з використанням самоонавчанням карт Кохонена.

Для істотного скорочення часу обробки зображення дослідницький інтерес представляє сам алгоритм, оскільки ця операція повторюється багато разів і домінує в обчислювальної складності спектрального стиснення. Навіть незначне її спрощення дозволить отримати відчутний ривок в швидкості виконання всього алгоритму. Інший перспективною галуззю дослідження є скорочення числа доменів, що беруть участь в порівнянні з рангом, шляхом їх класифікації за числовим характеристикам, які можна вважати інваріантними щодо перетворень, що застосовуються до блокам. В результаті кількість порівнянь зменшується, а швидкість стиснення збільшується.

Список літератури

1. Barthel K. U., Schiittemeyer J., Voye T., Noll P., A new image coding technique unifying fractal and transform coding, in: Proc. ICIP-94 IEEE International Conference on Image Processing, Austin, Texas, Nov. 1994.
2. Bedford T., Dekking F.M., Keane M. S., Fractal image coding techniques and contraction operators, Nieuw Arch. Wisk. (4) 10,3 (1992) 185-218.
3. Breazu M., Toderean G., Region-based fractal image compression using deterministic search, IEEE ICIP 98, Chicago, Oct. 1998.
4. Bogdan A., Meadows H., E., Kohonen neural network for image coding based on iteration transformation theory, in: Proceedings from SPIE Neural and Stochastic Methods in Image and Signal Processing, Vol. 1766, pp. 425-436, 1992.
5. Boss R. D., Jacobs E. W., Archetype classification in an iterated transformation image compression algorithm, in: Fractal Image Compression Theory and Applications, Y. Fisher (ed.), Springer-Verlag, New York, 1994.

UDC 004.89

N.ZH. Sabitova[1], B.Sh. Razakhova[2], S.O. Gnatyuk[3].
[1]*Doctoral student Eurasian International University named after. L. N. Gumilev, Kazakhstan, Astana.*
[2] *t.s.d, associate pofessor L. N. Gumilyov Eurasian National University, Kazakhstan, Astana.*
[3]*Foreign consultant, t.s.d., professor National Aviational University, Ukraina, Kiev.*
[1]*sab_nazym@mail.ru,* [2]*utalina@mail.ru,* [3]*s.gnatyuk@nau.edu.ua*

AN ONTOLOGICAL MODEL FOR AUTOMATING THE PROCESS OF PREPARING ELECTRONIC COURSES IN THE FIELD OF INFORMATION AND COMMUNICATION TECHNOLOGIES

Annotation. Intelligent information technologies (IT) influence the processes in the economic, scientific, technical, humanitarian, educational and other fields of activity. Informatization or digitalization of the world society is focused on building an IT -oriented society. Knowledge engineering technologies are becoming significant. Ontological engineering can also be considered as a special case of knowledge engineering.

Keywords: *intelligent technologies, subject area, ontology.*

Modern IT uses Knowledge Management. We can say that success in this direction is determined by the level of efficiency of computer systems. As shown in, scientific research is being intensified on the creation of information systems based on knowledge bases, the development of methods for the ontological analysis of subject areas to extract aspects of the application of ontologies from them. The latter is of interest, for example, in the context of the development of electronic training courses (EC) and electronic textbooks (EC).

At the current stage of IT development, it has become possible to bring the existing theoretical foundations of artificial intelligence systems closer to real implementation, while taking into account the latest achievements of general engineering practice and subsequent promising trends in the development of computer technology in the preparation of relevant content of electronic courses in the field of ICT.

It should be noted that computerization of the educational process already at the level of secondary school or even primary classes, according to many authors, is a large-scale innovation in the field of education. It is impossible to imagine teaching in a modern school if a teacher does not use a variety of computer technologies and the Internet in his educational work. This is especially true for disciplines where content is updated rapidly, in particular, disciplines related to the field of information and communication technologies (ICT). Today, visual-figurative components of thinking occupy a predominant place in the worldview of modern schoolchildren who have many gadgets, starting with smartphones and ending with high-performance PCs or laptops. Which, accordingly, encourages teachers to present educational material in a visual expressive form, involving a diverse color palette, animation elements, dynamic illustrations, so characteristic of many modern EC and/or EC.

The study of the ICT course should introduce students to the methods of the most effective use of informatization tools in everyday practice. The examples given in the process of teaching students should clearly demonstrate that ICT tools are able to increase efficiency in the study of most disciplines that are taught within the framework of secondary schools and further colleges or universities.

Considering the above, we can state that the relevance of new research in this direction is justified by the need to develop effective methods of architectural and structural organization and synthesis of relevant content for EC and EC in the field of ICT, especially for the contingent of secondary school students. Such methods, in our opinion, enable all interested persons, starting with teachers in schools and colleges and ending with commercial structures offering their EC and/or EC on the educational services market, not only to design relevant EC and/or EC with the processing of subject knowledge, but also to digitalize the process of their synthesis based on processing colossal volumes of textual information of subject disciplines inherent in the content of the ICT field.

As a result of the research, the following main results were obtained:

a methodology for designing electronic courses (EC) and/or electronic textbooks (EC) in the field of ICT based on the application of an ontological model is proposed;

It is shown that the ontological model proposed in the article is intended primarily for the implementation of information technology for automated processing of ontologies of ICT subject areas, which will simplify procedures related to the implementation of EC and/or EC, based on relevant content in the field of ICS, corresponding to the current state of this subject area with the possibility of updating this content as necessary.

УДК 004.056

І.О. Супруненко, аспірант
науковий керівник д.т.н. проф. В.М. Рудницький
i.o.suprunenko.asp22@chdtu.edu.ua, rvn_2008@ukr.net
Черкаський державний технологічний університет, м. Черкаси

АДАПТИВНИЙ ПІДХІД ДО ЛОГУВАННЯ ЯК НОВИЙ ВИМІР СПОСТЕРЕЖНОСТІЗА ПРИКЛАДНИМ ПРОГРАМНИМ ЗАБЕЗПЕЧЕННЯМ

Написання комп'ютерних рішень сьогодні відбувається простіше, аніж це було навіть 25 років тому. Це, в свою чергу, робить розробника продуктивнішим та дозволяє швидше масштабувати результати розробки, використовуючи меншу кількість ресурсів. Однак, чим складніші та масштабніші програмні рішення, тим важче відслідковувати перебіг їх виконання та оцінювати поточний стан роботи. Це стосується як технічних аспектів, будь то мережа, серверне обладнання, пристрої вводу-виводу, так і власне самого коду. Потреба в належному рівні спостережності інформаційних систем зростає відповідно до складності даної системи. Коли ми говоримо про спостережність, зазвичай розуміють межу, до якої ми можемо зрозуміти, що відбувається всередині складної системи, користуючись лише інформацією, яку вона виводить назовні. Відповідно, чим вищий рівень спостережності – тим швидше та якісніше ми здатні оцінити та передбачити поведінку системи, без необхідності вносити корективи в процес роботи [1].

Для реалізації задач спостережності виокремлюють чотири важливих типи телеметрії:

- логи - незмінні, точні, стандартизовані повідомлення про події в системі;
- метрики - виміри стану системи – споживання процесорної квоти, використання оперативної пам'яті – протягом деякого часу;
- "сліди" (англ. trace) – записи цілісної сесії використання системи від інтерефейсу користувача до опрацювання запиту;
- залежності – взаємовідносини між складовими частинами системи;

Аспект логування представляє особливий інтерес, оскільки є найбільш наближеним та налаштовуваним, з прикладного рівня написання програм, засобом телеметрії. Інколи механізм дослідження логів є єдиним джерелом інформації для пошуку та вирішення проблем в системі, що перебуває в режими реальної роботи та опрацювання корисного навантаження [2]. Як для одного із найзручних механізмів реалізації належного рівня спостережності, існує багато праць та стандартів, як от "The Common Log Format"[3], що описує загальноприйнятий підхід до написання лог-повідомлень для веб серверів як Apache та проксі серверів як Squid. Це, в свою чергу, дозволяє системним адміністраторам досліджувати та ефективно виявлати неточності та помилки в роботі досліджуваного програмного забезпечення.

Одним із недоліків цих підходів до логування є відсутність механізму вказання бажаної підсистеми, деталізовану інформацію про яку ми хочемо отримати. Типовий формат лог повідомлення складається з:

- рівня критичності;
- часової мітки повідомлення;
- текстового вмісту;

Однак, наведена структура повідомлень не дає необхідної гнучкості для вирішення викликів, що з'являються в сучасних інформаційних системах. Наприклад, раніше програми були здебільшого монолітні, а сервери для проведення обчислень відносно часто перебували близько один біля одного, а тому виявлення неточностей в роботі системи могло спиратись на пошук проблеми в штучних умовах, як, наприклад, у випадку із Sun Microsystems та подіями, що передували випуску їх симетричного 64-бітного мультипроцесора в 1997 році [4]. Тоді проблема в роботі однієї з обчислювальних машин, що брала участь в процесі бенчмаркінгу, спотворювала метрики продуктивності при вимірюванні швидкодії системи із декількох комп'ютерів. І хоча причиною виявилась неправильна конфігурація, що перемикала одну з машин в режим роутера і просто здійснювала обмін пакетами по мережі між іншими учасниками експерименту без якогось корисного навантаження, складність при оцінюванні можливого джерела проблеми та затрати часу при перезбірці необхідних модулів (що інколи займало до 90хв) сповільнювали продуктивність та негативно впливали на результативність всього проекту.

Наразі ж, у світі глобалізованих систем, що охоплюють мільйони та десятки мільйонів користувачів, розташованих географічно в різних куточках планети, і, як наслідок, для яких необхідний пошук інших підходів в розташуванні обчислювальних потужностей та датацентрів, аніж це було в минулому, більш гнучкі підходи до спостережності цілком ймовірно можуть досить відчутно покращити процес роботи.

Для більш ефективного опрацювання та точнішої конфігурації механізму логування пропонується використати механізм тегування повідомлень згідно з логічними частинами системи, до яких вони належать. Пропонується назва "адаптивний підхід до логування", де "адаптивність" означає "можливість слідкувати за конкретною частиною системи". Формально ми можемо представити його як:

$$f_i(L_{adp}) = f(Sev, T_{incl}, T'_{excl})$$, де

i – ітерація інстанціювання механізму логування,
Sev – бажаний рівень критичності повідомлень для поточної ітерації,
T_{incl} – множина тегів, які ми хочемо включити у вивід,
T'_{excl} – множина тегів, які необхідно виключити із виводу (може бути порожня).

Схематично запропонований підхід має такий вигляд:

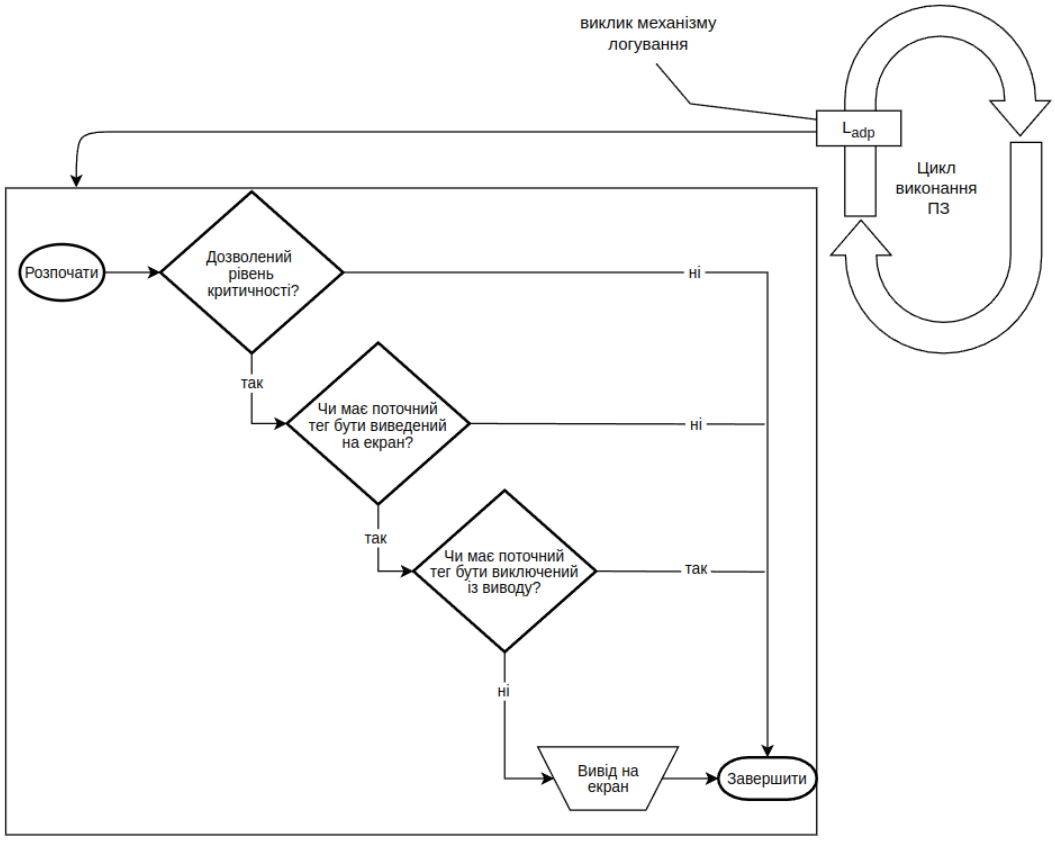


Рис. 1. Загальна схема вбудовування адаптивного логування в цикл виконання ПЗ

Відтак, володіючи новим, більш точним інструментарієм, розробник матиме змогу вести спостереження не лише керуючись загальним підходом критичності повідомлень, а також орієнтуючись на конкретні системи та підсистеми, які представляють особливий інтерес в даний момент. Маючи цю інформацію ми з одного боку здатні мінімізувати вплив на поточний процес виконання надмірним виводом інформації, що не представляє зараз для нас інтересу, а з іншого — отримуємо змогу більш аргументовано та точно досліджувати метрики виконання тієї чи іншої частини програмного коду.

Список літератури

1. What is observability? | IBM. URL: https://www.ibm.com/topics/observability.
2. S. Gu, G. Rong, H. Zhang and H. Shen, "Logging Practices in Software Engineering: A Systematic Mapping Study," in IEEE Transactions on Software Engineering, vol. 49, no. 2, pp. 902-923, 1 Feb. 2023, doi: 10.1109/TSE.2022.3166924.
3. RFC 6872 The Common Log Format (CLF) for the Session Initiation Protocol (SIP): Framework and Information Model
4. Bryan Cantrill. 2006. Hidden in Plain Sight:. Queue 4, 1 (February 2006), 26–36. https://doi.org/10.1145/1117389.1117401

УДК 004.921

О. С. Ткаченко студент, Є. В. Мелешко, д.т.н., професор
alex.tranduil@gmail.com, elismeleshko@gmail.com
Центральноукраїнський національний технічний університет, м. Кропивницький

ДОСЛІДЖЕННЯ МЕТОДІВ КОМП'ЮТЕРНОЇ ГРАФІКИ ДЛЯ ЗАЛИВКИ ПЕВНОЇ ОБЛАСТІ НА ЗОБРАЖЕННІ

Заливка – алгоритм, що визначає область, «пов'язану» з певним елементом у багатовимірному масиві (найчастіше це двовимірний масив точок растрового зображення). Він використовується в інструменті заповнення «ковша» програм для малювання, щоб заповнити з'єднані області однакового кольору іншим кольором.

Метою даної роботи було порівняння трьох методів заливки: методу рекурсивної заливки, методу правої руки, методу сканування рядків, – та визначення який з них краще за певними критеріями.

Метод рекурсивної заливки

Алгоритм рекурсивної заливки використовується для заповнення області, що зафарбовується на зображенні або в графічному редакторі. Він ґрунтується на принципі рекурсії і працює наступним чином:

1) Задається початкова точка (координати пікселя) для заливки.

2) Перевіряється колір цієї точки. Якщо він збігається з кольором, яким потрібно заливати, алгоритм переходить до наступного кроку. Якщо колір відрізняється, алгоритм завершується.

3) Закрашується поточна точка новим кольором.

4) Рекурсивно викликається алгоритм для сусідніх точок (верхньої, нижньої, лівої, правої). При цьому перевіряється колір кожної сусідньої точки і якщо він збігається з початковим кольором, алгоритм повторно викликається для неї.

5) Алгоритм продовжує викликатися рекурсивно для всіх сусідніх точок, доки не будуть перевірені всі точки в області.

Цей алгоритм дозволяє швидко заповнити область певного кольору на зображенні і може використовуватися для різних цілей, наприклад, для малювання, редагування або обробки даних.

Метод правої руки

Метод правої руки – використовує алгоритм заливання закритих областей на зображенні, який ґрунтується на русі "правої руки" вздовж кордону області. Алгоритм методу правої руки починається з вибору точки усередині області, яку потрібно заповнити. Потім алгоритм рухається по межі області, дотримуючись правила "правої руки". Якщо межа знаходиться ліворуч від напрямку руху, алгоритм повертає праворуч. Якщо межа знаходиться праворуч, алгоритм продовжує рух уперед. Алгоритм продовжує рухатися вздовж кордону доти, доки повернеться у початкову точку. У процесі руху по кордоні алгоритм заповнює пікселі всередині області певним кольором або значенням.

Переваги методу правої руки включають простоту реалізації та ефективність для простих та складних областей. Алгоритм також може бути легко модифікований для роботи з різними типами кордонів.

Однак метод правої руки може зіткнутися з проблемами при обробці складних областей із самоперетинами або внутрішніми отворами.

Метод сканування рядків

Метод сканування рядків (scanline fill) – використовується для заливання закритих областей на зображенні. Він ґрунтується на скануванні кожного рядка зображення та визначенні, чи потрібно заповнити пікселі всередині області чи ні.

Алгоритм сканування рядків при заливці починається з вибору точки всередині області, яку потрібно заповнити. Потім алгоритм сканує кожен рядок зображення, починаючи з вибраної точки і рухаючись горизонтальною віссю. У кожному рядку алгоритм перевіряє кожен піксель щодо належності області. Якщо піксель знаходиться в області, він заповнюється певним кольором або значенням.

Переваги методу сканування рядків при заливці включають простоту реалізації та невелику кількість обчислень, оскільки алгоритм працює лише з пікселями всередині області.

Однак, цей метод може бути неефективним для складних або великих областей, оскільки він вимагає сканування кожного пікселя всередині області.

Експериментальне дослідження різних методів заливки

Вказані алгоритми було реалізовано мовою програмування Python та порівняно їх за такими критеріями при різних вхідних даних: результат програми, швидкодія, кількість повторень циклу, об'єм пам'яті файлу.

Для того щоб не використовувати додаткові бібліотеки, було вирішено замість певного малюнка використовувати матрицю 7x7 для заливки, так як матриця являє собою область пікселів зображення.

У таблиці 1 наведено результати проведених нами порівняльних експериментів.

Таблиця 1

Результати порівняльних експериментів різних методів заливки

		Вхідна матриця		
		Проста ціла область	Складна область з проміжками	Дві області (заливаємо просту)
Критерії	Метод заливки	Проста вхідна матриця (рис. 1)	Складна вхідна матриця (рис. 2)	Вхідна матриця з двома областями (рис. 3)
Результат	Рекурсивний	+	+	+
	Правої руки	+	-	+
	Сканування рядків	+	+	+
Кількість повторень	Рекурсивний	37	85	45
	Правої руки	9	-	12
	Сканування рядків	37	75	42
Час	Рекурсивний	1.0728836059570312e-05	1.52587890625e-05	2.1219253540039062e-05
	Правої руки	2.2172927856445312e-05	-	2.384185791015625e-05
	Сканування рядків	2.0503997802734375e-05	5.2928924560546875e-05	3.6716461181640625e-05
Об'єм пам'яті файлу (байт)	Рекурсивний	2315		
	Правої руки	3109		
	Сканування рядків	2249		

```
matrix = [
    ['-', '-', '-', '-', '-', '-', '-'],
    ['-', '-', '-', '-', '-', '-', '-'],
    ['-', '-', 'X', 'X', 'X', '-', '-'],
    ['-', '-', 'X', 'X', 'X', '-', '-'],
    ['-', '-', 'X', 'X', 'X', '-', '-'],
    ['-', '-', '-', '-', '-', '-', '-'],
    ['-', '-', '-', '-', '-', '-', '-']
]
```

Рис. 1. Проста вхідна матриця

```
matrix = [
    ['X', 'X', 'X', '-', '-', '-', '-'],
    ['-', '-', 'X', 'X', 'X', '-', '-'],
    ['X', 'X', 'X', '-', '-', '-', '-'],
    ['-', '-', 'X', 'X', 'X', '-', '-'],
    ['X', 'X', 'X', '-', '-', '-', '-'],
    ['-', '-', 'X', 'X', 'X', '-', '-'],
    ['X', 'X', 'X', '-', '-', '-', '-']
]
```

Рис. 2. Складна вхідна матриця

```
matrix = [
    ['-', '-', '-', 'X', '-', '-', '-'],
    ['-', '-', '-', 'X', 'X', '-', '-'],
    ['-', 'X', 'X', '-', 'X', 'X', '-'],
    ['-', 'X', '-', 'X', '-', 'X', '-'],
    ['-', 'X', '-', 'X', '-', 'X', '-'],
    ['-', 'X', '-', 'X', '-', 'X', '-'],
    ['-', 'X', 'X', 'X', '-', '-', '-']
]
```

Рис. 3. Вхідна матриця з двома областями

Як бачимо з результатів дослідження: метод правої руки не впорався з складною областю, але правильно залив вказану область з двох областей, так як вона була проста; по кількості повторень циклу алгоритм рекурсії виявився найбільш повторюваним, а метод правої руки найменш повторюваним; за часом алгоритм рекурсії однозначно найшвидший; метод сканування рядків потребує менше всього пам'яті.

Висновки. Можемо зробити висновок, що алгоритм рекурсії є найбільш оптимальним для застосування, хоча при обмеженій кількості пам'яті краще підійде метод сканування рядків, а для простих областей та контурів – метод правої руки. Отже, обираючи алгоритми заливки треба чітко оцінити: яку задачу буде вирішувати алгоритм, з якими областями він буде працювати, чи важлива швидкість і об'єм пам'яті, чи має значення кількість повторень циклу програми; та врахувати особливості кожного алгоритму, щоб уникнути помилок і проблем.

Список літератури

1. Henrich, Dominik (1994). Space-efficient region filling in raster graphics. The Visual Computer. pp. 205–215. doi:10.1007/BF01901287

2. Flood fill – [Електронний ресурс]. – Режим доступу: https://en.wikipedia.org/wiki/Flood_fill

UDC 519:004.8

I. Aksonova[1], Master student
in the specialty «Cyber security and information protection»,
T. Milevska[1], Master student
in the specialty «Cyber security and information protection»
S. Yevseiev[1], Doctor of technical science, Professor,
Head of the Cybersecurity Department,
ivaksyonova@gmail.com, milevskats@gmail.com serhii, yevseiev@gmail.com
[1]National Technical University
«Kharkiv Politechnical Institute», Kharkiv

WEB ANALYTICS: BASIC PRINCIPLES OF USE IN BUSINESS DIGITIZATION CONDITIONS

In today's world, the processes of digitalization of business occupy an increasingly significant place, which involves its transformation, high customer orientation, the use of digital technologies to optimize business processes and increase the efficiency of the company's work. This trend is related to the rapid processes of digitization of society, the introduction of technological innovations, the spread of access to Internet resources, and the increase in the use of mobile devices. All this creates new opportunities for business structures and organizations in any spheres of socio-economic life in terms of improving the quality of customer service, establishing communication within the company, automating production, financial, information and other processes. As a result of the introduction of digital technologies, the differentiation of communication channels, the development of e-commerce and social media tools, business entities interact more effectively with their consumers and attract new customers. Digitalization of business and transition to the Internet allows business structures to work effectively even in difficult economic conditions and force majeure circumstances.

The main modern trends of digital business are:

rapid adaptation of websites and various applications of business structures for mobile devices, due to the increase in mobile traffic;

an increase in the use of data by enterprises and organizations about users of their goods and services to customize offers and recommendations, which is associated with the strengthening of information personalization processes;

the expansion of social influence on consumers through social media tools, which is due to the spread of access to Internet resources of various population groups;

the spread of technological process automation, the formation of databases and Big Data analysis, the use of machine learning and intelligent analysis, which helps enterprises make informed management decisions in conditions of uncertainty and challenges of the internal and external environment.

In these conditions, a special role is assigned to web analytics, which is an integral part of successful website promotion and business management. Web analytics is carried out using various tools and technologies, the most popular of which are:

Google Analytics, aimed at detecting the behavior of users and their interaction with the product or service on websites and applications of business structures, which helps businesses adjust and improve their strategies, that is, effectively manage their activities;

Adobe Analytics, which provides extensive opportunities for measuring and analyzing data based on Big Data;

Piwik PRO, which is a private analytics platform that allows the collection, analysis and reporting of website user data and provides a high level of data protection;

Matomo, which is an open source web analytics system that gives you full control over your data.

All web analytics tools are aimed at collecting, analyzing and interpreting data on such basic indicators as the number of visitors, traffic sources, number of page views, bounces, geography of customers and their demographic characteristics, time spent on the site, conversions, etc. The system of monitoring and control of indicators can be presented in the form of the following diagram, fig. 1.

The monitoring system includes a database, that is, information and analytical support of the process, which is expressed in the form of certain indicators, and a knowledge base, that is, methodical support, which includes a set of methods used in web analytical activities.

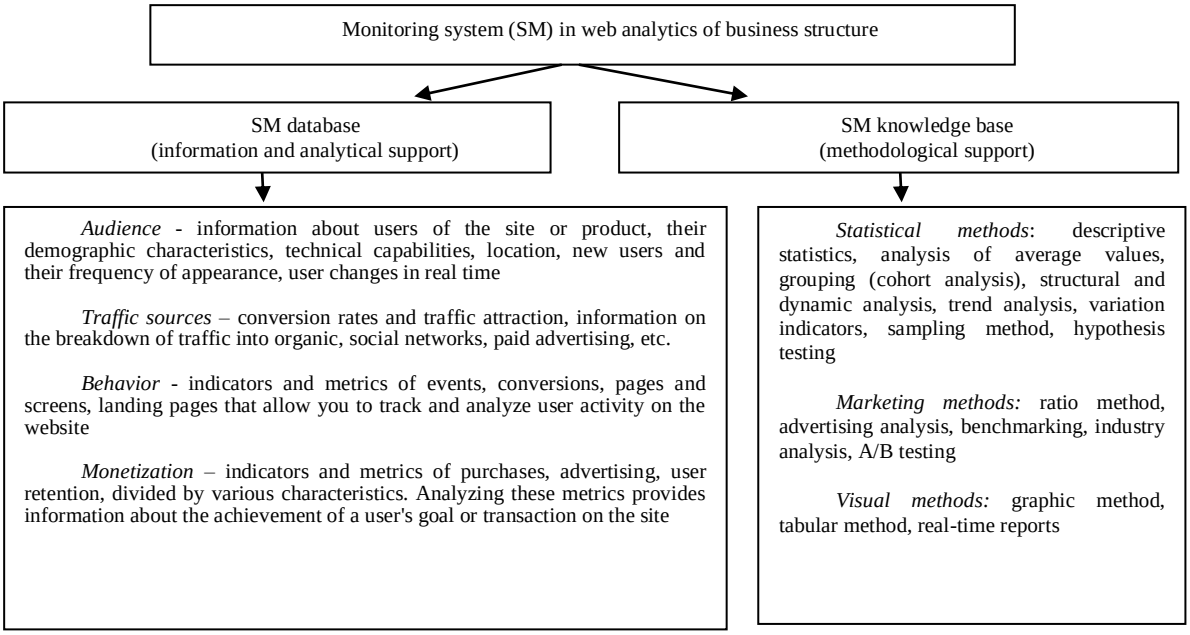


Fig. 1. Monitoring system (SM) in web analytics of the business structure

The main principle of operation of web analytical tools in the implementation of SM is to direct them to monitor the results of the activities of business structures in the online environment and measure the key performance indicators (KPI) of the business. As a result, the identified problems and possibilities of the website of the business structure are analyzed in order to improve it. In general, on the basis of information from web analytics, reasonable management decisions are made on the development of business structure development strategies, especially in the digital environment.

It should be noted that the combination of web analytics and digital business occurs at all stages of the development of the business structure. On the one hand, web analytics allows you to obtain information on the basis of which management decisions are made regarding financial, marketing, production and other strategies and directions of development of the business entity. On the other hand, digital business opportunities are aimed at the distribution of web analytics tools to collect data on the effectiveness of advertising companies, analyze user behavior, evaluate marketing channels, test, improve the website in order to achieve the best results in the work of a particular business.

Recently, the use of artificial intelligence and machine learning has become an increasingly popular tool in web analytics. The application of intelligent data analysis and machine learning algorithms allows automating the processes of data collection, storage, analysis, making forecasts and formulating recommendations based on large volumes of information. All this helps web analytics to reveal complex interdependencies between indicators and processes in user behavior, which allows business structures to make better management decisions.

The development of web analytics takes place permanently, taking into account constant changes in information technologies; new trends in digital marketing and the economy as a whole; expanding the volume of data and increasing the number of their sources; increasing the role of analytics in real time; development of mobile analytics; new requirements for data privacy and data security.

In the era of digital transformations, business recommendations for the successful use of web analytics include the following:

clear definition of the purpose of the analysis and formation of those indicators that must be measured, investigated and achieved;

selection of appropriate web analytics tools that best meet the needs and capabilities of the analysis;

conducting constant analysis and control of business structure indicators, their correction and making the necessary changes in the operational goals of the business in order to achieve the strategic goal of the company.

Adherence to these recommendations for conducting web analytics of the business structure will reveal potential problems and opportunities to improve development efficiency; to improve interaction with customers based on the study of their behavior and requests; make informed management decisions regarding business development in general.

УДК 004.4

Б.Ю. Вінтенко[1], І. В. Миронець[1] С.А. Смірнов[2], К.О. Буравченко[2], О.А. Смірнов[2]
boris.vintenko@gmail.com, i.myronets@chdtu.edu.ua, smirnov.ser.81@gmail.com,
buravchenkok@gmail.com, dr.SmirnovOA@gmail.com
Черкаський державний технічний університет, м. Черкаси
Центральноукраїнський національний технічний університет, м. Кропивницький

ДОСЛІДЖЕННЯ ВИМОГ IEC 60880 ТА IEC 62138 З РОЗРОБКИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНО-КЕРУЮЧИХ СИСТЕМ АЕС

На сьогоднішній день значна частина електричної енергії виробляється атомними електростанціями. Атомна енергетика – це дешевий, економічно вигідний та екологічний спосіб забезпечення потреб людини електроенергією. Разом з тим, це виробництво пов'язане з необхідністю забезпечення захисту людини та навколишнього середовища від іонізуючого випромінювання ядерного палива під час нормальної експлуатації станції та при виникненні аварійних ситуацій. Атомні електростанції (АЕС) містять велику кількість обладнання для забезпечення технологічних процесів та виконання функцій безпеки.

Метою роботи є дослідження вимог до формування життєвого циклу, основних етапів проектування і документуванням програмного забезпечення комп'ютерних систем управління атомних електростанцій (ПЗ КСУ АЕС), що виконують функції безпеки категорій «А», «В» та «С». Вимоги до ПЗ, що виконує функції безпеки категорії «А», наведені в міжнародному стандарті IEC 60880 «Nuclear power plants – Instrumentation and control systems important to safety – Software aspects for computer-based systems performing category A functions», вимоги до ПЗ, що виконує функції безпеки категорії «В» і «С», наведені в міжнародному стандарті IEC 62138 «Nuclear power plants – Instrumentation and control important for safety – Software aspects for computer-based systems performing category B or C functions».

Об'єктом дослідження є процес розробки програмного забезпечення для комп'ютерних систем управління АЕС.

Предметом є дослідження вимог міжнародних стандартів IEC 60880 та IEC 62138 з розробки програмного забезпечення інформаційно-керуючих систем АЕС, важливих для безпеки.

Аналіз останніх досліджень і публікацій. Функції безпеки в залежності від наслідків відмови і хибного спрацювання класифікують за категоріями. У різних нормативних документах класифікація функцій безпеки може відрізнятися. У відповідності з міжнародним стандартом IEC 61226 («КСУ АЕС ВБ. Розподіл за категоріями ФБ») [4] виділяють 3 категорії функцій безпеки: «А», «В» та «С». У відповідності з нормативним документом МАГАТЕ «Safety Classification of Structures, Systems and Components in Nuclear Power Plants: Specific Safety Guide No. SSG-30» [5] виділяють 3 класи безпеки: «1», «2» та «3». З метою уникнення дублювання класифікації категорій в даній статті буде використовуватися позначення категорій за допомогою літер «А», «В» та «С», як вказано в стандарті IEC 61226. Функції категорії «А» є найбільш важливими для попередження або захисту під час аварійних ситуацій, функції категорій «В» та «С» мають менший ступінь важливості. Всі пристрої, системи і компоненти, включаючи програмне забезпечення (ПЗ) для контроля і управління, що являються елементами, важливими для безпеки, повинні бути визначені, а потім класифіковані на основі функції, що виконується, і важливості для безпеки. Огляд класифікації комп'ютерних систем управління (КСУ) і програмного забезпечення (ПЗ) у відповідності із стандартами і нормативними документами наведений у [12].

Загальна структура вимог стандартів IEC 60880 та IEC 62138

Область застосування. У розділі 1 обох стандартів областю застосування вказуються вимоги до ПЗ комп'ютерних систем управління, що виконують функції безпеки категорії «А» (IEC 60880) і «В» і «С» (IEC 62138). Мета цих вимог – створення ПЗ високого ступеню надійності, яке має мінімальну імовірність наявності прихованих програмних дефектів.

Нормативні посилання. У розділі 2 обох стандартів міститься перелік нормативів, що мають відношення до розробки ПЗ КСУ АЕС, важливих для безпеки. Це стандарти IEC 61508, IEC 61513, IEC 61226, нормативні документи МАГАТЕ тощо.

Терміни та визначення, скорочення. У розділі 3 обох стандартів визначаються поняття, які використовуються при формуванні вимог. Серед цих термінів та визначень необхідно відмітити найголовніші: універсальна мова, проблемно-орієнтована мова, раніше розроблене ПЗ, автоматизована генерація коду, ущільнення коду, самоконтроль, різноманітність тощо.

У розділі 4 обох стандартів наводиться список використовуваних скорочень та абревіатур.

Детальні вимоги. Починаючи з розділу 5, в обох стандартах наводиться основна частина вимог до розробки ПЗ.

Типи ПЗ та даних. Стандарти розробки ПЗ КСУ АЕС поділяють програмне забезпечення на типи: операційне ПЗ та прикладне ПЗ. Кожне ПЗ використовує конфігураційні дані, які також поділяються на категорії: незмінні (є частиною специфікації проекту) та змінні (можуть бути змінені оперативним персоналом в необхідних межах).

Етапи життєвого циклу ПЗ. Стандарт IEC 61513 описує життєвий цикл (ЖЦ) КСУ в цілому та визначає заходи, які мають відбуватися на всіх його етапах. Згідно концепцій цього стандарту, програмне забезпечення є невід'ємною частиною КСУ, ЖЦ ПЗ тісно пов'язаний з ЖЦ всієї системи. Стандарти КСУ IEC 60880 та IEC 62138 містять вимоги до ЖЦ ПЗ та конкретизують види діяльності, що відносяться до розробки ПЗ. Вони розглядають розробку апаратного та програмного забезпечення як паралельні процеси, які об'єднуються на етапі інтеграції.

В таблиці 1 наведені етапи ЖЦ КСУ АЕС, види діяльності з розробки в межах цих етапів та номери підрозділів стандартів IEC 60880 та IEC 62138, що описують вимоги до відповідного виду діяльності.

Виходячи з структури вимог до розробки ПЗ КСУ АЕС, можна виділити окремі групи учасників цього процесу та побудувати схему взаємодії між ними.

Групи учасників, які приймають участь в розробці ПЗ КСУ АЕС

Одним з результатів дослідження вимог стандартів до розробки ПЗ КСУ АЕС є розподілення учасників розробки на функціональні групи. Це дає можливість створити колектив учасників з відповідними компетенціями та спроектувати їх комунікацію між собою. Наступний розділ описує можливий варіант розподілу видів діяльності з розробки ПЗ між групами.

Розподілення видів діяльності з розробки ПЗ між групами

Слід зазначити, що розподілення вимог стандарту між учасниками не усуває необхідність знайомства окремих учасників з повним змістом всього стандарту. Проте головний **висновок** цього розподілення вказує на те, що при підготовці до розробки ПЗ з урахуванням вимог стандартів IEC 60880 та IEC 62138 учасники груп можуть визначити, які розділи та вимоги стандартів, види діяльності стосуються їх першочергово, а які – опосередковано.

Аналіз вимог загальних вимог та вимог до етапу розробки специфікації ПЗ

Керування проектуванням, планування та створення специфікації вимог до ПЗ є процесами, які є підготовчими до створення проекту та реалізації ПЗ розробниками.

Аналіз вимог до етапу проектування та реалізації ПЗ

Вимоги стандартів до розробки ПЗ значно відрізняються в залежності від категорії. Стандарт IEC 60880 зобов'язує дотримуватися правил кодування та наводить велику кількість детальних рекомендацій. Стандарт IEC 62138 містить загальні вимоги з дотримання правил кодування без їх зазначення.

Аналіз вимог до етапу верифікації, інтеграції та валідації

Після завершення реалізації ПЗ розробниками мають відбутися етапи верифікації ПЗ, інтеграції ПЗ до КСУ та валідації ПЗ в складі КСУ. Мета цих етапів – перевірити якість розробленого ПЗ та відповідність його специфікації вимог. Будь-який етап може створити ітерацію в процесі розробки при виявлені дефекту. В цьому випадку інформація про винайдений дефект повинна бути передана розробникам ПЗ для аналізу та усунення, після чого має відбутися повторна перевірка.

Глибина верифікації та валідації залежить від категорії функціональної безпеки ПЗ. Наприклад, одна з основних особливостей верифікації ПЗ категорії «А» – необхідність верифікації його реалізації: архітектури та вихідного коду.

Аналіз вимог до етапу встановлення експлуатації та модифікації

Функціональна безпека КСУ забезпечується за умови вірного встановлення та кваліфікованої експлуатації її програмного забезпечення. Це можливо завдяки постійному контролю за станом ПЗ на місці експлуатації кваліфікованим персоналом. Персонал, що експлуатує КСУ, повинен мати зв'язок з представниками розробника для передачі інформації про виявлені аномалії в роботі та загальний досвід експлуатації системи.

Засоби імплементації вимог

Як приклад, дотримання вимог стандартів розробки дозволило науково-виробничому підприємству «Радій», провідним інженером-програмістом якого є автор, розробити та поставити велику кількість КСУ на АЕС України, Болгарії, Канади, Аргентини та інших країн станом на 2023 рік. Ці КСУ успішно експлуатуються протягом багатьох років.

Проблема оцінки відповідності стандарту

Можна відмітити, що в стандартах розробки ПЗ КСУ АЕС не наводиться конкретних методик оцінки та метрик відповідності ПЗ цим стандартам. Виходячи з цього, оцінка відповідності ПЗ вимогам стандартів включає суб'єктивну складову і залежить від методів перевірки, що використовуються в конкретній організації.

У результаті дослідження розглянута загальна структура вимог стандартів IEC 60880 та IEC 62138, визначені групи учасників, які приймають участь в розробці ПЗ КСУ АЕС та розподілення видів діяльності з розробки ПЗ між цими групами, проведений аналіз вимог загальних вимог та вимог до етапу розробки специфікації ПЗ, вимог до етапу проектування та реалізації ПЗ, вимог до етапу верифікації, інтеграції та валідації та вимог до етапу встановлення, експлуатації та модифікації, сформована таблиця розподілення вимог до ПЗ, досліджені засоби імплементації вимог, визначена проблема оцінки відповідності стандарту.

Висновки. Міжнародні стандарти IEC 60880 та IEC 62138 містять важливі вимоги до всіх етапів розробки ПЗ КСУ АЕС, важливого для безпеки. Вимоги стосуються як організаційних питань, так і технічних аспектів. Згідно з цими стандартами, кожне підприємство, що займається розробкою ПЗ КСУ АЕС, має визначити робочі групи, які будуть реалізовувати різні етапи ЖЦ (проектування, реалізація, верифікація тощо). Стандарти не містять вимог до інтерфейсів користувача ПЗ. Тому одним з напрямків наступних досліджень стануть вимоги інших міжнародних стандартів – IEC 61772 «Nuclear power plants – Control rooms – Application of visual display units (VDUs)» («Візуальні пристрої відображення») та IEC 62646 «Nuclear power plants – Control rooms – Computer-based procedures» («Комп'ютеризовані процедури»), а також вимоги галузевих нормативних документів, таких як NUREG-0700 «Human-System Interface Design Review Guidelines» – «Побудова інтерфейсів «людина-машина» (U.S. Nuclear Regulatory Commission, США). В стандартах не визначається загальноприйнятих метрик, що вказують ступінь відповідності ПЗ даним стандартам. Виходячи з цього, кожна організація, яка виконує оцінку відповідності ПЗ та КСУ в цілому вимогам стандартів, повинна створити власну методику такої оцінки. Тому метою наступних досліджень є вивчення засобів оцінки специфікацій вимог, метрик коду ПЗ, критеріїв повноти тестування ПЗ, які можуть бути використані для розробки формальних методик оцінювання ПЗ вимогам стандартів.

Список літератури

1. Nuclear power by country. [Електронний ресурс] – Режим доступу: https://en.wikipedia.org/wiki/Nuclear_power_by_country.
2. IEC61508-2010: Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements. Geneva, International Electrotechnical Commission (IEC), 2010.
3. IEC61513-2011: Nuclear power plants – Instrumentation and control important to safety – General requirements for systems requirements. Geneva, International Electrotechnical Commission (IEC), 2011.
4. IEC61226-2009: Nuclear power plants – Instrumentation and control important to safety – Classification of instrumentation and control functions. Geneva, International Electrotechnical Commission (IEC), 2009.
5. Safety Classification of Structures, Systems and Components in Nuclear Power Plants: Specific Safety Guide No. SSG-30. Vienna, IAEA, 2014.
6. IEC60880-2006: Nuclear power plants – Instrumentation and control systems important to safety – Software aspects for computer-based systems performing category A functions. Geneva, International Electrotechnical Commission (IEC), 2006.
7. IEC62138-2004: Nuclear power plants – Instrumentation and control important for safety – Software aspects for computer-based systems performing category B or C functions. Geneva, International Electrotechnical Commission (IEC), 2004.
8. Tor Stålhane, Vikash Katta, Thor Myklebust. Scrum and IEC 60880. Norwegian University of Science and Technology, 2013.
9. IEC61772:2009: Nuclear power plants — Control rooms — Application of visual display units (VDUs). Geneva, International Electrotechnical Commission (IEC), 2009.
10. IEC62646-2019: Nuclear power plants – Control rooms – Computer based procedures. Geneva, International Electrotechnical Commission (IEC), 2012.
11. NUREG-0700 Revision 3. Human-System Interface Design Review Guidelines. U.S. Nuclear Regulatory Commission, 2020.
12. Вінтенко Б.Ю., Смірнов О.А., Коваленко О.В., Смірнов С.А., Коваленко А.С. «Дослідження нормативних документів та галузевих стандартів розробки програмного забезпечення комп'ютерних систем управління АЕС, важливих для безпеки». *Системи управління, навігації та зв'язку*, 2023, вип. 2(72), С. 161-180.

УДК 004

Я.О. Козлов, С.А, Смірнов, О.В. Кравчук, О.А. Смірнов
kozlov.yan1@gmail.com, smirnov.ser.81@gmail.com, lerotka@i.ua, dr.SmirnovOA@gmail.com
Центральноукраїнський національний технічний університет, м. Кропивницький

ДОСЛІДЖЕННЯ ОСОБЛИВОСТЕЙ СУЧАСНИХ SIEM-СИСТЕМ

SIEM-система (англ. Security Information and Event Management) – централізований хаб для обробки, аналізу безпекових даних та реагування на загрози до того як вони нанесуть певну шкоду.

Іншими словами SIEM – це додаток який надає можливість отримувати дані безпеки з компонентів інформаційно-комунікаційних систем та представляти їх як корисну інформації в єдиному місці [6]

Аналіз сучасних рішень SIEM-системи показує, що хоч усі вони і мають спільні властивості та функціонал (навіть можуть інтегруватися одне з одним), кожне рішення поступово запроваджує передові рішення та технології у сфері інформаційних технологій загалом.

В роботах [1-5] розглядаються основні рішення SIEM-систем та їхня роль у забезпеченні інформаційної безпеки, але, на думку авторів цієї публікації, дані дослідження не повною мірою охоплюють сучасні рішення, особливо вільні з відкритим кодом, та можливості таких систем.

Таким чином дослідження сфокусоване на досліджені особливостей сучасних SIEM-систем.

З розвитком машинного навчання різноманітні продукти почали запроваджувати його у своїх цілях – загалом, пошук патернів у великій кількості даних та, відповідно, покращення рекомендацій. SIEM-системи не залишилися повз і також використовують машинне навчання, до того ж велика кількість даних з однієї системи (загального інформаційно-комунікаційного середовища як єдиного цілого) є сприятливим підґрунтям для навчання нейронної мережі помічати аномалії у поведінці тих чи інших компонентів системи, на які звичайний спеціаліст міг би і не звернути уваги (наприклад, підключення до системи у позаробочий час).

Також, не кожна організація може дозволити собі виділити достатньо потужну апаратуру для цілодобової роботи системи, яка особливо і не захищає організацію. Зважаючи на це, основні рішення SIEM-систем надають можливість розгортати відповідну інфраструктуру у хмарному середовищі, перетворюючи SIEM на сервіс.

Такий підхід, з одного боку, перешкоджає фізичній ізоляції внутрішньої частини інформаційної системи, пов'язуючи її з хмарою, але водночас зберігає усі переваги SIEM-системи та за належної конфігурації нівелює недоліки.

До того ж, такий підхід є оптимальним у випадку знаходження частини компонентів інформаційної системи у хмарі, адже популярні SIEM-системи мають багату палітру інтеграцій з усіма основними хмарними провайдерами.

Також, як зазначалося раніше, більшість розробників SIEM ідуть в парі з агентами для кінцевих точок. Такі агенти можуть не тільки відправляти на сервер потрібну інформацію, але й виконувати роль антивіруса чи сканера вразливостей локального хоста, та, що особливо важливо, автоматично ізолювати уражені хости від мережі у випадку поміченої загрози, забезпечуючи безпеку решти системи.

Список літератури

1. Кількість кібератак під час війни зросла втричі. [Електронний ресурс]. Доступно: https://cip.gov.ua/ua/news/kilkist-kiberatak-pid-chas-viini-zrosla-vtrichi. Дата звернення: Вер. 27, 2023.

2. Billy K Leung, "Security Information and Event Management (SIEM) Evaluation Report", May 2021. [Online]. Available: https://scholarworks.calstate.edu/downloads/41687p49q. Accessed on: Sep. 28, 2023.

3. Gustavo González-Granadillo, Susana González-Zarzosa, Rodrigo Diaz. "Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures", July 12, 2021. [Online]. Available: https://www.mdpi.com/1424-8220/21/14/4759. Accessed on: October 3, 2023.

4. Muhammad Sheeraz, Muhammad Arsalan Paracha, Mansoor Ul Haque, Muhammad Hanif Durad, Syed Muhammad Mohsin, Shahab S. Band, Amir Mosavi. "Effective Security Monitoring Using Efficient SIEM Architecture", April 30, 2023. [Online]. Available on: http://hcisj.com/data/file/article/2023040003/13-17.pdf. Accessed on: October 3, 2023.

5. NIST. "Guide for Security-Focused Configuration Management of Information Systems", August, 2011. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-128.pdf. Accessed on: October 5, 2023.

УДК 004.89

О.П. Доренський, О.М. Дрєєв, Р.М. Минайленко
dorensky@ukr.net, drey_sanya@ukr.net, aron70@ukr.net
Центральноукраїнський національний технічний університет,м. Кропивницький

МЕТОД ВИЗНАЧЕННЯ ОЗНАК, ЗА ЯКИМИ НЕЙРОННА МЕРЕЖА ПРИЙМАЄ РІШЕННЯ ПРО КЛАСИФІКАЦІЮ

В системах розмітки та класифікації зображень, нейронні мережі можуть приймати хибні рішення, але при цьому матимуть сильні показники впевненості у власному рішенні [1, 2]. Такі похибки класифікації є небезпечними в різноманітних системах автоматизації, тому для систем керування використовують ряд засобів, які засвідчують нормальний плин процесів у нейронній мережі. Одним із засобів визначення правильної класифікації, є визначення зони підвищеної уваги нейронної мережі для класифікації [3, 4], де визначають приблизну локалізацію ознак, на основі яких виведено результат класифікації. Якщо візуальна оцінка показує, що центри уваги знаходяться на об'єктах класифікації, то приймається рішення про нормальну роботу нейронної мережі.

Пропонується вдосконалити систему визначення центрів уваги нейронної мережі, шляхом виділення компонентів зображення, які саме надали ваги для ознак класифікації, що і є метою роботи. Поставлена задача деградації на вхідному зображенні незначущих деталей, з метою візуального підкреслення елементів, на основі яких здійснено класифікацію. Поставлена задача розв'язана за допомогою оптимізаційного процесу на коефіцієнтах вхідного зображення, коли функція втрат зростає згідно оцінювання різкості вхідного зображення і зростає при відхиленні значень вихідного згорткового шару від еталону, який отримано в результаті первинної класифікації. В процесі оптимізації, коефіцієнти нейронної мережі є константами, змінюється лише вхідне зображення. Логіка описаного процесу показано на рисунку:

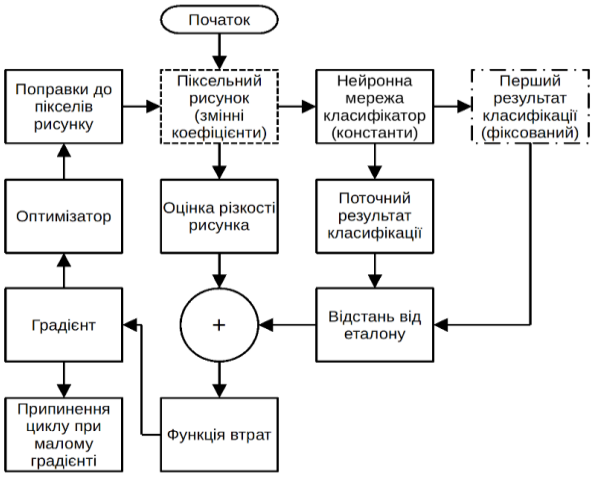


Рис 1. Схема конкуруючих процесів виділення ознак

В результаті роботи алгоритму отримується зображення з видаленими елементами, які не беруть участі в класифікації. Результати можуть бути використані для візуального оцінювання використання на зображенні ключових елементів класифікації, не лише за їх положенням, але й за виглядом.

Список літератури

1. Danilo Vasconcellos Vargas, Jiawei Su "Understanding the One-pixel Attack: Propagation Maps and Locality Analysis", CEUR-WS, Vol-2640, paper 4. URL: https://ceur-ws.org/Vol-2640/paper_4.pdf

2. One Pixel Attack. URL: https://github.com/Hyperparticle/one-pixel-attack-keras

2. R. R. Selvaraju, M. Cogswell, A. Das, R. Vedantam, D. Parikh and D. Batra, "Grad-CAM: Visual Explanations from Deep Networks via Gradient-Based Localization," 2017 IEEE International Conference on Computer Vision (ICCV), Venice, Italy, 2017, pp. 618-626, doi: 10.1109/ICCV.2017.74.

3. Pil Moo Byun, Jeong-Hwan Choi, Joon-Hyuk Chang, "Class Activation Mapping-Driven Data Augmentation: Masking Significant Regions for Enhanced Acoustic Scene Classification", 2023.

УДК 004.89

О.М. Дрєєв, Р.М. Минайленко, Г.М. Дрєєва
drey_sanya@ukr.net, aron70@ukr.net, gannadreeva@gmail.com
Центральноукраїнський національний технічний університет,м. Кропивницький

СИСТЕМА ПОПЕРЕДЖЕННЯ ПРО НЕБЕЗПЕКУ ВИНИКНЕННЯ ТИСНЯВИ В ГРОМАДСЬКИХ МІСЦЯХ

В роботі поставлено за мету створення автоматизованої системи визначення небезпеки утворення тисняви в громадських місцях. Це обумовлено небезпекою отримання травм людьми у тисняві, що вимагає від адміністрації прийняття вчасних профілактичних заходів по перенаправленню потоків людських мас. Для забезпечення досягнення мети, поставлено низку задач:

1) розглянути та обрати методи спостереження за підконтрольною територією з метою забезпечити можливість визначення наявності людських тіл;

2) розробити методи та засоби визначення людських тіл на зображеннях з систем спостереження;

3) розробити методи та алгоритми оцінювання концентрації людських тіл на ділянці території та пріоритетні вектори їх руху;

4) використати математичні моделі, які враховують градієнти переміщення людських мас з оцінюванням темпів змін концентрації людських мас на ділянках території.

На теперішньому етапі колектив є на етапі розв'язання задач 1-2, результати яких можна використати для розв'язання наступних задач.

Визначення розміщення людських тіл є істотним покласти на нейронну мережу, що показано у великій кількості робіт [1, 2]. В результаті аналізу джерел зображень вуличних ділянок доступними засобами відеоспостереження, зроблено висновок, що зображення в IR діапазоні є менш різноманітними – на зображеннях є значно меншим вплив факторів фарбування одягу, колір шкіри та інше. Це значно звузило коло ознак, на які спирається нейронна мережа для пошуку людських тіл в кадрі. В результаті, кількість інформації, яка потрапляє на вхід нейронної мережі втричі менше при використанні кольорового зображення і більш інформативне, ніж зображення у відтінках сірого (де людина в залежності від одягу має можливість виділятися як і білим так і чорним кольором). Тому за основу інформації про положення та переміщення людських тіл було обрано відео з камер спостереження у тепловому діапазоні. Результати роботи такої нейронної мережі показано на рисунку:

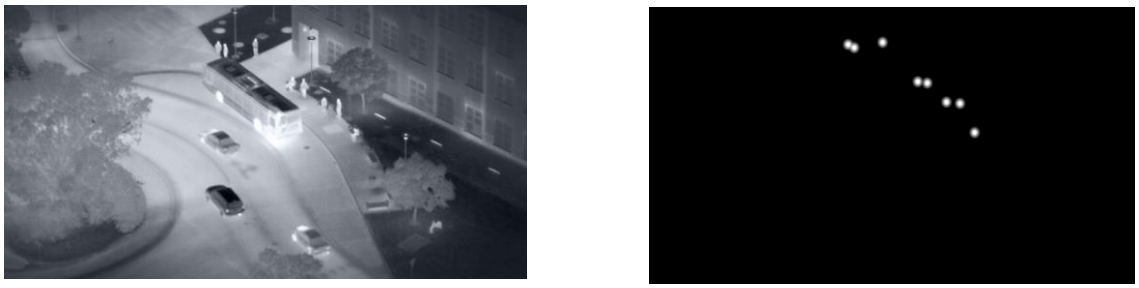


Рис.1. Результат роботи нейронної мережі по розмітці людських тіл

З причини великої кількості пристроїв спостереження, забезпечити мережу для передачі відео до центру обробки є недоцільним, тому кожен пристрій має бортову обчислювальну систему на якій проводиться розмітка людських тіл. Мобільність та автономність обчислювальної системи відеоспостереження вимагає мінімальних обчислювальних витрат від побудованої нейронної мережі. Пошук та оптимізації архітектури нейронної мережі є актуальними задачами в багатьох застосунках. Тому авторами здійснено пошук нейронної мережі за гіперпараметрами глибини та кількості фільтрів на один шар. В результаті отримано мережу, яка містить 21101 коефіцієнт, проти мільйонів в аналогічних рішення.

Список літератури

1. Yang, YueXian Zou, Jian Zhang, Ge Li "Promoting object detection in real world via a cascade structure of Region Proposal Networks" Neurocomputing, Volume 367, 2019, Pages 20-30, ISSN 0925-2312

2. Manssor, S.A.F., Sun, S., Abdalmajed, M. et al. Real-time human detection in thermal infrared imaging at night using enhanced Tiny-yolov3 network. J Real-Time Image Proc 19, 261–274 (2022). https://doi.org/10.1007/s11554-021-01182-z

УДК 004.72

Ю.О. Глущук[1], А.О. Фесенко[1]
Науковий керівник - к.т.н. доцент Фесенко А. О.
yuriihlushchuk@gmail.com, aafesenko88@gmail.com
[1]*Національний авіаційний університет, м. Київ*

РОЛЬ ШТУЧНОГО ІНТЕЛЕКТУ І МАШИННОГО НАВЧАННЯ В ОПТИМІЗАЦІЇ ПРОЦЕСУ АВТОМАТИЗОВАНОГО ТЕСТУВАННЯ ПРОГРАМНИХ ПРОДУКТІВ

Вступ

Індустрія тестування програмного забезпечення (ПЗ) постійно зазнає трансформацій через зміни в методах роботи, потреби у модернізації діючих інструментів, намагання отримати якомога швидше заявлений продукт. Як наслідок, це призвело до зосередження уваги на якісній інженерії та зростанні автоматизації. У той же час, досягнення в галузі штучного інтелекту (Artificial Intelligence), машинного навчання (Machine learning) та нейронних мереж (Neural Networks) формують майбутнє розробки та тестування ПЗ безпрецедентним чином. Щоб бути на крок попереду, все більше компаній розглядають можливість використання штучного інтелекту (ШІ) та машинного навчання (МН) для вдосконалення процедур тестування, застосування інструментів безпеки на основі ШІ та впровадження методів тестування, заснованих на ризиках, які використовують аналітику великих даних [1].

Основна частина

У широкому сенсі, штучний інтелект - це галузь комп'ютерних наук, яка фокусується на створенні систем, що можуть виконувати завдання, які зазвичай вимагають людського інтелекту. Ця область включає в себе розробку алгоритмів, програм та моделей, які надають комп'ютерам здатність розуміти, вивчати, аналізувати, робити висновки, приймати рішення та виконувати завдання. ШІ може використовувати різні методи, такі як машинне навчання, глибинне навчання, нейронні мережі, генетичні алгоритми та інше. Аналіз існуючих методів тестування ПЗ з використанням ШІ показує, що такі методи є дуже ефективними, особливо в умовах швидкого розвитку технологій та збільшення складності програмних систем [2].

Інструменти тестування автоматизації на основі ШІ такі як Applitools, TestRigor, TestSigma, Functionize вже революціонізують спосіб автоматичної перевірки коду, відіграючи значну роль у процесі тестування ПЗ. Використовуючи потужність ШІ, вони здатні запропонувати розширені можливості та покращити ефективність, що забезпечує кращий загальний досвід тестування. Ось кілька способів впливу ШІ на автоматизацію тестування [3].

1. Генерація тестових сценаріїв. ШІ може аналізувати вихідний код та автоматично генерувати тестові випадки з урахуванням змін, які вносяться розробниками, визначати пріоритетність тестових сценаріїв на основі таких факторів, як покриття коду, ризик та ймовірність дефектів або помилок.
2. Виконання тесту. ШІ дозволяє виконувати тести шляхом їх одночасного планування та запуску, тим самим скорочуючи час перевірки. Таким чином відбувається контроль виконання тесту в режимі реального часу, щоб миттєво виявити недоліки та внести необхідні коригування для проходження тесту без зайвої затримки.
3. Оптимізація тесту. ШІ допомагає оптимізувати тестування, аналізуючи тестовану систему (System under test), щоб визначити та видалити зайві або непотрібні етапи перевірки, а також контролювати систему, щоб передбачити ймовірні збої і підготуватися до планового обслуговування.
4. Підтримка неперервної інтеграції (Continuous Integration): ШІ дозволяє автоматизувати процеси тестування в рамках неперервної інтеграції, допомагаючи швидше виявляти і вирішувати проблеми в процесі розробки.
5. Постійне навчання з генерації даних. ШІ і автоматизація тестування працюють разом, щоб спостерігати за тим, як користувач взаємодіє із програмою для визначення його нормальної поведінки. Така інформація суттєво допомагає при створенні тестових сценаріїв на основі фактичних життєвих даних.
6. Тестування з імітацією: ШІ може створювати середовища для тестування, що імітують різні умови роботи програми, такі як навантаження, мережеві проблеми та інші фактори, що можуть вплинути на її працездатність.

Окремою галуззю ШІ є машинне навчання. МН вивчає, як комп'ютерні системи можуть навчатися із обраних даних та робити передбачення чи приймати рішення без явного програмування. У методах ШІ машинне навчання застосовується для розв'язання різноманітних завдань, таких як класифікація, регресія, кластеризація, виявлення аномалій та інше [4]. МН використовує алгоритми та моделі, які

здатні адаптуватися до нових даних та знаходити складні залежності між вхідними та вихідними параметрами. Застосування МН може значно полегшити та прискорити роботу з даними та зробити її більш ефективною і точною. Що саме мається на увазі:

1. Виявлення дефектів. Алгоритми МН здатні сприяти виявленню потенційних дефектів в програмному коді, аналізуючи його структуру і динаміку виконання.
2. Аналіз тестового покриття. Інструменти на основі МН можуть визначити, які частини програмного коду були покриті тестами і де є недоліки в тестовому покритті.
3. Автоматична оцінка результатів тестування. МН може бути використане для автоматичної оцінки результатів тестування, виявлення стабільних і повторюваних дефектів і надання рекомендацій для подальших дій.
4. Підвищення надійності автоматизованих тестів. У міру того, як програмні додатки розвиваються відповідно до мінливих вимог користувачів або оновлень бізнес-процесів, автоматизовані тести можуть стати застарілими і ненадійними, потребуючи технічного обслуговування. Використання МН спрямоване на вирішення цієї проблеми [1].
5. Тестування на основі ризиків. Підхід, який полягає в пріоритетному тестуванні ПЗ на найбільш схильних до помилок ділянках системи. Моделі МН можуть використовувати записи минулих розробок, тестувань і релізів, щоб визначити, де були виявлені дефекти, внесені зміни в код і де виникли проблеми, що полегшує розподіл ресурсів на основі рівнів ризику.
6. Прогнозування дефектів. Алгоритми МН використовуються для вивчення історичних даних про помилки та визначення закономірностей для прогнозування майбутніх дефектів.

Висновок

Поєднання ШІ та МН здатне створити інфраструктуру, де потенційні помилки коду будуть знайдені та виправлені ще до їх появи. Завдяки автоматизації завдань, покращенню точності, пріоритезації тестових випадків, сприянню неперервного тестування та наданню цінних висновків, ШІ може зробити тестування більш ефективним і результативним. Усі ці можливості дозволяють оптимізувати процес автоматизованого тестування, знижуючи час і зусилля, необхідні для перевірки програмного продукту, і, покращуючи при цьому якість кінцевого результату.

Слід пам'ятати, що системи ШІ і МН можуть давати інноваційні результати, зіставляючи відповіді з наборами даних, але ці результати можуть бути невизначеними і неперевіреними. Для осіб, відповідальних за тестування та нагляд за системами ШІ та МН, дуже важливо мати глибоке розуміння їхнього передбачуваного використання в бізнесі та наявності обмежень.

Мета використання ШІ для тестування ПЗ не в тому, щоб усунути людей від завдання. Натомість, технологія доповнює людські навички та інтуїцію і полегшує тестування на етапі життєвого циклу розробки ПЗ. Оскільки технологія ШІ продовжує розвиватися, її роль в автоматизованому тестуванні ймовірно стане ще важливішою, що призведе до подальшого покращення якості ПЗ та ефективності процесу його перевірки.

Список літератури

1. Зліщев С. Як і чому змінюється тестування і що з цим робити? [Електронний ресурс] / Сергій Зліщев // blog.ithillel – 2023. – Режим доступу до ресурсу: https://blog.ithillel.ua/articles/how-and-why-testing-is-changing/.

2. Haenlein, M., Kaplan, A. A Brief History of Artificial Intelligence: On the Past, Present, and Future of Artificial Intelligence. California Management Review. URL: https://www.researchgate.net/publication/334539401_A_Brief_History_of_Artificial_Intelligence_On_the_Past_Present_and_Future_of_A rtificial_Intelligence.

3. Ханна Д. Як ШІ впливає на автоматизацію тестування та які інструменти тестування є успішними? [Електронний ресурс] / Джон Ханна // techlila – 2023.– Режим доступу до ресурсу: https://www.techlila.com/uk/how-does-ai-impact-test-automation/.

4. О. Ф. Лановий, О. В., Золотухін. Застосування нейромережевого підходу для класифікації втручань в роботу комп'ютерних систем // Застосування інформаційних технологій у діяльності НПУ: матеріали наук.-практ. семінару (м. Харків, 21 грудня 2018 р.) / МВС України, Харк. нац. ун-т внутр. справ. Харків. ХНУВС, 2018.– С.78-79.

УДК 004

Я.О. Козлов, Н.Л. Козірова, О.А. Смірнов
kozlov.yan1@gmail.com, natalidonchenko23@gmail.com, dr.SmirnovOA@gmail.com
Центральноукраїнський національний технічний університет, м. Кропивницький

ДОСЛІДЖЕННЯ СТРУКТУРИ ТА ПРИНЦИПУ РОБОТИ SIEM-СИСТЕМИ

За визначенням, SIEM – це додаток який надає можливість отримувати дані безпеки з компонентів інформаційно-комунікаційних систем та представляти їх як корисну інформації в єдиному місці [3]. Фактично, такі системи поєднують у собі два більш давніх рішення: SIM (англ. Security Information Management – керування інформацією безпеки) та SEM (англ. Security Events Management – керування подіями безпеки), що має сенс через схожу природу походження даних [1-3]. SIEM виконує роль моніторингової системи, яка має велике різноманіття надбудов для аналізу переважно безпекових даних, однак, як і будь-яка моніторингова системи, може збирати та візуалізувати метрики та журнали подій, які напряму не пов'язані з безпекою, однак показують загальний стан системи. За допомогою потужних двигунів візуалізації спеціалісти можуть краще аналізувати стан системи, швидше помічати аномальне навантаження та відповідно реагувати на можливі загрози, що можуть бути джерелом такої поведінки.

Як було зазначено раніше, SIEM-системи є потужною зв'язуючою ланкою систем безпеки, однак сама по собі вона жодним чином не покращить так звану «безпекову поставу» організації (від англ. security posture), тобто рівень захисту та готовності до реагування на загрози. Сучасні рішення, як то Splunk Enterprise Security, Elastic Security чи IBM QRadar, мають безліч плагінів для інтеграції з усіма видами систем захисту: журнали аудиту кінцевих точок (персональні комп'ютери, віртуальні машини, контейнери тощо) та окремих веб-сервісів і баз даних, мережеві пристрої, мережеві екрани, сканери вразливостей, системи виявлення та запобігання проникнення, хмарні ресурси, розвідка про кіберзагрози (з англ. threat intelligence) та інше. Стандартні протоколи логування, як то Syslog, що доступні за замовчуванням в більшості систем, мають функцію віддаленого логування – у такому випадку журнали аудиту, незалежно від того, зберігаються вони локально чи ні, переправляються до центрального хабу, який відповідає за обробку та збереження журналів. У той час як елементи інформаційної системи мають змогу використовувати стандартні протоколи логування, для більшості з них розроблені більш спеціалізовані інтеграції у вигляді агентів. Агенти збирають більш збагачені та актуальні дані, враховуючи їхню природу та існуючі вектори загроз, тобто є більш оптимізованими під окремий компонент, але зазвичай додатково мають опцію тонкого налаштування спеціалістом.

Чим більше компонентів системи генерують дані безпеки, тим більш потрібною стає SIEM-система. Окрім моніторингу, важливим завданням будь-якої SIEM-системи є акумулювання та уніфікація журналів аудиту безпеки, або «керування журналами аудиту» (від англ. log management). Зважаючи на це, сучасні системи мають можливість працювати з розподіленими базами даних, реплікувати їх, стежити за терміном зберігання даних (від англ. data retention). Іншим елементом SIEM є модуль збагачення журналів, тобто їхня попередня обробка (аналіз та пошук корисної інформації) для кращого структурування та уніфікації отриманих даних. Спеціаліст, у свою чергу, має потужний апарат для фільтрації логів, створення змістовних послідовностей логів та, відповідно, краще бачення загальної картини. Через збагачені дані пошук закономірностей стає більш інтерактивним і від того простішим. Аналізуючи послідовні логи, які характеризують якусь загрозу, SIEM може автоматично генерувати сповіщення про помічену загрозу та навіть автоматично її зупиняти. Окремою особливістю будь-якої SIEM-системи є наявність інформаційних панелей з візуалізованою інформацією про актуальні характеристики стану системи, починаючи від метрик завантаженості ресурсів закінчуючи кількістю віддалених підключень та списком адрес, з яких надходить найбільше запитів. Таким чином, SIEM стає центром контролю та керування безпекою системи. Загалом, ці властивості роблять такі системи добре пристосованим середовищем роботи спеціалістів для швидкого реагування на загрози та кіберінциденти.

Список літератури

1. Кількість кібератак під час війни зросла втричі. [Електронний ресурс]. Доступно: https://cip.gov.ua/ua/news/kilkist-kiberatak-pid-chas-viini-zrosla-vtrichi. Дата звернення: Вер. 27, 2023.

2. Billy K Leung, "Security Information and Event Management (SIEM) Evaluation Report", May 2021. [Online]. Available: https://scholarworks.calstate.edu/downloads/41687p49q. Accessed on: Sep. 28, 2023.

3. NIST. "Guide for Security-Focused Configuration Management of Information Systems", August, 2011. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-128.pdf. Accessed on: October 5, 2023.

УДК 004.658

Є. І. Горбачов, Л. В. Константинова
zekagor0@gmail.com, liliyashel1976@gmail.com
Центральноукраїнський національний технічний університет, м. Кропивницький

ОГЛЯД SQL SERVER MANAGEMENT STUDIO ДЛЯ РОБОТИ З БД

У світі, насиченому інформацією, обробка та управління даними стають ключовими завданнями. Вдалий вибір засобів для роботи з даними дуже важливий для програмістів. SQL Server Management Studio (SSMS) як інструмент для адміністрування та розробки баз даних Microsoft SQL Server відкриває перед користувачами багато можливостей для роботи з базами даних. Важливо дослідити, як саме цей інструмент спрощує адміністрування та розробку баз даних, а також як він впливає на продуктивність та результативність фахівців у галузі обробки даних.

Досліджуючи можливості SQL Server Management Studio необхідно звернути увагу на основні функції та інструменти, що сприяють оптимізації процесу адміністрування та розробки баз даних. SQL Server Management Studio (SSMS) - це високопродуктивне та потужне інтегроване середовище, розроблене Microsoft для роботи з базами даних, спеціально зорієнтоване на обслуговування Microsoft SQL Server. Це корисний інструмент для адміністраторів баз даних, розробників та аналітиків, які працюють з SQL Server [1].

SSMS є інтегрованим з іншими інструментами та сервісами, що робить його важливим компонентом в роботі з SQL Server. Є можливість легко створювати резервні копії баз даних, відновлювати дані, керувати безпекою та налаштовувати параметри сервера, що спрощує процес адміністрування та розробки баз даних. Різноманітні функції та можливості SSMS дозволяють створювати, модифікувати та оптимізувати структуру бази даних, а також виконувати завдання моніторингу та забезпечення безпеки даних.

На етапі проектування, розгортання та підтримки баз даних у корпоративному середовищі, де важлива властивість живучості системи, використання SSMS дозволяє ефективно вирішувати завдання з оцінки ризиків, моніторингу та оптимізації баз даних. Ця програма має функцію системи захисту інформації у корпоративних мережах зв'язку (КМЗ) часто працюють у розподіленому середовищі та функціонують за умов невизначеності впливу чинників дестабілізації. У цьому контексті, використання теорії нечітких множин стає дорогоцінним інструментом для опису структури системи захисту інформації (СЗІ) та прогнозування її параметрів.

Основні можливості SQL Server Management Studio включають можливість здійснення адміністративних дій над базами даних, виконання SQL-запитів, розробку та налагодження об'єктів баз даних, а також моніторинг і оптимізацію продуктивності SQL Server [2]. Завдяки інтерфейсу та інструментарію SSMS, адміністратори та розробники можуть ефективно працювати з базами даних, забезпечуючи їх надійність і продуктивність.

Відзначаються ключові функції, які включені до функціоналу SQL Server Management Studio, що надають переваги та можливості [1]:

1. Зручний інтерфейс: SSMS надає інтуїтивно зрозумілий інтерфейс, що дозволяє легко навігувати та виконувати завдання для роботи з базами даних. Це дозволяє користувачам працювати ефективно без значних зусиль для вивчення інструменту.

2. Підтримка версій SQL Server: SSMS підтримує різні версії SQL Server, що робить його універсальним інструментом для роботи з різними версіями цієї СКБД. Є можливість легко підключатися до будь-якого SQL Server, від SQL Server 2008 до найновіших версій. Це особливо важливо для організацій, які використовують різні версії SQL Server у своєму інфраструктурному середовищі.

3. Скриптова робота: SSMS дозволяє розробникам створювати, редагувати та виконувати SQL-скрипти. Це особливо корисно при розробці складних операцій з базами даних та автоматизації завдань. Є можливість легко створювати SQL-скрипти для створення об'єктів бази даних, працювати з збереженими процедурами та функціями.

4. Моніторинг та оптимізація: Інструменти моніторингу в SSMS допомагають відслідковувати продуктивність сервера бази даних. Ви можете перевіряти завантаженість сервера, виявляти та вирішувати проблеми з продуктивністю. Це дозволяє забезпечити стабільну та швидку роботу бази даних для користувачів.

5. Розширені можливості безпеки: SSMS дозволяє налаштовувати рівні безпеки для об'єктів бази даних, керувати доступом до даних та забезпечувати їх конфіденційність. Є можливість налаштування прав доступу для користувачів та ролей, а також використовувати інші механізми захисту даних.

6. Спрощення адміністрування: SQL Server Management Studio надає інструменти для зручного управління базами даних, включаючи створення резервних копій, відновлення даних та налаштування

параметрів сервера. Це спрощує рутинні завдання адміністраторів і дозволяє їм швидко реагувати на проблеми, такі як відновлення даних після аварії.

7. Розробка та налагодження: SQL Server Management Studio стає невід'ємною частиною процесу розробки та налагодження баз даних. Розробники використовують його для створення нових об'єктів баз даних, написання та відлагодження SQL-запитів, а також для взаємодії з системою керування версіями. Інтегрованість засобів розробки сприяє рівномірному та продуктивному процесу створення програмних продуктів, які використовують дані з баз даних Microsoft SQL Server.

8. Інтеграція з іншими інструментами: SQL Server Management Studio може легко інтегруватися з іншими інструментами і службами, такими як Azure Data Studio та Azure SQL Database, забезпечуючи розширені можливості розробки та адміністрування баз даних в хмарних середовищах. Ця інтеграція дозволяє спростити роботу з різними ресурсами та забезпечити більшу ефективність керування базами даних.

9. Підтримка розширень та плагінів: SQL Server Management Studio дозволяє встановлювати різноманітні розширення та плагіни, що розширюють його можливості та дозволяють користувачам адаптувати інструмент до конкретних потреб. Це відкриває безмежні можливості для налаштування інтерфейсу та функціоналу відповідно до власних вимог і завдань.

10. Підтримка різних мов програмування: SSMS підтримує різні мови програмування, наприклад, T-SQL, Python та R. Це дозволяє розробникам створювати складні запити та аналізувати дані відповідно до своїх потреб та впроваджувати різноманітні розв'язки у мовах, з якими вони знайомі.

SSMS – це фактично стандартний інструмент розробки та керування базами даних SQL Server. Він надає багатий графічний інтерфейс і спрощує налаштування, адміністрування та завдання розробки, пов'язані з керуванням середовищами SQL Server і бази даних SQL Azure. SSMS також містить надійний редактор сценаріїв T-SQL і поставляється з багатьма шаблонами, зразками та функціями створення сценаріїв. SSMS – це програма лише для Windows. Він не працює в середовищах Linux або macOS. Потужність SSMS полягає в багатьох способах, якими можливо використовувати його для взаємодії з одним або кількома екземплярами SQL Server [3].

Наприклад, функція реєстрації сервера в SSMS може як заощадити час, так і полегшити керування складним середовищем, зберігаючи список екземплярів, до яких часто звертаються. Попередня реєстрація підключень для повторного використання в майбутньому забезпечує такі переваги: збереження інформації про підключення; створення груп серверів псевдоніми серверів з більш значущими іменами; можливість додавати детальні описи як до серверів, так і до груп серверів; імпорт і експорт зареєстрованих груп серверів для спільного використання між машинами або членами команди.

Є можливість використовувати SSMS для реєстрації чотирьох різних типів серверів і служб та керування ними: механізм баз даних; послуги аналізу; служби звітності; служби інтеграції [3].

Ці та інші функції роблять SQL Server Management Studio потужним інструментом для адміністрування та розробки баз даних Microsoft SQL Server та сприяють підвищенню продуктивності розробників і адміністраторів баз даних. SSMS спрощує процес розробки, дозволяючи програмістам та адміністраторам легко взаємодіяти зі схемами, таблицями, збереженими процедурами та іншими об'єктами бази даних [3].

Отже, розглядаючи питання розробки баз даних, SQL Server Management Studio відіграє значущу роль у спрощенні рутинних завдань, що дозволяє фахівцям з баз даних зосередитися на творчому процесі розробки та вдосконаленні структури та функціональності бази даних.

Висновки. SQL Server Management Studio є ключовим інструментом для адміністрування та розробки баз даних Microsoft SQL Server. Не зважаючи на деякі недоліки, його багатофункціональність та інтуїтивний інтерфейс допомагають забезпечити високий рівень надійності та продуктивності баз даних у корпоративних середовищах. Використання SSMS спрощує роботу адміністраторів та розробників, забезпечуючи ефективну роботу з даними, що є надзвичайно важливим у сучасному інформаційному світі.

Список літератури

1. What is SQL Server Management Studio (SSMS)? // Microsoft Ignite, 31.03.2023р. [Електронний ресурс] – Режим доступу: https://docs.microsoft.com/en-us/sql/ssms/sql-server-management-studio-ssms (дата звернення: 16.10.2023).

2. SQL Server Central [Електронний ресурс] – Режим доступу: https://www.sqlservercentral.com/ (дата звернення: 14.10.2023).

3. Randolph West, Melody Zacharias, William Assaf, Deepthi Goguri, Elizabeth Noble, Meagan Longoria, Joseph D'Antoni, Louis Davidson. SQL Server 2022 Administration Inside Out. Microsoft Press, May 2023, 992p. ISBN: 9780137899845.

УДК 621.397

О.В. Марушин, К.О. Бобровський, С.О. Комаров
marushin.o@ukr.net, Kostua1632@gmail.com, 7281092@gmail.com
Державний університет інтелектуальних технологій та зв'язку, м. Одеса

АЛГОРИТМ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ФРАКТАЛЬНОГО СТИСНЕННЯ

Нові алгоритми підвищення ефективності фрактального стиснення, можно описати трьома напрямками. Перший напрям це основа алгоритму квадродерева, де розробляється нова мозаїчна схема розбиття зображення з перекриванням ранговими блоками. Нова схема дозволяє скоротити кількість рангових блоків, завдяки чому зменшується кількість порівнянь ранг-домен, а також збільшується коефіцієнт стиснення.Другий напрям розроблений для прискорення порівняння рангу і домена вводиться новий критерій оптимальності - коефіцієнт кореляції, що тягне за собою і зміну самого алгоритму порівняння. Коефіцієнт кореляції дозволяє відразу, без додаткових обчислень, оцінити схожість між рангом і доменом. І останнім третім відноситься до класифікація доменного пулу по полярному куту центрів мас блоків. Цей критерій класифікації дозволяє об'єднати блоки з високою взаємною кореляцією. Завдяки цьому домени, погано корельовані з даними рангом, з пошуку виключаються, що дозволяє значно скоротити час стиснення.

Другий напрям розроблений для прискорення порівняння рангу і домена вводиться новий критерій оптимальності - коефіцієнт кореляції, що тягне за собою і зміну самого алгоритму порівняння. Коефіцієнт кореляції дозволяє відразу, без додаткових обчислень, оцінити схожість між рангом і доменом.

Пропоновані удосконалення можуть використовуватися як в комплексі, так і окремо, для модифікації способів фрактального стиснення зображень, розроблених іншими авторами. Розглянемо їх більш детальніше

В алгоритмі квадродерева, запропонованому Фішером, як критерій, що визначає перехід на інший рівень розбиття, використовується середньоквадратична помилка, рівна r , де r – величина, що обчислюється за формулою (1). Для середньоквадратичні помилки встановлюється граничне значення. Якщо після порівняння рангу з усіма доменами поточного рівня розбиття не вдалося підібрати доменну область, що забезпечує покриття рангу з помилкою, менше порогової, то ранг розбивається на 4 субблока. Очевидно, що для формування мозаїчної схеми розбиття такий підхід використовувати не вдасться.

$$z = \frac{1}{M}\sum_{i=1}^{N}\sum_{j=1}^{N}\sum_{k=1}^{N} k \cdot B_{i,j,k} - \frac{N+1}{2} \qquad (1)$$

де $B_{i,j,k}$ - значення вагової функції з координатами, при $M = \sum_{i=1}^{N}\sum_{j=1}^{N}\sum_{k=1}^{N} B_{i,j,k}$

де D і R – матриці, що представляють собою відповідно домен, зменшена до розміру рангу, і ранг, N – розмір сторони рангового блоку.

$$x = \frac{1}{M}\sum_{i=1}^{N}\sum_{j=1}^{N}\sum_{k=1}^{N} i \cdot B_{i,j,k} - \frac{N+1}{2} \qquad (2)$$

У формулі (2) в чисельнику фактично записана коваріація рангу і домену, а в знаменнику - дисперсія домену. Якщо чисельник і знаменник помножити на середньоквадратичне відхилення (СКВ) рангу, то коефіцієнт перетворення контрасту можна виразити через коефіцієнт кореляції рангу і домена. Якщо домен з точністю до пікселя перетвориться в поточний ранг за допомогою коефіцієнтів s і o, то тоді коефіцієнт кореляції ρ (R , D) = 1 и r = 0 .

Якщо ж домен абсолютно корельовані з рангом, то тоді ρ (R , D) = 0 і значення r досягає свого максимуму для даного рангу і стає рівним його дисперсії $r = \sigma^2 R$. На практиці часто замість дисперсії зручніше використовувати СКВ $\sigma R = \sigma^2 R$ [1]. Таким чином, СКВ рангу є обмеженням зверху середньоквадратичної помилки при порівнянні даного рангу з будь-якими доменами, і, отже, його можна використовувати в якості критерію для зменшення розмірів рангів при адаптивному розбитті зображення. За допомогою СКО рангів можна безпосередньо сформувати адаптивну схему розбиття, що добре підходить для мозаїки. Для збільшення ступеня стиснення при розробці мозаїчної схеми було вирішено використовувати перекриваються рангові блоки.

Другий напрямок досліджень пов'язаний зі зміною критерію оптимальності, що використовується при порівнянні рангів і доменів. Як уже зазначалося, кожен ранг порівнюється з безліччю доменів. Спростивши процедуру цього порівняння, можна отримати значний виграш в швидкості стиснення. Для

прискорення процесу автором було запропоновано в якості критерію оптимальності замість (1) використовувати коефіцієнт кореляції.

Формулу (2) для коефіцієнта перетворення контрасту так само можна переписати через коефіцієнт кореляції. СКО яскравостей пікселів рангів і доменів можна підрахувати заздалегідь, а не обчислювати при кожному порівнянні, що дозволить збільшити швидкість обробки на комп'ютері. Для коефіцієнта перетворення контрасту має виконується умова $s < 1$. Коефіцієнт кореляції, який є першим співмножником, не може бути більшим за одиницю за абсолютним значенням. Зміна критерію оптимальності, що використовується при порівнянні рангів і доменів з традиційною середньоквадратичної помилки на коефіцієнт кореляції, спричинило за собою модифікацію самого алгоритму порівняння. Це дозволило не тільки прискорити процес стиснення більш ніж в 9 разів, але і краще зрозуміти сам механізм фрактального стиснення[2].

Третій напрям досліджень пов'язаний з класифікацією блоків. В інтересах прискорення фрактального стиснення число доменів, які використовуються для порівняння з даними рангом, бажано скоротити. У великій кількості робіт для скорочення доменного пулу пропонується використовувати різні способи класифікації блоків. Класифікаційні методи використовують ті числові характеристики рангів і доменів, які можна вважати приблизно інваріантними щодо перетворень, що застосовуються до доменів. Домени і ранги підрозділяються на певну кількість класів у відповідності зі своїми характеристиками, і пошук кандидата ведеться в тому ж класі, до якого відноситься ранг, або обмежується декількома класами, характеристики яких близькі до характеристик рангу.

При використанні генетичного алгоритму для пошуку оптимальних рішень кожен елемент $x \in X$ простору оптимізації повинен бути представлений як вектор $b \in B$ з N символів двійкового алфавіту $A = \{0,1\}$, де $B = A^N$. Необхідно також, щоб простір оптимізації X складався з кінцевим числом елементів[3].

Популяцією $П = (\chi^1, \chi^2, \ldots, \chi M)$ чисельності M вважається вектор простору B^M, координати якого називаються генотипами особин даної популяції.

Кроком генетичного алгоритму є перехід від поточного покоління до наступного, тобто отримання нової популяції Π_{t+1} з Π_t. У побудові черговий особини нової популяції беруть участь оператори кросинговеру, мутації і випадковий оператор відбору $B^M \to \{1,\ldots,M\}$ дія якого полягає у виборі номера особини батька при породженні чергового нащадка.

Для визначення необхідно задати оператор кросинговеру (схрещування) $B \times B \to B \times B$ і оператор мутації Mut: $B \to B$. Дія кросинговеру $(\chi', \tau') = Cross(\chi, \tau)$ полягає у виборі випадковим чином деякої позиції j, рівномірно розподілені від 1 до $N-1$, після чого результат формується у вигляді $\chi' = (\chi_1, \chi_2, \ldots, \chi_j, \tau_{j+1}, \ldots, \tau_N)$, $\tau' = (\tau_1, \tau_2, \ldots, \tau_j, \chi_{j+1}, \ldots, \chi_N)$.

Вплив кросинговеру регулюють за допомогою ймовірності P_{Cross} спрацьовування цього оператора (в іншому випадку все залишається без змін). Оператор мутації в кожній позиції аргументу із заданою вірогідністю P_{mut} замінює її вміст на випадковий елемент двійкового алфавіту A, обраний у відповідності з рівномірним розподілом (в іншому випадку все залишається без змін).

Цільова функція вихідної задачі, замінюється в генетичному алгоритмі на не негативну функцію придатності генотипу $\Phi(\chi)$, де $\chi \in B$. Процес роботи алгоритму являє собою послідовну зміну поколінь, на кожному кроці якої популяція Π_{t+1} наповнюється парами нащадків від особин популяції Π_t за формулою

$$(\chi_k^{t+1}, \chi_{k+1}^{t+1}) = Mut(Cross(\chi_{Select(\Pi_t)}^t, \chi_{Select(\Pi_t)}^t)) \qquad (3)$$

де $(\chi_k^{t+1}, \chi_{k+1}^{t+1})$ - особини з найменшою придатністю популяції Π_t. Тобто індивіди витягуються попарно з Π_t і після кросинговеру і мутації поміщаються в Π_{t+1}. Зміна ймовірностей мутації кросинговері дозволяє регулювати роботу генетичного алгоритму і налаштовувати його на конкретні завдання[4].

Список літератури

1. Arya S., Mount D.M., Netanyahu N. S., Silvernam R., Wu A., An optimal algorithm for approximate nearest neighbour searching, Proc. 5th Annual ACM-SIAM Symposium on Discrete Algorithms (1994) 573-582.
2. Уэлстид С. Фракталы и вейвлеты для сжатия изображений в действии. Учебное пособ.- М.: Изд. Триумф, 2003 320 с. Эфрос82] Эфрос А.JT. Физика и геометрия беспорядка. - М.: Наука, 1982.
3. Bani-Eqbal B., Speeding up fractal image compression, in: Proceedings from IS&T/SPIE 1995 Symposium on Electronic Imaging: Science & Technology, Vol. 2418: Still-Image Compression 1995.
4. Barnsley M. F., Fractals Everywhere, New York: Academic, 1988.

УДК 004.6

Л.В. Константинова
liliyashel1976@gmail.com
Центральноукраїнський національний технічний університет, м. Кропивницький

ОГЛЯД ІНСТУМЕНТІВ ДЛЯ ПІДТРИМКИ ОПЕРАЦІЙ З BIG DATA

Для оптимізації різних сфер життя: від ведення бізнес-процесів, телекомунікацій, виробництв до державного управління застосовуються Big Data. До складу поняття «великі дані» входить значна кількість технологій. Для вирішення проблеми вибору відповідного поцінного інструменту для підтримки операцій з Big Data необхідно зробити огляд існуючих засобів.

Визначальними характеристиками для великих даних є, окрім їх фізичного об'єму, й інші, які підкреслюють складність задачі обробки і аналізу цих даних.

Простіше кажучи, великі дані - це сукупність неструктурованих, структурованих і напівструктурованих даних, які компанії збирають для отримання інформації. Структуровані дані надходять у фіксованому форматі. Напівструктуровані дані схожі на структуровані дані, але не відповідають моделям даних баз даних. Понад 80% даних, накопичених сьогодні підприємствами, є неструктурованими або напівструктурованими [1].

Технології Big Data – це програмні засоби, розроблені для оцінки, обробки та вилучення інформації зі складних даних. Зазвичай ці дані надходять у величезних обсягах, що не дає можливості традиційному програмному забезпеченню впоратися з ними.

Технології великих даних можна розділити на чотири основні типи: зберігання даних, інтелектуальний аналіз даних, аналітика даних і візуалізація даних [2]. Кожен із них пов'язаний із певними інструментами.

1. Зберігання даних. Технологія великих даних, яка стосується зберігання даних, має можливість отримувати, зберігати та керувати великими даними. Він складається з інфраструктури, яка дозволяє користувачам зберігати дані так, щоб до них було зручно отримати доступ. Більшість платформ зберігання даних сумісні з іншими програмами. Серед популярних інструментів виділяють два: Apache Hadoop і MongoDB.

Apache Hadoop - є найпоширенішим інструментом великих даних. Це програмна платформа з відкритим вихідним кодом, яка зберігає та обробляє великі дані в розподіленому обчислювальному середовищі між апаратними кластерами. Цей розподіл дозволяє швидше обробляти дані. Фреймворк розроблено для зменшення кількості помилок і збоїв, масштабованості та обробки всіх форматів даних.

MongoDB - це база даних NoSQL, яку можна використовувати для зберігання великих обсягів даних. Використовуючи пари ключ-значення (базова одиниця даних), MongoDB класифікує документи в колекції. Вона написана мовами C, C++ і JavaScript і є однією з найпопулярніших баз даних великих даних, оскільки в ній можна легко керувати та зберігати неструктуровані дані.

2. Інтелектуальний аналіз даних. Інтелектуальний аналіз даних витягує корисні закономірності та тенденції з необроблених даних. Технології великих даних, такі як Rapidminer і Presto, можуть перетворювати неструктуровані та структуровані дані на корисну інформацію.

Rapidminer - це інструмент аналізу даних, який можна використовувати для створення прогнозних моделей. Він використовує ці дві ролі як сильні сторони, обробку та підготовку даних, а також створення машин і моделей глибокого навчання. Наскрізна модель дозволяє обидві функції впливати на всю організацію [3].

Presto - це механізм запитів із відкритим вихідним кодом, спочатку розроблений Facebook для виконання аналітичних запитів щодо великих наборів даних. Тепер цей засіб широко доступний. Один запит у Presto може об'єднати дані з кількох джерел в організації та виконати їх аналітику за лічені хвилини.

3. Аналітика даних В аналітиці великих даних технології використовуються для очищення та перетворення даних в інформацію, яку можна використовувати для прийняття бізнес-рішень. На наступному етапі (після аналізу даних) користувачі виконують алгоритми, моделі тощо за допомогою таких інструментів, як Apache Spark і Splunk.

Apache Spark є популярним інструментом для аналізу великих даних, оскільки він швидко та ефективно запускає програми. Він швидший за Hadoop, оскільки використовує оперативну пам'ять (RAM) замість того, щоб зберігати та обробляти пакетами за допомогою MapReduce [4]. Spark підтримує широкий спектр завдань і запитів аналітики даних.

Splunk – є інструментом аналітики Big Data для отримання інформації з великих наборів даних. Його популярність ґрунтується на можливостях генерувати графіки, діаграми, звіти та інформаційні панелі. Splunk також дозволяє користувачам включати штучний інтелект (AI) в результати даних.

4. Візуалізація даних

Технології великих даних можна використовувати для створення ефектних візуалізацій із даних. У ролях, орієнтованих на дані, візуалізація даних - це навичка, яка є корисною для представлення рекомендацій зацікавленим сторонам.

Tableau є дуже популярним інструментом у візуалізації даних, оскільки його інтерфейс перетягування дозволяє легко створювати секторні діаграми, стовпчасті діаграми, прямокутні діаграми, діаграми Ганта тощо. Це безпечна платформа, яка дозволяє користувачам обмінюватися візуалізаціями та інформаційними панелями в режимі реального часу.

Looker - це інструмент бізнес-аналітики (BI), який використовується для аналізу великих даних, а потім для обміну цією інформацією з іншими командами. Діаграми, графіки та інформаційні панелі можна налаштувати за допомогою запиту, наприклад, щотижневого моніторингу взаємодії з брендом за допомогою аналітики соціальних мереж.

Також технології, що застосовують для обробки великих даних розділяють на 3 групи:

– програмне забезпечення;

– обладнання;

– сервісні послуги.

Серед розповсюджених підходів також виділяють:

- MapReduce - модель розподілу обчислень. Використовується для паралельних обчислень над великими наборами даних. У програмному інтерфейсі дані передаються на обробку програмі, а програма - даним. Таким чином запит є окремою програмою. Принцип роботи полягає у послідовній обробці даних двома методами Map та Reduce. Map вибирає попередні дані, Reduce агрегує їх.

- SQL - мова структурованих запитів, що дозволяє працювати з базами даних. За допомогою SQL можна створювати та модифікувати дані, а керуванням масивом даних займається відповідна система керування базами даних та ін.

Окрім того існують корисні онлайн-ресурси та інструменти для роботи з Big Data**,** оформлення матеріалів, аналізу та пошуку даних в інтернеті.

Google Refine - інструмент для модерації даних, переведення з одного формату в інший, прив'язки до веб-сервісів та баз даних.

Mr. Data Converter: переводить дані у різні формати – HTML, JSON, PHP, XML тощо.

Storage Features - єдиний хмарний сервіс для збереження даних з Google Drive, Gmail, Google Photos.

На сьогоднішній день на ринку доступно безліч інструментів для підтримки операцій з великими даними. Деякі з них інструменти з відкритим кодом, а інші - платні.

Нижче наведено список з дев'яти найкращих технологій великих даних на 2023 рік [1]. Це такі продукти: Apache Hadoop, NoSQL , Apache Spark, Apache Kafka, Apache Hive, Apache Cassandra, Apache Pig, Tableau, Sqoop.

Доцільно перш ніж робити будь-який вибір треба проаналізувати засоби, зрозуміти їх особливості, переваги та недоліки.

Поряд із безліччю можливостей та більш ефективної роботи щодо традиційних баз даних, технології Big Data мають низку проблем при впровадженні їх в організацію. Але прогнозується, що до 2024 року обсяг даних, які генеруються, копіюються, споживаються та збираються, досягне 149 зетабайт [1]. Щоб підприємства могли зберігати, обробляти й аналізувати ці дані, потрібно вдосконалювати технології великих даних. Також потрібно розумно вибирати правильний інструмент великих даних відповідно до потреб та цінової політики проекту. За прогнозами інновації у сфері великих даних продовжуватимуть розвиватись.

Список літератури

1. Top Big Data Technologies in 2023: How They Can Benefit Your Business// DOIT Software, 18.08.2023 [Електронний ресурс] – Режим доступу: https://doit.software/blog/big-data-technologies# (дата звернення: 15.10.2023)

2. 4 Types of Big Data Technologies (+ Management Tools)// Coursera, 16.06.2023 [Електронний ресурс] – Режим доступу: https://www.coursera.org/articles/big-data-technologies (дата звернення: 16.10.2023)

3. Data Mining Tools// RapidMiner [Електронний ресурс] – Режим доступу: https://rapidminer.com/glossary/data-mining-tools/. (дата звернення: 17.10.2023)

4. [Електронний ресурс] – Режим доступу: https://www.ibm.com/blog/hadoop-vs-spark/ (дата звернення: 17.10.2023)

УДК 621.39 (043.2)

А.Д. Пінчук[1], Р.С. Одарченко[1]
pinchuk.ad87@gmail.com, odarchenko.r.s@ukr.net
[1]*Національний авіаційний університет, м. Київ*

РЕЗУЛЬТАТИ РОЗГОРТАННЯ ТА ТЕСТУВАННЯ МЕРЕЖІ LTE НА ОСНОВІ ВІДКРИТИХ РІШЕНЬ

На сьогоднішній день велика кількість проєктів реалізовується на основі open-source рішень (проєктів з відкритим вихідним кодом). Зокрема, завдяки таким таким рішенням є можливим розгортання тестових стендів стільникових мереж зв'язку різних поколінь. При цьому, найбільш розповсюдженими тут є четверте та п'яте покоління. Тому таким інженерним задачам присвячена низка наукових праць. Зокрема, в [1] показано, як налаштувати стільникову мережу LTE для експериментальних досліджень та вимірювань, використовуючи стандартне обладнання та програмне забезпечення з відкритим кодом. У [2] описано, як побудувати приватну мережу LTE/5G корпоративного рівня, наведено рекомендації щодо використання певного програмного та апаратного забезпечення, а також базову схему розгортання.

Для розгортання мережі LTE на основі відритих рішень було обрано наступні програмні та апаратні рішення (всі знаходяться в одній підмережі та підключені до одного віртуального комутатора) (табл.1). Схема розгорнутої мережі показана на рис.1. Вона включає зв'язок між усіма розгорнутими компонентами мережі, IP-адресами, програмним та апаратним забезпеченням. Додатково були розгорнуті системи моніторингу Grafana (Monitoring-4G, RAN Logging and Monitoring).

Таблиця 1
Використані програмні та апаратні рішення

№ п/п	Компонент	Рішення програмне/апаратне
1.	Network Core	SD-CORE/віртуальна машина на сервері
2.	RAN (Radio Access Network)	srsENB/Raspberry PI, LimeSDR
3.	RIC (RAN Intelligent Controller)	SD-RAN/віртуальна машина на сервері
4.	SMO (Service Management Orchestration)	Aether ROC/віртуальна машина на сервері
5.	UE (User Equipment)	GRSIMWrite4.2.10/смартфон з підтримкою стандарту LTE, blank SIM-card

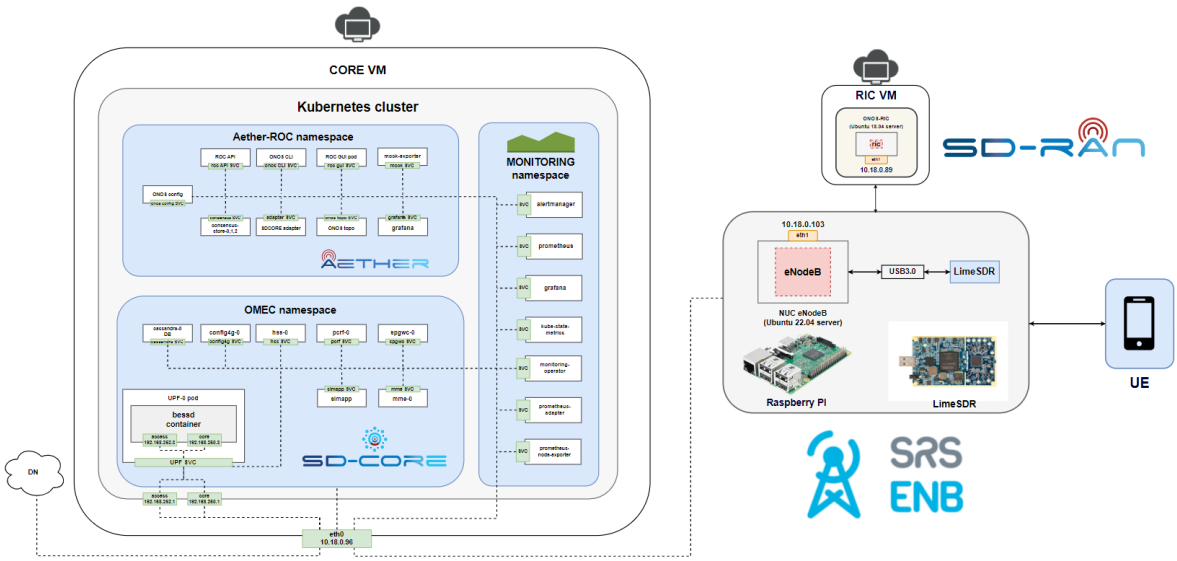


Рис.1. Схема розгортання мережі LTE

Тестування мережі. У результаті даного варіанту розгортання мережі LTE на основі відкритих рішень було успішно зареєстровано користувача у цій мережі, що можна бачити на моніторингу (рис.2).

Доступна наступна інформація: статус базової станції (eNodeB Status), кількість та інформація (IMSI) про активних користувачів (Active subscribers та Subscriber info відповідно), графічно відображено активний час користувача в мережі та пропускна здатність по двом каналам Tx Bitrate (Transmitter), Rx Bitrate (Receiver) (поточна та за весь час перебування користувача в мережі).

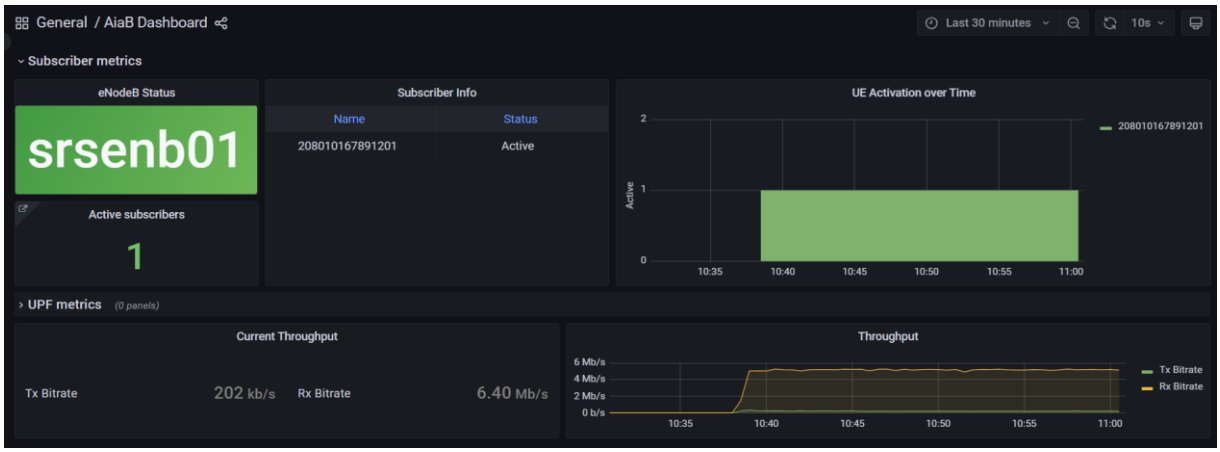


Рис.2. Система моніторингу LTE

Мережа була протестована декількома варіантами використання: звичайне користування веб-додатками, відеодзвінок з використанням Google Meet, завантаження UL (Uplink) та DL (Downlink). Всі тести були успішними. Тому дане рішення можна вважати PoC (Proof of Concept), що розгорнути дієздатну приватну мережу 4G можливо.

Подальший розвиток. Наразі проводяться роботи щодо вдосконалення мережі четвертого покоління, шляхом розгортання near-RT RIC (near Real Time) та xApps (додатки на основі мікросервісів для постійного підвищення ефективності використання радіочастотного спектру RAN), що у цілому дозволить контролювати та оптимізувати функції та ресурси RAN.

Паралельно цьому відбувається розгортання мережі стільникового зв'язку п'ятого покоління також на основі open-source рішень. Оскільки проєктів для розгортання мереж 5G досить велика кількість, було проведено порівняльний аналіз найбільш використовуваних світовою спільнотою та обрано робочу опцію розгортання [3]. Було успішно розгорнуто ядро мережі та протестовано за допомогою симулятору базової станції та користувача (gNBSim). Проте, повноцінний запуск цієї мережі наразі унеможливлює відсутність більш потужного SDR (Software Defined Radio) – Ettus USRP B210.

Висновки. Нинішня екосистема open-source зробила як 4G, так і 5G відкритими для всіх, хто хоче заглибитися, дослідити і вивчити роботу цих мереж. Результати розгортання та тестування мережі LTE на основі відкритих рішень підтверджують їхню ефективність та можливість створення сучасних мереж без наявності комерційних рішень. Це сприяє зниженню витрат, збільшенню гнучкості та стимулює інновації у сфері зв'язку. Реалізація таких тестових стендів стільникових мереж зв'язку дозволить проводити велику кількість різноманітних досліджень, експериментів та окремих наукових проєктів, зокрема у напрямку вдосконалення самих мереж, тестування різного обладнання тощо. Також це створює всі необхідні умови для навчання студентів і їх розвитку як спеціалістів у галузі телекомунікацій та радіотехніки.

Список літератури

1. Y. Boussad, A. Legout, W. Dabbous, L. Lizzi, F. Ferrero and M. N. Mahfoudi, "Open-Source 4G Experimental Setup", 2020 IEEE International Symposium on Antennas and Propagation and North American Radio Science Meeting, Montreal, QC, Canada, 2020, pp. 1399-1400, doi: 10.1109/IEEECONF35879.2020.9330245.

2. Mazur M. Introduction to open source private LTE and 5G networks | Ubuntu [Електронний ресурс] / Maciej Mazur // Ubuntu. URL: https://ubuntu.com/blog/introduction-to-open-source-private-lte-and-5g-networks (accessed on May 19, 2023)

3. Пінчук А. Д., Одарченко Р. С. Аналіз open-source проєктів для розгортання та тестування стільникових мереж зв'язку 5G. International scientific conference Sustainable Development of the Global Communication, Navigation, Surveillance and Air Traffic Management Systems CNS/ATM: матеріали Міжн. наук. конф., Національний авіаційний університет, м. Київ. 2023. С. 101–104.

УДК 389:681.2

Н.О.Пунченко[1]
iioonn24.01@gmail.com
[1]*Одеський Державний аграрний університет, м Одеса*

МЕГАНАУКА МЕТРОЛОГІЯ ПЛАТФОРМА НЕЙРОМЕРЕЖЕВИМ АЛГОРИТМАМ ДЛЯ НАВІГАЦІЙНИХ СИСТЕМ

Штучні нейронні мережі є потужними інструментами в галузі інтегрованих навігаційних систем судноводіння. Вони можуть бути використані для вирішення різних завдань у цій галузі. Розвиток інформаційних технологій та застосування нейронних мереж в сфері навігації та орієнтації рухомих об'єктів є важливим кроком у покращенні точності та надійності навігаційних систем. Використання інерційних та супутникових систем навігації разом з нейромережами може покращити якість визначення координат та орієнтації об'єктів, особливо в умовах обмеженого доступу до супутникового сигналу.

Штучні нейронні мережі по своїй організації мають важливі якості: структурну однорідність і, біологічні прототипи, надмірність, які використовують для підвищення надійності їх функціонування. Пояснення дозволить краще зрозуміти ці концепції. Структурна однорідність означає, що у складі нейронної мережі можуть бути кілька однотипних нейронів чи шарів. Ці нейрони чи шари мають схожу структуру та функцію. Що дозволяє спростити архітектуру мережі, оскільки однотипні елементи можуть виконувати схожі обчислення. Однак, різні елементи можуть адаптуватися до різних типів завдань. Надмірність у штучна нейронна мережа може бути використана для підвищення надійності та стійкості мережі.. Створені Владиславом Кондратовим (інститут кібернетики ім. В.М.Глушкова НАН України) фундаментальна фізична теорія та методи надлишкових та надмірних вимірів величин різної фізичної природи та інші науково-технічні завдання відкрили нову еру розвитку у XXI столітті фундаментальної метрології не лише в Україні і у всьому світі. Теорія надлишкових і надмірних вимірів, наприклад, спирається на загальнонаукову методологію системного підходу та інформативної надмірності та, на відміну від існуючої методології системного аналізу. Створення теорії та методів надмірних вимірів дозволили сформувати новий погляд на цю проблему. Методи надлишкових вимірів є багатоцільовими. Вони забезпечують визначення як значень фізичної величини невідомого розміру, а й значень параметрів функції перетворення вимірювального каналу та його відхилень від номінальних значень згодом. Останнє необхідне визначення параметрів метрологічної надійності засобу вимірів. Методи надлишкових вимірів припускають вимірювальні перетворень не однієї, а кількох рядів фізичних величин, розміри яких пов'язані між собою певним чином. Дані методи забезпечують автоматичне виключення систематичних похибок природним чином, - за рахунок обробки результатів проміжних вимірювань по апріорі виведеного рівняння надлишкових вимірювань або рівняння числових значень[1].

Дані методи забезпечують автоматичне виключення систематичних похибок природним чином, - за рахунок обробки результатів проміжних вимірювань по апріорі виведеного рівняння надлишкових вимірювань або рівняння числових значень. Дослідження сутності та методології надлишкових вимірювань показало, що іншим ефективним способом зменшення випадкової складової похибки є обробка поодиноких результатів надлишкових вимірювань, визначених не по одному, а за рівняннями n рівняннями надлишкових вимірювань з подальшою статистичною обробкою отриманих даних. Висновок n рівнянь надлишкових вимірів обумовлений введенням та вимірювальним перетворенням нових додаткових рядів фізичних величин та виведенням необхідного та достатнього числа нових рівнянь надлишкових вимірів з нової системи рівнянь величин, що характеризує процес надмірних вимірювань[1]. Від рівня розвитку фундаментальної метрології залежить науково-технічний прогрес будь-якої країни. При цьому засоби вимірювань повинні мати високу метрологічну надійність. Виходячи з цього висловлювання, використання структурної однорідності та надмірності в штучних нейронних мережах дозволяє створювати більш надійні та гнучкі моделі, здатні адаптуватися до різноманітних умов та завдань. Ці концепції надихнути біологічними прикладами, такими як структура мозку, що складається з мільярдів нейронів, що мають схожу структуру, але здатні виконувати різноманітні функції, і мозок може відновлювати свою функціональність при пошкодженнях через надмірність. Що й застосовується у роботі інформаційно-керуючих навігаційних систем, тобто. надмірність інформації, тобто дублювання її з різних незв'язаних між собою пристроїв визначення місцезнаходження в просторі, як яких виступають інерційна і супутникова системи навігації. Дані кількох пристроїв навігації необхідно коректна поєднати для зменшення апаратних та деяких інших помилок обох пристроїв. Тут необхідно дати чіткі визначення надмірності та сверхнадлишковості. За визначенням В. Кондратова «надмірність — властивість вимірювальних систем виконувати більше функцій, ніж потрібно, причому з отриманням нової якості досяганні сукупності цілей (результатів надмірних вимірів)».

Надмірність - наявність чого-небудь у кількості, що перевищує вже додатково використовуване та необхідне для досягнення нової якості та обсягу виконуваних завдань (функцій) [1]. Саме цей напрямок

використовується алгоритмами поєднання. способів розв'язання задачі суміщення даних, одержуваних від кількох навігаційних пристроїв, є використання нейромережевого фільтра[2]. Коректне навчання та використання нейромережі дозволить на кожному кроці, враховуючи статистику попередніх вимірювань, формувати спільне рішення, точніше, ніж кожне окремо взяте, а також прогнозувати подальшу поведінку об'єкта[3].

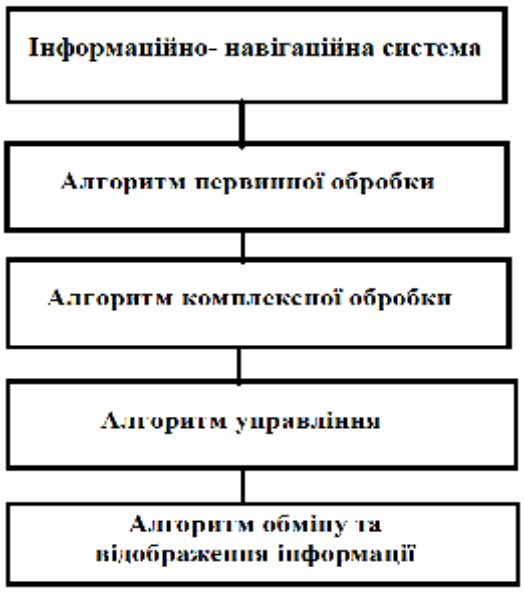


Рис. 1 Структурна схема загального алгоритму функціонування систем.

Загальний алгоритм інформаційно-керуючих навігаційних систем є сукупністю приватних алгоритмів, функціонально пов'язаних між собою, що реалізують завдання надійної обробки інформації з необхідною точністю та заданою дискретністю та вироблення керуючих та інформаційних сигналів. На рисунку1 наведено структурну схему загального алгоритму інформаційно-керуючих навігаційних систем. Комплексна обробка інформації включає завдання суміщення даних, одержуваних від кількох навігаційних пристроїв. Використання нейромережевих моделей для вирішення цього завдання дозволяє створювати адаптивні системи, обробка даних у яких здійснюється за допомогою паралельних операцій. Нейронні мережі мають ряд переваг: дозволяють враховувати попередні стану, паралельно виконувати безліч операцій, здатні до навчання та узагальнення, практично не враховують неінформативні шумові вхідні сигнали. Окрему групу нейронних мереж складають мережі із зворотним зв'язком між різними шарами нейронів. Мережа в якій кожен прихований шар пов'язаний із вхідним шаром називається нейронною мережею Елмана. Для вирішення завдання суміщення двох навігаційних даних у складі алгоритму за допомогою нейромережевого фільтра необхідно спочатку навчити нейронну мережу. Після навчання нейромережі Елмана здійснюється її моделювання. Враховуємо параметри руху, такі як: швидкість, синус і косинус кута щодо осі абсцис подаються на вхід мережі, що навчається. Критерієм оцінки похибки вибрано середньоквадратичне відхилення, значення для різних траєкторій вибирають після навчання зворотної мережі та додається траєкторія, отримана в внаслідок моделювання навченої нейромережі. Тому видно, що нейромережевий фільтр дозволяє визначити більш точно параметри руху, ніж кожна модель навігаційного пристрою окремо.

Список літератури

1. В.Т. Кондратов, Теория избыточных измерений:сверхизбыточные измерения — второй качественный скачок в фундаментальной метрологии. Вісник Хмельницького національного університету №4, с. 222-229, 2013.

2. П.В. Тимощук, Штучні нейронні мережі / П.В. Тимощук. – Львів : Вид-во НУ "Львівська політехніка", 2011. – 441 с.

3. А.М. Чернодуб, Навчання рекурентних нейронних мереж методом псевдорегуляризації для багатокрокового прогнозування часових рядів Математичні машини і системи, № 4 43 с. 41-51, 2012.

УДК 004.056, 004.75

С.В. Науменко[1,2], І.О. Розломій[1], Т.А. Стабецька[1]
naumenko.serhii1122@vu.cdu.edu.ua, inna-roz@ukr.net, tatiana_ami@vu.cdu.edu.ua
[1]Черкаський національний університет ім. Б. Хмельницького, м. Черкаси
[2]Active Bridge, м. Черкаси

СТРАХОВІ СМАРТ-КОНТРАКТИ: МАЙБУТНЄ СТРАХУВАННЯ НА ОСНОВІ БЛОКЧЕЙНУ ТА IOV

У світі постійно зростає значущість цифрових технологій у всіх сферах життя. Однією з галузей, яка не залишається поза цією трансформацією, є страхування. В сучасному суспільстві, де обмін даними стає все більш важливим, страхування не може лишитися осторонь від цієї цифрової революції [1]. Один із способів, яким цифрові технології революціонізують галузь страхування є впровадження страхових смарт-контрактів на базі технології блокчейн та Інтернету речей (IoT).

Страхування завжди було важливою галуззю для господарства та суспільства загалом. Однак у сучасних цифрових часах страхування зазнає суттєвих змін та адаптацій. Споживачі мають змогу отримувати доступ до різних видів страхування через онлайн-платформи та мобільні додатки. Такі технології надають змогу клієнтам обирати страхові поліси, порівнювати пропозиції різних компаній, та купувати страхові послуги безпосередньо через інтернет. Оглядаючи сучасні тенденції у страхуванні, стає очевидним, що дігіталізація та цифрові технології мають рішущий вплив на галузь [2].

Однією з ключових тенденцій є перехід від традиційних страхових полісів до цифрових послуг. Споживачі більше не мають бажання заповнювати складні анкети та спілкуватися безпосередньо з агентами. Вони вимагають зручності та доступності, які можуть надати цифрові платформи. Це вимагає від страхових компаній розвивати нові технологічні рішення та змінювати свій бізнес-підхід.

Однією з ключових інноваційних технологій, яка впливає на страхування, є блокчейн. Блокчейн - це розподілена база даних, яка забезпечує безпеку та надійність інформації. Використовуючи цю технологію, страхові компанії можуть підвищити довіру клієнтів, зменшити ризики шахрайства та спростити процеси врегулювання збитків.

Використання IoT в галузі страхування сприяє автоматизації та підвищує ефективність багатьох процесів. Інтеграція IoT-пристроїв дозволяє страховим компаніям збирати реальний час дані про стан об'єктів страхування, що створює унікальні можливості для точного визначення ризиків та оптимізації страхових послуг.

Страхування на основі використання в додатках Інтернету речей транспортних засобів (IoV) відоме як страхування на основі використання (UBI), що означає «usage-based insurance» [3]. Цей підхід до страхування дозволяє страховим компаніям встановлювати премії за страхування на основі реального використання транспортних засобів клієнтами. Основні принципи та механізми цього виду страхування такі:

1. Збір даних за допомогою сенсорів та мобільних додатків. Для збору даних використовуються сенсори в транспортних засобах, які відстежують різні параметри водіння, такі як швидкість, прискорення, гальмування та кут повороту.
2. Аналіз та оцінка ризику. Зібрані дані аналізуються для визначення рівня ризику, пов'язаного зі стилем водіння та поведінкою водіїв.
3. Персоналізоване страхування. UBI дозволяє страховим компаніям пропонувати персоналізовані тарифи, які відображають реальний ризик кожного конкретного водія.
4. Нагороди за безпечне водіння. Деякі програми UBI надають нагороди водіям за безпечне водіння, такі як знижки на премії або бонуси за кожен період без аварій.
5. Забезпечення персонального зворотного зв'язку. Ще одним важливим аспектом UBI є надання водіям персонального зворотного зв'язку на основі аналізу їхнього водіння.

UBI в додатках IoV дозволяє страховим компаніям більш точно оцінювати ризики, надавати персоналізовані страхові послуги та сприяти покращенню безпеки на дорозі.

Страхування на основі використання, що базується на використанні в додатках IoV, є інноваційним підходом до страхової сфери, де страхові політики та тарифи встановлюються на основі фактичного використання автотранспортних засобів, зібраних за допомогою датчиків та інших пристроїв IoT в автомобілях.

Цей підхід дозволяє страховим компаніям встановлювати страхові тарифи на основі реальних даних про використання автомобіля, таких як відстань, швидкість, стиль водіння та час. Він може забезпечити персоналізований підхід до страхування, де кожен водій може отримати страховий тариф, який відображає його конкретний стиль водіння та ризики, пов'язані з ним. Це може призвести до більш справедливого та ефективного встановлення страхових тарифів, сприяючи водіям, які виявляють безпечні стилі водіння, водночас заохочуючи інших водіїв до більш відповідальної поведінки за кермом.

Технології IoV та UBI можуть сприяти створенню більш адаптивних та інноваційних моделей страхування, які враховують індивідуальні ризики та особливості водіння кожного користувача.

IoV в основному ґрунтується на використанні технологій IoT для підключення транспортних засобів до Інтернету, щоб забезпечити збір, обмін та аналіз даних для поліпшення безпеки, ефективності та комфорту управління транспортом [4].

Основний принцип дії IoV включає в себе встановлення різних типів датчиків та пристроїв у транспортні засоби, таких як автомобілі, автобуси, вантажівки тощо. Ці пристрої забезпечують збір даних про різні аспекти роботи транспортного засобу, такі як швидкість, стан двигуна, температура, рівень палива, а також дані про середовище навколо транспортного засобу. Отримані дані передаються через бездротові мережі до центральної системи управління, де вони обробляються та аналізуються для отримання цінної інформації щодо ефективності роботи транспортних засобів, прогнозування технічного обслуговування, виявлення несправностей та управління транспортними потоками [3].

Цей принцип дії IoV сприяє покращенню безпеки на дорозі, оптимізації транспортних потоків, зменшенню витрат на паливо та технічне обслуговування, а також поліпшенню загального досвіду користувачів транспортних засобів. Шляхом збору, передачі та аналізу даних з транспортних засобів, IoV відіграє важливу роль у вдосконаленні транспортних систем та прискоренні переходу до майбутніх «розумних» транспортних інфраструктур.

Блокчейн відіграє ключову роль у підтримці страхування на основі використання в контексті IoV, забезпечуючи безпеку, прозорість та довіру в обміні даними між учасниками системи [1]. Децентралізована природа блокчейну дозволяє створювати недоступні для змін децентралізовані записи про угоди та дії, які можуть зберігати дані про використання транспортних засобів та страхові премії.

В основі блокчейну лежить принцип безпеки та невідворотності, що дозволяє створювати недоступні для змін записи даних. Це може бути використано для збереження важливих даних про страхові політики, включаючи дані про використання автотранспорту, винагороди за безпечне водіння та інші пов'язані з UBI деталі. Блокчейн також забезпечує конфіденційність даних, дозволяючи учасникам системи контролювати доступ до своїх особистих даних та забезпечувати їх захист від несанкціонованого доступу.

Завдяки використанню блокчейну, страхові компанії можуть забезпечити ефективний обмін даними з клієнтами та партнерами, забезпечуючи персоналізовані та справедливі страхові тарифи на основі реальних даних про використання автотранспорту. Це також сприяє покращенню відносин між страховиками та клієнтами, збільшуючи довіру та прозорість у страховій сфері.

IoV відіграє ключову роль у трансформації сучасних транспортних систем, прискорюючи їхню ефективність, безпеку та стійкість. Завдяки збору та аналізу різноманітних даних про стан транспортних засобів та дорожнє середовище, IoV надає можливості для оптимізації управління транспортними потоками, прогнозування несправностей, а також зменшення витрат на паливо та технічне обслуговування. Це сприяє підвищенню загальної ефективності транспортних систем і покращенню досвіду користувачів.

У майбутньому розвиток технологій IoV може призвести до створення ще більш розумних та автономних транспортних систем, які будуть взаємодіяти між собою та з інфраструктурою міст, забезпечуючи швидке реагування на змінні умови дорожнього руху. Впровадження IoV може також сприяти зменшенню екологічного впливу транспорту за рахунок оптимізації маршрутів, ефективного використання палива та підтримки розвитку електричних та екологічно чистих транспортних засобів. За умови правильної інтеграції та розробки стандартів безпеки та приватності, технології IoV можуть сприяти створенню безпечнішого майбутнього транспорту.

Список літератури

1. Li, Z., Xiao, Z., Xu, Q., Sotthiwat, E., Goh, R. S. M., & Liang, X. (2018, December). Blockchain and IoT data analytics for fine-grained transportation insurance. In 2018 IEEE 24th international conference on parallel and distributed systems (ICPADS) (pp. 1022-1027). IEEE.

2. Pettersson, D., Lillieskӧld, J., Händel, P., & Agerman, J. (2019, August). Usage-based auto insurance on the Swedish market: a case study. In 2019 Portland International Conference on Management of Engineering and Technology (PICMET) (pp. 1-9). IEEE.

3. Zhuo, Q. R., & Huang, Y. Z. (2019, October). Investigation on Consumers' Acceptance of Usage Based Insurance with Internet of Vehicles. In 2019 IEEE Eurasia Conference on IOT, Communication and Engineering (ECICE) (pp. 331-334). IEEE.

4. Peng, J., Liu, N., Zhao, H., & Yu, M. (2015, August). Usage-based insurance system based on carrier-cloud-client. In 2015 10th International Conference on Communications and Networking in China (ChinaCom) (pp. 579-584). IEEE.

УДК 004.056, 004.75

П.Р. Соляник
Науковий керівник: проф. Д.А. Кудій
Pavlo.Solianyk@cit.khpi.edu.ua
Національний технічний університет «Харківський політехнічний інститут», м. Харків

ЗАСТОСУВАННЯ ПЕРЕТВОРЕНЬ У ГРУПІ ТОЧОК ЕЛІПТИЧНОЇ НЕСУПЕРСИНГУЛЯРНОЇ КРИВОЇ ДЛЯ ФОРМУВАННЯ КЛЮЧОВИХ ХЕШ-ФУНКЦІЙ

Аналіз наявного підходу до побудови безключових хеш-функцій на основі перетворень у групі точок суперсингулярної еліптичної кривої (Map2Group і Map3Group) схеми цифрового підпису BLS засвідчив, що для застосування апарату еліптичних кривих у побудові ключових ітераційних схем хешування необхідно однозначно представити текст, який хешується, точкою кривої.

В наявних способах Map2Group і Map3Group ця необхідність викликає неоднозначність, або підвищення обчислювальної складності та накладає додаткове обмеження.

Розглянемо один із можливих підходів до побудови ключової схеми хешування, що дасть змогу уникнути недоліків схем Map2Group і Map3Group. Цей підхід полягає в застосуванні групи кручення точок еліптичної несингулярної кривої для побудови строго універсальних класів хеш-функцій.

Зафіксуємо довільну еліптичну несингулярну криву Ep і отримаємо всі точки кривої. Представимо інформаційні дані у вигляді блоків Mi. Кожен блок відкритого тексту Mi будемо представляти точкою Pi, порядок якої дорівнює n, а ключові дані представимо у вигляді чисел ki, при чому потужність множини можливих k, K кратна n. Як функцію відображення елементів множини Mi в елементи множини хеш-кодів h, Σn представимо скалярний добуток точки. У такому разі розподіл значень функції відображення можна представити у вигляді матриці.

kj\Qi	Q 1	Q 2	Q3
k1	Q1	Q2	Q3
k2	Q2	Q3	Q1
k3	Q3	Q1	Q2

При скалярному множенні точки кривої Pi на kj , за умови, що kj < n, усі результати добутку (точки) лежать у групі кручення, причому одноразово.

Отриманий розподіл має такі властивості:

1. Для кожного k кількість h, для яких h(M1) = h(M2) дорівнює 0.
2. Кількість k, для яких hk(M1) = hk(M2) не перевищує 1.

Отже, представлене сімейство функцій відображення відповідає строго універсальному класу хеш-функцій з параметрами -SU(n, n, n). Зауважимо, що в такому разі обсяг ключових даних дорівнює обсягу хешованих.

Перевагою цієї схеми є складність розкриття ключових даних, яка еквівалентна складності розв'язання задачі дискретного логарифмування в групі точок еліптичної кривої.

Розглянемо інший варіант застосування арифметики еліптичних кривих для побудови ключових ітераційних хеш-функцій.

Обмеження способів безключового хешування на базі арифметики суперсингулярної еліптичної кривої можна уникнути шляхом подання тексту Mi у вигляді числа si, де 0 < si < n, n - порядок групи крутіння точок кривої, а як секретний параметр використовувати базову точку кривої Q (секретна точка).

Таким чином, у результаті досліджень було отримано новий спосіб ключового хешування на базі арифметики в групі точок скручування несингулярної еліптичної кривої (спосіб Q-хешування), що дає змогу отримати новий підхід до побудови ключових хеш-функцій з використанням арифметики еліптичних кривих. Це дало змогу уникнути наявного обмеження в схемах хешування Map2Group і Map3Group. Розроблений спосіб одноразундового Q-хешування дає змогу за однократного використання ключа для кожного повідомлення забезпечити безумовну стійкість схем автентифікації, а за багатогранного - стійкість, яку можна довести, що є безсумнівною перевагою порівняно з наявними методами та способами ключового хешування. У разі багаторазової схеми ключового хешування запропонований спосіб дає змогу забезпечити стиснення і потенційно підвищити автентичність даних.

УДК 004.45

В.Д. Митренко, І.О. Розломій
mytrenko.vadym1118@vu.cdu.edu.ua, inna-roz@ukr.net
Черкаський національний університет ім. Б. Хмельницького, м.Черкаси

ВИКОРИСТАННЯ РОЗПІЗНАВАННЯ ОБРАЗІВ ПІД ЧАС СОРТУВАННЯ ПОБУТОВИХ ВІДХОДІВ

Сортування побутових відходів є надзвичайно важливою складовою сталого розвитку та збереження навколишнього середовища. Правильне сортування відходів допомагає зменшити кількість сміття, яке потрапляє на сміттєзвалища, що в свою чергу зменшує забруднення ґрунту та підземних вод. Також воно дозволяє максимально ефективно використовувати вторинні ресурси, такі як папір, скло, метал, і пластик, сприяючи ефективному використанню природних ресурсів та зменшенню виробництва нового сировини.

Застосування сучасного штучного інтелекту для розпізнавання образів сміття може стати надзвичайно корисним та прогресивним інструментом. Системи штучного інтелекту здатні розпізнавати та сортувати відходи на основі зображень, забезпечуючи високу точність у визначенні видів сміття. Завдяки штучному інтелекту сортування стає більш ефективним та автоматизованим процесом, що сприяє підвищенню якості переробки та зниженню навантаження на сміттєзвалища.

На початкових етапах розпізнавання образів сміття за допомогою смартфона та його камери може допомагати людині швидко та ефективно визначати, у який вид контейнеру слід відправляти ті чи інші відходи. Це стає корисною та зручною ініціативою. Перш за все, це дозволяє звичайним користувачам стати більш екологічно свідомими, оскільки їхні смартфони можуть стати потужними інструментами для сортування відходів. Також це означає можливість одним натисканням камери смартфона розпізнати види сміття і отримати інформацію про правильний спосіб його сортування. Така додаткова функція може значно спростити і популяризувати процес сортування вдома, на роботі чи навіть на вулиці. Додатково, такий вид використання може сприяти розвитку спеціалізованих додатків та платформ, які надають інформацію про місця збору та переробки сміття, а також сприяти моніторингу та обліку власного внеску до захисту довкілля. Такий підхід допомагає залучити більше людей до важливих процесів сортування відходів та зменшити навантаження на довкілля.

Сучасний штучний підхід до розпізнавання образів сміття включає в себе декілька ключових аспектів, які працюють спільно для досягнення найкращих результатів. Оптичне розпізнавання символів [1] використовується для ідентифікації текстової інформації, наприклад, на упаковці відходів. Воно дозволяє визначити текстові позначки або ідентифікувати інформацію, яка допомагає класифікувати сміття на основі підписів, що присутні на відходах. Класифікація об'єктів**,** виявлення об'єктів, виявлення контурів та виявлення особливостей розширюють можливості ШІ в розпізнаванні сміття. Вони працюють спільно для ідентифікації конкретних видів сміття та встановлення їхнього місця в класифікаційній системі. Виявлення об'єктів і контурів [2] допомагає ідентифікувати фізичні характеристики сміття, в той час як виявлення особливостей може бути корисним для виділення особливих деталей, таких як зношеність або дефекти у відходах. Ці різні методи розпізнавання допомагають створити комплексну систему, яка ефективно класифікує та сортує сміття, що сприяє збереженню навколишнього середовища та раціональному використанню ресурсів.

Отже, використання штучного інтелекту для сортування відходів представляє собою інноваційний підхід, що відкриває безліч переваг у сфері охорони навколишнього середовища та оптимізації управління відходами. Завдяки оптичному розпізнаванню символів, класифікації об'єктів, виявленню об'єктів, виявленню контурів та виявленню особливостей, сучасні системи ШІ здатні точно і ефективно визначати види сміття та ідентифікувати їхні особливості. Ця інтеграція допомагає покращити якість сортування відходів та підвищує свідомість населення щодо важливості екологічної відповідальності. Виходячи з цього, сучасний штучний інтелект сприяє зменшенню негативного впливу нашого суспільства на довкілля, сприяючи збереженню природних ресурсів та зменшенню навантаження на сміттєзвалища. Дана технологія відкриває нові можливості для боротьби з глобальними екологічними проблемами та сприяє створенню більш сталого та чистого оточуючого середовища для майбутніх поколінь.

Список літератури

1. Метод оптичного розпізнавання символів [Електронний ресурс]: https://en.wikipedia.org/wiki/Optical_character_recognition
2. Робота алгоритмів із виявлення об'єктів на зображенні [Електронний ресурс]: https://machinelearningmastery.com/object-recognition-with-deep-learning/

УДК 004.8, 656.02

В.С. Лебеденко, О.А. Кислун
lebedenkovitalik0@gmail.com, kyslun@gmail.com
Центральноукраїнський національний технічний університет, м. Кропивницький

ВИКОРИСТАННЯ КЛАСИЧНИХ МЕТОДІВ РОЗВ'ЯЗАННЯ ЛОГІСТИЧНИХ ЗАДАЧ ДЛЯ ПОБУДОВИ АЛГОРИТМУ ПОШУКУ МАРШРУТІВ ОПТИМАЛЬНОГО ПОСТАЧАННЯ

Оскільки, кінцевою метою дослідження в рамках якого отримані результати, що наводяться, є розробка програмного забезпечення для пошуку оптимальних маршрутів за певних специфічних умов постачання, то, відповідно, саме класичні алгоритми пошуку найкоротшого шляху лягають в основу побудови алгоритму пошуку [1].

Вивчивши роботу класичних алгоритмів пошуку A*, Дейкстри, Беллмана-Форда та інших, скорегуємо алгоритм пошуку маршрутів оптимального постачання [2].

Формально маємо потребу в адаптації алгоритму класичної задачі про найкоротші шляхи з одним виходом, на яку накладено умову затратності використання додаткового прохідного пункту в маршруті. Оскільки вартість вантажних робіт загалом є основною складовою витрат, то для врахування вказаних затрат пропонується ввести в якості опису матрицю затрат. Нехтуючи можливою відмінністю величин вантажних робіт в одному прохідному пункті для різних вхідних та вихідних шляхів, а залишивши лише відмінність вантажних робіт в самому пункті - матриця затрат буде представлена лише вектором.

Враховуючи, що має будуватися повний набір найменш затратних шляхів з усіх вершин до вказаної, постановка задачі про найкоротший шлях з класичної зводиться (відповідно до економічного змісту задачі) до наступної. Нехай на визначеному направленому граф G (з скінченним набором вершин вектор V з зазначеним вектором затрат Z) та ребер E (з зазначеною функцією ваги f, для пари заданих вершин v^a та v^k), необхідно знайти набір оптимальних маршрутів постачання (найменші шляхи P (ланцюги від всіх V до вказаної вершини v^k серед усіх можливих шляхів, що поєднують вершини з урахуванням направленості та затратності).

По аналогії до класичних алгоритмів, перед початком знаходження менш затратних шляхів, проводимо початкові визначення: для кожної вершини - вартості доставки нескінченно великі, шляхи відсутні (пусті множини); для кінцевої вершини вартість доставки нуль, шлях до неї - сама вершина (її безпосередня назва, кодований шифр або номер) .

Наступною дією є позначення наявності менш затратного шляху, для входження в перебір вершин для відшукання можливого більш економного шляху постачання (позначення наявної можливості знаходження менш затратного шляху).

Організація перебору всіх вершин (з попереднім визначенням відсутності менш затратного шляху), в якому проводиться відшукання з кожної вершини дешевшого шляху постачання, для чого для кожної з вершин організовується перебір дуг, які поєднують вибрану вершину з вершиною, з якої задане постачання, і якщо порівнявши наявну вартість доставки з вершини з сумою вартості доставки з вершиною, що поєднано дугою, вартістю вантажних робіт у вершині поєднаної дугою та величини доставки з вершини визначеною за допомогою дуги, і якщо вартість доставки з вершини буде більшою, то вона перевизначиться на суму з якою порівнювалася, при цьому перевизначається шлях до вибраної вершини на саму вершину плюс шлях до вершини, поєднаної дугою, та позначається наявної можливості знаходження менш затратного шляху.

Якщо після переборів вершин та дуг виявляється можливість знаходження менш затратного шляху, то перебір повторюється аж до появи після перебору визначеності відсутності менш затратного шляху, що свідчить про завершення пошуку маршрутів оптимального постачання.

Для задачі оптимального постачання початкова умова доповнена потребою (величина a) та наявністю (вектор наявності N), а до алгоритму буде додано лише послідовний добір менш затратних шляхів до повного задоволення потреби.

Список літератури

1. Лебеденко В.С., Кислун О.А.. Огляд методів розв'язання логістичних задач пошуку оптимальних маршрутів / Матеріали VI Міжнародної науково-практичної конференції "Інформаційна безпека та комп'ютерні технології": тези доповідей, 20-21 квітня 2023р. -Кропивницький: ЦНТУ, 2023. стр.42

2. Креневич А.П. Алгоритми і структури даних. Підручник. – К.: ВПЦ "Київський Університет", 2021. – 200 с.

УДК 004.6:514:519.2

O.Y. Chepurna[1], O. Grushina[2], Y.R. Kuleshova[1]
chepurna@onua.edu.ua, grushinaolga@gmail.com, evgeniya.kuleshowa@gmail.com
[1]National University "Odesa Law Academy", Odesa
[2]FedEx Express, Miami, FL

INFORMATION GEOMETRY AS TOOLS FOR DATA ANALYSTS

Information geometry is a new method that applies the principles of differential geometry to the study of information. In recent years, this field has received increasing attention, especially in the natural sciences, where it has been applied to various fields such as physics, biology, and neuroscience and data analysis.

A core aspect of information geometry is its mathematical background. The field relies heavily on concepts from differential geometry, topology, and probability theory. These concepts are used to describe the properties of different statistical models and their interrelationships. Information geometry also uses tools such as Riemannian metrics and curvature tensors to develop a geometric understanding of statistical spaces [1].

The main advantage of information geometry is that it provides a unified approach to the study lot of objects and allows researchers and practitioners from different fields to communicate more effectively. One area where information geometry is particularly useful is in statistical computing algorithms. By using geometric concepts such as curvature, researchers have been able to develop new algorithms for optimization problems that are efficient and robust. This has led to improvements in techniques for analyzing large data sets in fields ranging from genetics and neuroscience to economics and finance [2].

Another application of information geometry in the natural sciences is the understanding of complex systems. By modeling these systems as manifolds embedded in high-dimensional spaces, researchers can use geometric tools such as differential equations to gain insight into their behavior [3].

Information geometry provides geometric concepts and tools for exploring the space of probability distributions. These spaces arise naturally in theory and applications. For example, the unit simplex describes the possible distribution of independent signals in a finite alphabet. A statistical model such as the multivariate normal distribution can be viewed as a collection of probability distributions over an appropriate state space [4].

Information geometry uses the formal tools of differential geometry to describe the space of probability distributions as a Riemannian manifold with an additional dual structure. The formal equivalence of compositional data with discrete probability distributions makes it possible to apply the same description to the sample space of Compositional Data Analysis (CoDA) [5]. The latter is formally described as a Euclidean space with an orthogonal basis, the components of which are appropriate combinations of primitive parts. In contrast to the Euclidean metric, the information geometry description emphasizes that the Fisher information metric is the only metric that preserves the geometric structure of the manifold under equivalent representations of the underlying random variables. Well-known concepts valid in Euclidean coordinates, such as B. Pythagoras' theorem, are generalized through information geometry to corresponding ideas applicable to more general coordinates [6].

From a geometric perspective, information geometry deals with various probability distributions [7]. It studies invariant structures using Riemannian geometry equipped with a pair of affine connections. Since probability distributions are used in many problems in optimization, machine learning, vision, statistical inference, neural networks, etc., information geometry is a useful and powerful tool in many areas of information science and engineering [8].

It is worth noting that some information theory problems, including parameter estimation, entropy maximization, dimensionality reduction, and interpolation between distributions, can be explained from a geometric perspective. For example, information geometry is based on distances between parameterized probability distributions on the Fisher Information Matrix (FIM) [9].

The results of information geometry are therefore directly related to the foundations of estimation theory. This geometric approach provides valuable insights into the design and understanding of algorithms.

Traditionally, information geometry has been viewed as a parametric statistical model of Riemannian manifolds. For such models, the Riemannian metric (called the Fisher information metric) is a natural choice. In the special case where the statistical model is an exponential family, the statistical manifold can be derived using the Hessian metric (i.e., the Riemannian metric given by the potential of the convex function) [10].

Much of the past work has been devoted to studying the geometries associated with these examples. In modern settings, information geometry is applied in a wider range of contexts, including non-exponential families, non-parametric statistics, and even abstract statistical manifolds that are not generated by known statistical models [11].

Since the introduction of Riemannian geometry to statistics, information geometry has been developed along various directions. The statistical curvature as the differential-geometric analogue of information loss and sufficiency was proposed by Efron. The α-duality of information geometry was found by Amari. Not being

limited to statistical inference, information geometry has become popular in many different fields, such as information-theoretic generalization of the expectation-maximization algorithm [5], hidden Markov models, interest rate modeling, phase transition and string theory. More applications can be found in the literature [11] and the references therein.

In particular, time series analysis and signal processing are well-known applications of information geometry. Ravishanker et al. found the information geometry of autoregressive moving average (ARMA) models in the coordinate system of poles and zeros. It was also extended to fractionally integrated ARMA (ARFIMA) models. The information geometry of autoregressive (AR) models in the reflection coefficient coordinates was also reported by Barbaresco. In the information-theoretic framework, Bayesian predictive priors outperforming the Jeffreys prior were derived for the AR models by Komaki.

Kähler manifolds are interesting topics in differential geometry. On a Kähler manifold, the metric tensor and the Levi–Civita connection are straightforwardly calculated from the Kähler potential, and the Ricci tensor is obtained from the determinant of the metric tensor. Moreover, its holonomy group is related to the unitary group. Because of these properties, many implications of Kähler manifolds are found in mathematics and theoretical physics. In addition to these fields, information geometry is one of those fields where the Kähler manifolds are intriguing. After the symplectic structure in information geometry and its connection to statistics were discovered, notably introduced Kähler manifolds to information geometry for time series models and also generalized the differential-geometric approach with mathematical structures, such as Koszul geometry. Additionally, Zhang and Li found symplectic and Kähler structures in divergence functions [12].

By studying the application of information geometry in machine learning and statistical inference, one can understand the geometric structure of statistical models and optimize learning algorithms. Information geometry provides a logical framework for evaluating and improving a variety of machine learning and statistical inference tasks by examining the underlying geometry of probability distributions and parameter spaces.

Information geometry's ability to measure similarities or differences between probability distributions using geometric distances is one of its main advantages. This makes it possible to create distance-based algorithms for tasks such as anomaly detection, classification, and grouping. Furthermore, the geometric properties of the parameter space aid in the development of effective optimization techniques by revealing information about the optimization environment of the learning algorithm.

Information geometry has significant potential for improving our empower tools for data analysis. From data analysis to statistical inference, its application is wide-ranging and powerful. The applications of information geometry are impressive, from statistical physics to machine learning, and have the ability to provide us with more accurate predictions and more meaningful insights. Moreover, it can bridge the gap between disciplines by providing a common language for conversation and collaboration. Information geometry is certainly an exciting area of research that warrants further exploration in the future.

Reference

1. C. R. Rao. Information and the accuracy attainable in the estimation of statistical parameters, Bulletin of Calcutta Mathematical Society, vol. 37, pp. 81–91, 1945.
2. S. Amari and H. Nagaoka, Methods of Information Geometry. American Mathematical Society, 2000.
3. S. Amari, Information Geometry and Its Applications. Springer, 2016.
4. K. V. Mishra and M. A. Kumar:" Generalized Bayesian Cramer- Rao inequality via information geometry of relative α-entropy", in IEEE Annual Conference on Information Sciences and Systems, 2020, pp. 1–6.
5. Plastino, A. S. R. S. Rao, and C. R. Rao, Information Geometry, ser. Handbook of Statistics. Elsevier, 2021, vol. 45.
6. J. Brehmer, K. Cranmer, F. Kling, and T. Plehn, Better Higgs boson measurements through information geometry, Physical Review D, vol. 95, no. 7, p. 073002, 2017.
7. S. Mac Lane, Categories for the Working Mathematician, 2nd ed. Springer, 1971.
8. S. Amari, "Information geometry," Japanese Journal of Mathematics, vol. 16, pp. 1–48, 2021.
9. Doucet, A., Godsill, S., Andrieu, C.:" On sequential Monte Carlo sampling methods for Bayesian filtering". Stat. Comput. 10(3), 197–208 (2000)
10. Liu, X., Srivastava, A., Gallivan, K.:" Optimal linear representations of images for object recognition". IEEE Pattern Analitics. Mach. Intell. 25(5), 662–666 (2004)
11. Lenglet, C., Rousson, M., Deriche, R., Faugeras, O.: Statistics on the manifold of multivariate normal distributions: theory and application to diffusion tensor MRI processing. J. Math.Imaging Vis. 25, 423–444 (2006)
12. J. Mikes at al. Differential Geometry of Special Mapping. Univerzita Palackého v Olomouci, 2019

УДК 004.94

Р.О. Антонов, Є.В. Мелешко, Я.П. Шуліка, Д.В. Бащенко
elismeleshko@gmail.com
Центральноукраїнський національний технічний університет, м. Кропивницький

ПРОГРАМНЕ ІМІТАЦІЙНЕ МОДЕЛЮВАННЯ СТОХАСТИЧНИХ ПРОЦЕСІВ У СКЛАДНИХ МЕРЕЖАХ МЕТОДОМ ВИПАДКОВИХ БЛУКАНЬ «LEVY FLIGHT»

Сучасна теорія складних мереж спрямована на моделювання різних існуючих мереж – біологічних, технічних, соціальних. Вона зосереджена переважно на моделюванні структури природних або технічних мереж з великою кількістю вузлів та зв'язків. Часто для створення повноцінної моделі треба крім структури моделювати також процеси, що відбуваються у складній мережі. Наприклад, для створення програмної імітаційної моделі комп'ютерної мережі необхідно генерувати не тільки топологію мережі, а й рух трафіку по ній тощо.

Метою цієї роботи було створення методу програмного імітаційного моделювання інформаційних процесів у складних мережах у вигляді стохастичних часових рядів.

Для програмного імітаційного моделювання інформаційних процесів у складних мережах було обрано клас методів, що називається *випадкові блукання*. Випадкове блукання – це випадковий процес, який описує шлях, що складається з послідовності випадкових кроків у деякому математичному просторі [1]. Після проведеного дослідження існуючих методів випадкових блукань було обрано метод випадкових блукань Levy flight [2, 3] для вирішення поставленої у роботі задачі.

Метод випадкових блукань Levy flight (політ Леві) – це випадкове блукання, у якому довжини кроків мають стійкий розподіл, тобто розподіл ймовірностей має важкий хвіст. Якщо визначити як блукання у просторі розмірності більше одиниці, зроблені кроки відбуваються в ізотропних випадкових напрямках. Польоти Леві за будовою є марківськими процесами. Для загальних розподілів розміру кроку, що задовольняє умові степеневого типу, відстань від початку випадкового блукання прагне, після великої кількості кроків, до стійкого розподілу через узагальнену центральну граничну теорему, що дозволяє моделювати багато різних процесів за допомогою польотів Леві.

Метод Levy flight було реалізовано на мові програмування Python наступним чином:

```
import numpy as np # Підключення бібліотек
import matplotlib.pyplot as plt
alpha = 1.5  # Параметр степеневого розподілу (1 < alpha < 2)
x = [0] # Початкові координати
y = [0]
max_x = 100 # Максимальні координати
max_y = 100
num_steps = 1000 # Кількість кроків
for _ in range(num_steps):
    step_length = np.random.pareto(alpha) # Генеруємо крок за розподілом Леві
    step_angle = np.random.uniform(0, 2 * np.pi) # Генеруємо випадковий кут
    new_x = x[-1] + step_length * np.cos(step_angle) # Обчислюємо нові
координати
    new_y = y[-1] + step_length * np.sin(step_angle)
    new_x = min(max_x, max(0, new_x)) # Обмеження координат за межами деякого
простору
    new_y = min(max_y, max(0, new_y))
    x.append(new_x)
    y.append(new_y)
plt.figure(figsize=(8, 8)) # Візуалізація траєкторії польоту Леві
plt.plot(x, y, 'b-', linewidth=0.5)
plt.title("Випадковий інформаційний процес методом Леві в обмеженому просторі")
plt.xlabel("X-координата")
plt.ylabel("Y-координата")
plt.xlim(0, max_x)
plt.ylim(0, max_y)
plt.grid(True)
plt.show()
```

Таким чином розроблений код дозволяє отримувати два випадкові числові ряди: x – список координат по осі X та y – список координат по осі Y. Їх можна використати наступним чином, для деякого x_0 вузла мережі може генеруватися його інформаційна активність методом Levy flight, де x_i може вказувати на номер вузла складної мережі, якому x_0 передає інформацію у поточний момент часу, а y_i –

кількість інформації, яку передає x_0 до x_i. Тобто, для кожного вузла мережі слід створювати свій окремий процес у вигляді Levy flight.

Візуалізація роботи реалізованого методу Levy flight представлена на рис. 1.

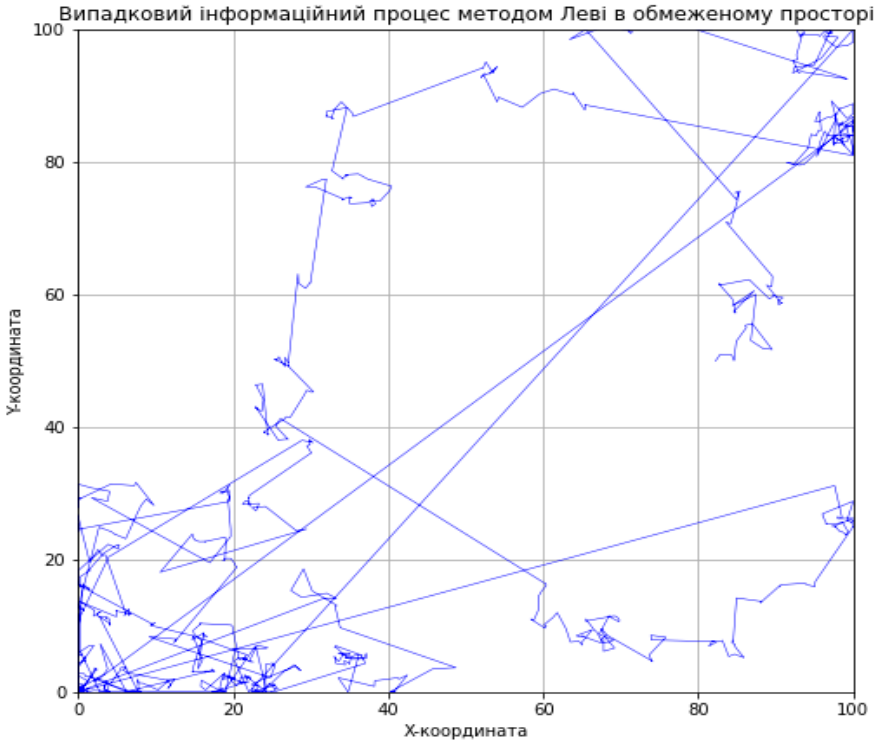


Рис. 1. Візуалізація результатів роботи реалізованого методу випадкового блукання Levy flight

У даному прикладі складна мережа містить 100 вузлів (приклад мережі на рис. 2) і кожен вузол мережі може надіслати іншому від 0 до 100 одиниць інформації за одиницю часу.

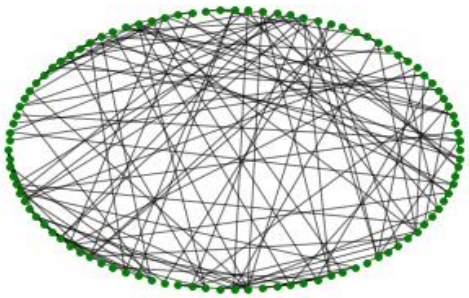


Рис. 2. Приклад структури складної мережі, для якої відбувалося моделювання стохастичних інформаційних процесів

Тож, у роботі було реалізовано метод програмного імітаційного моделювання стохастичних процесів у складних мережах на основі випадкових блукань «Levy flight».

Список літератури

1. Révész P. (2013) Random Walk in Random and Non-random Environments (Third Edition). World Scientific Pub Co. DOI: http://dx.doi.org/10.1142/8678

2. Chechkin A. V., Metzler R., Klafter J., Gonchar V. Yu. (2008) Introduction to the Theory of Lévy Flights. Anomalous Transport. pp. 129–162. DOI: http://dx.doi.org/10.1002/9783527622979.ch5

3. Kleinberg J. M. (2000) Navigation in a small world. Nature. Vol. 406(6798): 845. DOI: https://doi.org/10.1038/35022643

УДК 004.056, 004.75

Д.А. Амбросьєв, М.Д. Михайлов
DimaDA@gmail.com, Misha_DM@gmail.com
Центральноукраїнський Національний технічний університет, м. Кропивницький

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ ВЕБ-ЧАТУ ДЛЯ ОБМІНУ ДАНИМИ В МЕРЕЖІ ІНТЕРНЕТ

Інтернет зайняв важливе місце в житті сучасної людини. Сьогодні вже неможливо уявити життя без комп'ютера і звичайно ж доступу до Всесвітньої мережі. Мільярди людей ввесь час займаються серфінгом сайтів у пошуках потрібної інформації.

На сьогоднішній день сучасне уявлення про Інтернет значно змінилося із тих пір, коли почала широко розвиватись сфера інформаційних технологій. Інтернет набув великих змін, які у свою чергу дають змогу будувати принципово нові уявлення про Інтернет-технології та їх застосування. На даний час кожний веб-ресурс, який є у мережі Інтернет побудований на інноваційних принципах. Існує багато веб-технологій, які використовуються для побудови та створення веб-ресурсів (сайтів).

Метою роботи є дослідження та програмна реалізація системи веб-чату для обміну даними в мережі Інтернет.

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

– огляд існуючих систем веб-чату;
– дослідження діючої системи веб-чату;
– програмна реалізація системи веб-чату.

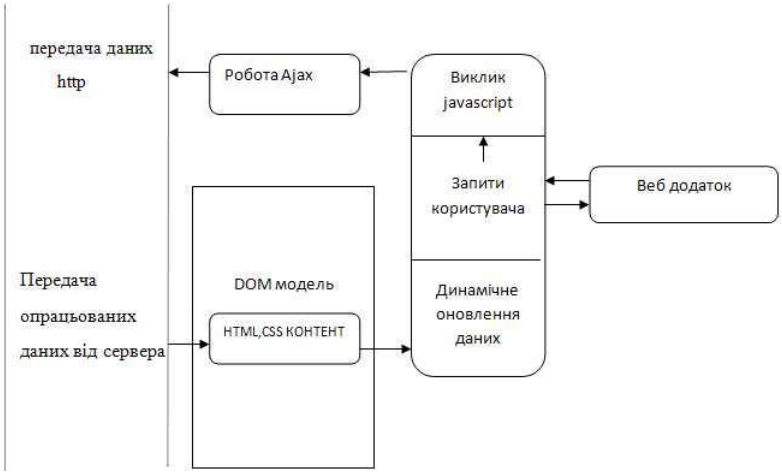


Рис. 1. Робота додатку з використанням технології Ajax.

У процесі рішення завдань, обумовлених цілями дослідження, отримані наступні результати:

– удосконалено систему передачі даних онлайн-чату з розробкою підсистеми безпеки передачі даних;
– проведено огляд технологій передачі миттєвих повідомлень в режимі реального часу.

Розроблено вітчизняний продукт з використанням технології Ajax є конкуретним на ринку і можливі подальші шляхи вдосконалення системи.

Список літератури

1. Scholz M., Fraunholz M., Selbig J., Nonlinear Principal Component Analysis: Neural Network Models and Applications, In: Gorban A. N. et al (Eds.), LNCSE 58, Springer, 2007 ISBN 978-3-540-73749-0

2.Люк Веллинг, Лора Томсон. Розробка Web -додатків за допомогою PHP і MySQL : Вільямс, 2012р., - 880 с.

3. SQL [Електронний ресурс] – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/SQL

4. TypeScript [Електронний ресурс] – Режим доступу до ресурсу: https://www.typescriptlang.org/

УДК 004.8

А.М. Мельник, Є.В. Мелешко, В.В. Босько
mselnikanna@gmail.com
Центральноукраїнський національний технічний університет, м. Кропивницький

ДОСЛІДЖЕННЯ ГРАФОВИХ НЕЙРОННИХ МЕРЕЖ

Останнім часом штучний інтелект значно прискорює прогрес у розвитку людства, трансформуючи спосіб життя, яким ми живемо та працюємо. Одним з сучасних інструментів штучного інтелекту є графові нейронні мережі (GNN), які відкривають шлях для машинного навчання нового покоління [1].

Структура GNN. Для розуміння графових нейронних мереж треба звернутися до теорії графів [2]. Ця теорія говорить про те, що граф – математична структура, яка представляє взаємодію між об'єктами. Граф складається з вузлів та вершин. Графові нейронні мережі представляються у вигляді графу та використовуються в задачах, які включають прогнозування вузлів, ребер і графів [3].

Використання GNN. В основному алгоритми машинного навчання часто мають проблеми з обробкою графових даних, тому на допомогу приходять графові нейронні мережі, які і були розроблені для обробки та аналізу графових даних. Графові нейронні мережі використовуються для обробки інформації в соціальних мережах (роботі з посиланнями та обміном), транспортних системах, молекулярних структурах (наприклад, порядок зв'язків в молекулярних структурах), обробка тексту та зображень [3].

Графові нейронні мережі мають як переваги так і недоліки, які були досліджені та розглянуті нижче.

Переваги графових нейронних мереж:

− Здатність обробляти різний розмір та структуру графів. Традиційні алгоритми машинного навчання в основному працюють саме з фіксованим розміром інформації і це є проблемою для обробки даних. В графових нейронних мережах розмір залежить від кількості вузлів та вершин, тому графова структура може бути динамічна та змінюватись з часом.

− Здатність аналізувати соціальні мережі. було помічено надзвичайну продуктивність в аналізі вподобань користувачів, визначенні впливових людей та виявленні спільнот в мережі.

− Здатність аналізувати молекулярні структури. Досягнуто значного успіху у передбаченні структур білків, аналізі даних про експресію генів та відкритті потенційних маркерів лікарських засобів.

Недоліки графових нейронних мереж:

− При збільшенні інформації, з якою працюють графові структури, можна стикнутись зі зростанням обчислювальної складності графових нейронних мереж, оскільки більше інформації (масштабування системи) потребує більших зусиль для її обробки.

− Через високі обчислювальні витрати цих мереж масштабування моделі для виробництва представляє проблеми.

− Навчати графові нейронні мережі складніше, оскільки їх структура динамічна.

− Поки що GNN є неглибокими мережами, зазвичай із трьома рівнями, а більшість сучасних нейронних мереж мають багато прошарків. Це ускладнює аналіз даних зі складною структурою.

− Графові нейронні мережі досі досліджуються, тому наразі вони є "чорними ящиками", але за допомогою сучасних технологій, ця проблема може у найближчому майбутньому вирішитись.

Порівняння графових мереж з іншими. Останнім часом графові нейронні мережі знайшли застосування в різних областях, включаючи комп'ютерний зір, рекомендаційні системи, комбінаторну оптимізацію тощо. Крім того, ці мережі можна використовувати для представлення складних систем, включаючи соціальні мережі, мережі білкової взаємодії, графи знань тощо. Важливою особливістю графових нейронних мереж від інших нейронних мереж є обробка саме графових структур даних. Також ці мережі дозволяють покращили аналіз та обробку динамічних даних та забезпечують високий рівень точності роботи для таких структур. Але цей тип мереж ще недостатньо досліджений, а також алгоритми їх роботи на даний час мають високу складність, що негативно впливає на обробку великих масивів даних та використанні для виробництва.

Список літератури

1. Sanchez-Lengeling B., Reif E., Pearce A., Wiltschko A. B. A Gentle Introduction to Graph Neural Networks [Електронний ресурс] // Distill. – 2021. – URL: https://distill.pub/2021/gnn-intro/

2. Gould R. Graph theory // Courier Corporation. – 2012. – 350 pages

3. PyTorch Graph Neural Network Tutorial [Електронний ресурс] // HashDork. – 2022. – URL: https://hashdork.com/pytorch-graph-neural-network-tutorial/

УДК 621.397.335.1

Е.В. Фауре[1], М.В. Махинько[2]
e.faure@chdtu.edu.ua
[1]*Черкаський державний технологічний університет, м. Черкаси*
[2]*GoodLabs Studio Inc.,м. Торонто*

ОЦІНКА ПОКАЗНИКІВ КАДРОВОЇ СИНХРОНІЗАЦІЇ НА ОСНОВІ ПЕРЕСТАНОВОК

Системи передавання даних з нероздільним факторіальним кодуванням [1, 2] слугують для захисту інформації від несанкціонованого доступу та помилок каналу зв'язку і використовують нестандартну та надлишкову структуру кадру – перестановку π чисел $\{0;1;\ldots;M-1\}$. У цій структурі не передбачено окремого поля роздільника кадрів, а кадрову синхронізацію встановлюють за робочим сигналом [3, 4]. Така структура кодового слова нероздільного факторіального коду дозволяє йому слугувати транспортним механізмом у системах зв'язку з короткими пакетами, що є особливістю сучасних бездротових мереж, мереж даних датчиків, а також наднадійних і машинних комунікацій.

Ця праця демонструє показники ефективності кадрової синхронізації на основі перестановок [3] у залежності від довжини M синхропослідовності – перестановки π.

Етапи методу кадрової синхронізації на основі перестановок [3]:

1) передавач використовує як синхропослідовність перестановку π довжини M, що володіє максимальним значенням мінімальної відстані Хеммінга d від її двійкового представлення до всіх її циклічних зсувів;

2) приймач накопичує прийняті з каналу зв'язку K блоків, що містять l фрагментів по n біт;

3) для кожного блоку незалежно мажоритарно обчислюють кожен біт уточненої послідовності R_k, $k \in [1, K]$;

4) для кожної R_k обчислюють відстані Хеммінга до всіх циклічних зсувів синхропослідовності. Якщо для якось зі зсувів ця відстань не перевищує значення $d_{lim} = \lfloor (d-1)/2 \rfloor$, система синхронізації приймає рішення щодо відповідності R_k цьому зсуву;

5) якщо всі R_k відповідають одному і тому ж циклічному зсуву синхропослідовності, синхронізм встановлено. У протилежному випадку необхідно повернутися до п. 2;

6) накопичення фрагментів відбувається до деякого, заздалегідь визначеного, порогу. Якщо після досягнення цього порогу синхронізм не знайдено, процедуру його пошуку завершують.

Під час дослідження ефективності описаного методу кадрової синхронізації виконано:

– теоретичну оцінку ймовірнісних показників системи кадрової синхронізації для $M = 8$ і $M = 16$, виконано їх порівняння за визначених показників імовірності бітової помилки p_0;

– комп'ютерне імітаційне моделювання системи кадрової синхронізації для $M = 8$ і $M = 16$, визначено та експериментально ймовірнісні показники системи кадрової синхронізації, виконано їх порівняння за визначених показників імовірності бітової помилки p_0.

Визначено, що система кадрової синхронізації на основі перестановок з $M = 8$ і $d_{lim} = 5$ вимагає для встановлення синхронізму менше біт у порівнянні з системою синхронізації з $M = 16$ і $d_{lim} = 14$. Разом з тим, більше значення M дозволяє збільшити потужність ключового простору, що може бути необхідним для забезпечення визначених показників криптостійкості.

Список літератури

1. Faure E. V. Factorial coding with data recovery. Bulletin of Cherkasy State Technological University. 2016. № 2. P. 33–39.

2. Al-Aazzeh J., Ayyoub B., Faure E., Shvydkyi V., Kharin O., Lavdanskyi A. Telecommunication systems with multiple access based on data factorial coding. International Journal on Communications Antenna and Propagation. 2020. Issue 10. № 2. P. 102–113.

3. Al-Azzeh J., Faure E., Shcherba A., Stupka B. Permutation-based frame synchronization method for data transmission systems with short packets. Egyptian Informatics Journal. 2022. Issue 23. № 3. P. 529–545.

4. Faure E. V., Stupka B. A. Evaluation of Frame Synchronization Efficiency for Non-Separable Factorial Codes Depending on Synchronization Parameters. Èlektron. model. 2022. Issue 44. № 6. C. 21–35.

УДК 004.891:681.518.5

І.А. Лисенко
min_max@i.ua
Центральноукраїнський національний технічний університет, м. Кропивницький

МЕТОДИ ПОБУДОВИ ТЕСТОВИХ НАБОРІВ В ІНФОКОМУНІКАЦІЙНИХ СИСТЕМАХ

Сучасні ІКС характеризуються високим рівнем складності розроблюваних компонентів, в першу чергу програмного забезпечення (ПЗ) інформаційної та комунікаційної підсистем. Це накладає певні вимоги на реалізацію фаз життєвого циклу розробки ПЗ ІКС, починаючи від фази аналізу і завершуючи фазою прийняття ПЗ. Однією з визначальних фаз життєвого циклу ПЗ ІКС, на якій здійснюється контроль його якості, є фаза тестування.

Тестування ПЗ – це перевірка відповідності між реальною і очікуваною поведінкою програмного продукту, що здійснюється з використанням заздалегідь сформованої множини тестових наборів. При цьому очікувана поведінка програмного продукту, як правило, представляється у вигляді вимог до ПЗ ІКС. Найбільш повну перевірку виконання вимог до ПЗ можна здійснити на рівні системного тестування.

Широкими можливостями з перевірки вимог до ПЗ володіють методи їх формалізованого опису, що використовуються в рамках відповідних інформаційних технологій тестування. У сучасному розумінні це технології побудови тестових наборів, які складаються з одного або декількох тестових випадків. У загальному вигляді їх можна розглядати як сукупність методів побудови, перевірки коректності і аналізу потоків управління тестових наборів. Одним з найзручніших методів, які використовуються для побудови тестових наборів для перевірки ПЗ інформаційних систем, що характеризуються залежністю від прийняття логічних рішень, є таблиці рішень (ТР).

Аналіз особливостей інформаційної підсистеми ІКС показав, що відповідна підсистема розглядається як підсистема залежна, насамперед, від прийняття логічних рішень, реалізованих за допомогою функцій інформаційної підсистеми ІКС в її ПЗ. У ході аналізу особливостей різних рівнів тестування ПЗ інформаційної підсистеми ІКС виявлено, що перевірку коректності ПЗ інформаційної підсистеми ІКС повною мірою можна здійснити в рамках його тестування на системному рівні. При цьому в якості методів побудови тестових наборів використовуються методи «чорного ящика».

Проведений аналіз основних груп методів побудови тестових наборів і тестових випадків з використанням методів «чорного ящика» показав, що в якості базового методу побудови тестових наборів для перевірки ПЗ інформаційної підсистеми ІКС найзручніше використовувати метод ТР. Водночас в якості показників глибини тестування побудованих тестових наборів і тестових випадків обрані відповідно:

- повнота тестового покриття вимог до ПЗ тестовими наборами,
- тестове покриття на базі аналізу потоків управління
- достовірність тестових наборів

У результаті аналізу можливостей методу ТР для формалізованого опису тестових наборів визначено необхідність його вдосконалення в напрямку підвищення описових можливостей для представлення впорядкованих умов і можливості формування каскадних ТР, а також у розробці методів перевірки коректності модифікованих ТР в рамках удосконаленої технології побудови тестових наборів [1].

Виконана практична апробація вдосконаленої технології побудови тестових наборів з використанням ВКТР на базі проектних рішень в нотації UML для програмного забезпечення клієнтського додатка розподіленої електронної банківської системи. В рамках практичної апробації розроблені відповідні тестові набори з використанням нового і традиційного підходів. Проведено оцінку витрат часу на виявлення неврахованих ситуацій в ТР з використанням удосконаленого методу перевірки коректності ТР зі складу ВКТР, який дозволяє зробити висновок про те, що витрати часу на виконання наведеного алгоритму ростуть поліноміально зі збільшенням розміру таблиць і не гірше, ніж в квадратичній залежності. Аналіз глибини тестування програмного забезпечення проведено шляхом перевірки показників ефективності застосування удосконаленої технології побудови тестових наборів також дав позитивний результат.

Список літератури

1. *Lysenko I.A.* Information technology of developing test kits based on software requirements / I.A. Lysenko, O.A. Smirnov // International Journal of Computational Engineering Research (IJCER). – Delhi (India), 2016. – Volume 6, Issue 1. – P. 35-38.

УДК 681.17

А.М Мацуй., М.С Мірошніченко., А.Р. Бокій, Д.Ю. Комаров
matsuyan@ukr.net, marymir@ukr.net, andrearhangel88@gmail.com, ppkomarovd@gmail.com
Центральноукраїнський національний технічний університет, м. Кропивницький

АНАЛІЗ ФАКТОРІВ ВПЛИВУ НА ЗМІНУ НОРМИ ВИСІВУ В ПОЛЬОВИХ УМОВАХ

При традиційній технології землеробства задана для даного поля норма висіву (кг/га) встановлюється один раз перед початком сівби, шляхом регулювання та фіксації відповідних значень передаточної величини, відстані до денця котушки та її робочої довжини. Але в процесі сівби на стабільність норми висіву впливає ряд зовнішніх факторів: фракція посівного матеріалу, тряска, вібрації, запиленість, ланцюгова передача, просковзування опорно-привідного колеса, коефіцієнт заповнення жолобків котушкового висівного апарата посівним матеріалом та інше.

Вплив цих факторів проявляється по різному. Нестабільність ланцюгової передачі повторюється з кожним обертом опорно-привідного колеса, тому компенсувати дію цього циклічного впливу зміною норми висіву не можливо. Просковзування опорно-привідного колеса є випадковим фактором, залежним від рельєфу поверхні та її стану, зворотньої дії навантаження дозуючих апаратів та іншого. Дія цього фактора може бути короткою за часом або тривалою. В останньому випадку її можна частково компенсувати регулюванням.

Найбільш суттєвим фактором, який діє на протязі усього терміну сівби є коефіцієнт заповнення жолобків посівним матеріалом. В результаті тряски та вібрації сівалки має місце сегрегація посівного матеріалу по висоті та горизонталі усередині бункера в залежності від розміру та щільності зерна: менші за розміром зернини, які мають однакову щільність, і більш важкі зернини, що мають однакові розміри, переміщуються в нижні шари, легші та більші за розміром зернини розміщуються в верхніх шарах. Швидкість розшарування підвищується із збільшенням розміру і різниць в щільностях відокремлюємих зернин, інтенсивності вібрацій та із зменшенням товщини шару. Крім того, при заповненні бункера близькому до 100%, посівний матеріал ущільнюється, що зменшує його подачу в зону дії дозуючих апаратів. Зменшення подачі посівного матеріалу спостерігається і при заповненні бункера менше ніж на 15% від його об'єму. В результаті тривалої роботи дозуючі апарати забиваються пилом, що також впливає на коефіцієнт їх заповнення посівним матеріалом. Для того, щоб врахувати дію вказаних факторів відомчими стандартами передбачено проведення випробувань при різних об'ємах зерна в бункері (100;50;25) відсотках заповнення бункеру, а також проведення повторних випробувань через 1 та 3 години безперервної роботи висівного аппарату.

З врахуванням фізико-механічних властивостей, розміру зернин, схожості посівного матеріалу, особливостей поля та кліматичних умов, що склалися, приймають рішення про щільність посіву. При визначеній нормі висіву необхідно на сівалці без втрат часу виставити необхідний режим сівби і впевнитися в цьому, тому, для забезпечення якісної сівби зернові сівалки необхідно обладнати системами автоматичного керування або регулювання норми висіву.

Список літератури

1. Пархоменко Ю. М. Теоретичне дослідження статики зернового потоку котушкового висівного апарата / Ю. М. Пархоменко // Техніка в сільськогосподарському виробництві, галузеве машинобудування, автоматизація – Кіровоград КНТУ. – 2007. – Вип. 19. – С. 151-156.
2. Заїка П. М. Теорія сільськогосподарських машин. Т.1, частина 2. Машини для сівби та садіння / П. М. Заїка - Харків: Око, 2002. - 452 с.

УДК 004.89

Г.О. Молнар, д-р техн. наук, проф. С.П. Євсеєв
hanna.molnar@cit.khpi.edu.ua, serhii_yevseiev@khpi.edu.ua
Національний технічний університет «Харківський політехнічний інститут», м. Харків

ШТУЧНІ НЕЙРОННІ МЕРЕЖІ

Актуальність дослідження штучних нейронних мереж залишається високою в сучасному світі з багатьма важливими застосуваннями і викликами. Їх починають активно використовувати медицині (сегментація зображення пухлини [1], діагностика біполярних та шизофренічних розладів [2], модель для передбачення виживання при раку легень [3] тощо), в автономних системах та транспортних засобах (автомобілі [4], дрони та роботи, прогнозування серйозності аварії [5] тощо), у питаннях екології та геології (передбачення областей видобутку сланцевої олії [6]), комп'ютерному зорі [7]), інформаційних системах [8] та кібербезпеці [9], хімії та фізиці та інших напрямках.

Рис. 1. Деякі з основних аспектів.

Зважаючи на ці фактори, дослідження штучних нейронних мереж продовжують розвиватися, що має великий вплив на багато сфер життя і може призвести до нових інновацій та можливостей.

Але не можна ігнорувати проблеми, пов'язані з нейронними мережами: прозорість та конфіденційність даних та застосування штучних нейронних мереж для вирішення конкретних завдань чи, наприклад, етичні питання їхнього використання.

Дослідження етичних аспектів є важливою частиною розвитку та використання штучних нейронних мереж, оскільки вони сприяють створенню етичних стандартів та забезпеченню етичної відповідальності в цій сфері.

Рис. 2. Дослідження різних аспектів застосування штучних нейронних мереж.

Ці дослідження допомагають визначити найкращі практики та створити етичні стандарти для використання штучних нейронних мереж в сучасному суспільстві.

Деякі вчені у своїх роботах [10] вже зазначають велику кількість етичних проблем, такі як:

- Обмежений доступ до інфраструктури та ресурсів, необхідних для розробки і впровадження систем штучного інтелекту, що може призвести до обмеження можливостей для інновацій та конкуренції.
- Зміни в трудових процесах, спричинені впровадженням систем штучного інтелекту, особливо в ризикових галузях з низькими кваліфікаціями, що породжують питання про існуючі соціальні захисти та розподіл ресурсів.
- Впровадження систем штучного інтелекту, які можуть діяти як фоновий процес, не відомий і невидимий для тих, на кого вони впливають, і не завжди можна перевірити їх точність і справедливість.
- Законодавчі обмеження, які загрожують проведенню досліджень в галузі відповідальності систем штучного інтелекту.
- Відсутність стандартних методів вимірювання та оцінки соціальних і економічних впливів систем штучного інтелекту.
- Відсутність участі тих, на кого впливають системи штучного інтелекту, у їхньому проектуванні та розробці.
- Недостатнє представництво різних голосів та перспектив в розробці та дослідженні систем штучного інтелекту.
- Недостатнє врахування соціальних та економічних складностей впровадження систем штучного інтелекту в професійних кодексах етики та освіті.

Підсумовуючи: оскільки тема нейронних мереж наразі досить актуальна і стрімко поширюється на великий сектор наукових галузей, необхідно освітлювати і звертати увагу на явні проблеми щодо етичності їхнього можливого використання. Для ефективного, безпечного та законного впровадження та розповсюдження штучних нейронних мереж ще необхідний деякий час.

Список літератури

1. Wang, S.H., Jiang, J.L. and Lu, X.B. (2020) Advances on Tumor Image Segmentation Based on Artificial Neural Network. Journal of Biosciences and Medicines, 8, 55-62.
2. Fonseca, M.B., de Andrades, R.S., de Lima Bach, S., Wiener, C.D. and Oses, J.P. (2018) Bipolar and Schizophrenia Disorders Diagnosis Using Artificial Neural Network. Neuroscience & Medicine, 9, 209-220
3. Rodrigo, H. and Tsokos, C.P. (2017) Artificial Neural Network Model for Predicting Lung Cancer Survival. Journal of Data Analysis and Information Processing, 5, 33-47.
4. Harris, T.P., Nix, A.C., Perhinschi, M.G., Wayne, W.S., Diethorn, J.A. and Mull, A.R. (2021) Implementation of Radial Basis Function Artificial Neural Network into an Adaptive Equivalent Consumption Minimization Strategy for Optimized Control of a Hybrid Electric Vehicle. Journal of Transportation Technologies, 11, 471-503.
5. Dipto, I.C., Rahman, Md.A., Islam, T. and Rahman H.M.M. (2020) Prediction of Accident Severity Using Artificial Neural Network: A Comparison of Analytical Capabilities between Python and R. Journal of Data Analysis and Information Processing, 8, 134-157
6. Wu, T. T., Bai, X., Shang, F., Zhou, H. Y., Wang, L., Zhou, X. X., Zhong, Z., Yang, Z., Zhang, J. Y., Cheng, X. Y., Zhang, P. Y., & Chen, R. Q. (2023). Quantitative and Comprehensive Prediction of Shale Oil Sweet Spots in Qingshankou Formation, Songliao Basin. Journal of Geoscience and Environment Protection, 11, 290-315.
7. Ribeiro, P. , Lopes, G. and Ribeiro, F. (2016) Neural Network in Computer Vision for RoboCup Middle Size League. Journal of Software Engineering and Applications, 9, 319-325.
8. Maqableh, M. , Karajeh, H. and Masa'deh, R. (2014) Job Scheduling for Cloud Computing Using Neural Networks. Communications and Network, 6, 191-200.
9. Journal of Information Assurance and Security, Volume: 16, Issue: 1, 2021, pp.010-023
10. Kate Crawford, Meredith Whittaker, Madeleine Clare Elish, Solon Barocas, Aaron Plasek, Kadija Ferryman, 2016 'The AI Now Report: The Social and Economic Implications of Artificial Intelligence.' Tabled with the White House Office of Science and Technology Policy for their Future of Artificial Intelligence Series. 25pp. C. 3-5

СЕКЦІЯ 3. ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ЕКОНОМІЦІ, МЕДИЦИНІ ТА ОСВІТІ

УДК 004.942

В.В. Решетняк, аспірант II курсу
v.v.reshetniak.asp22@chdtu.edu.ua
Науковий керівник Е.В. Фауре, доктор технічних наук, професор
Черкаський державний технологічний університет, м. Черкаси

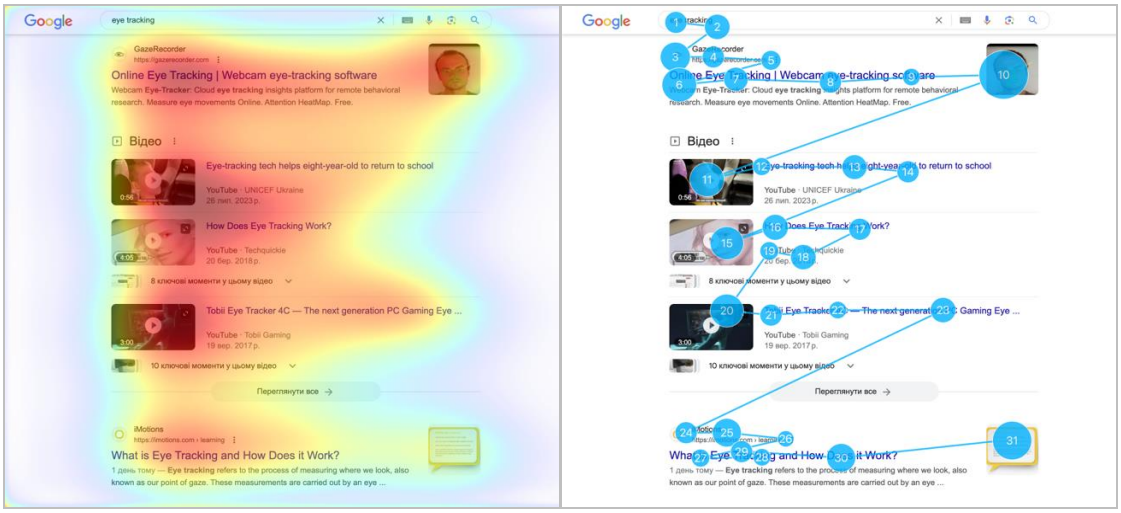
ВІЗУАЛІЗАЦІЯ РЕЗУЛЬТАТІВ ДОСЛІДЖЕНЬ З ВІДСЛІДКОВУВАННЯ ПОГЛЯДУ

Сфера відслідковування погляду (айтрекінгу) активно розвивається і має широке практичне застосування. Маючи десятиліття розвитку, ця сфера не втрачає актуальності і зараз: розробляються нові методи відслідковування, підвищується точність досліджень завдяки покращенню якості камер, відкриваються нові сфери застосування. Так, айтрекінг використовують у маркетингу, дизайн дослідженнях, а також у медичних дослідженнях, наприклад, для виявлення розладу аутистичного спектру [1], в розмежуванні доступу [2], і навіть у дресируванні тварин [3].

Для відслідковування погляду використовують декілька видів спеціальних програмно-апаратних комплексів — айтрекерів. Існують комплекси на основі пристроїв зовнішнього монтування, мобільних окулярів для відслідковування погляду, вбудованих камер пристроїв, а також комплекси, що відслідковують погляд у віртуальній та доповненій реальностях. Головною задачею таких пристроїв є зчитування відеопотоку з камер, що направлені на очі, виокремлення з цього потоку і розпізнавання переміщення очей, а також порівняння цих рухів з відповідною зоною на екрані або в просторі. Проте головну роль для аналізу поведінки користувача мають саме результати проведених досліджень і відповідне відображення зібраної інформації.

Айтрекери збирають як просторову інформацію про переміщення погляду, так і часову. Таким чином можна отримати інформацію про тривалість фіксації погляду в окремій області, швидкість переміщення погляду між такими фіксаціями, відстежити маршрут переміщення погляду за відповідним стимулом, а також визначити зону інтересу стимулу (Area of Interest, AOI), яка привертає більше уваги користувача.

У [4] подано детальний структурований огляд існуючих методів візуалізації. Запропоновано класифікувати методи за наступними групами: статистичні графіки, методи візуалізації на основі точок переміщення погляду та методи на основі зон інтересу. Запропоновано поділяти методи візуалізації на часові, просторові та просторово-часові. Додатковими характеристиками, що можуть описувати метод візуалізації, є статичність чи динамічність, двовимірність чи тривимірність, наявність візуалізації в контексті та поза ним, ступінь інтерактивності візуалізації, а також кількість користувачів, яких одночасно досліджують. У [5] наведено класифікацію методів візуалізації, сфокусовану на відображенні зібраних даних у тривимірному просторі.



(а) (б)

Рис. 1. Приклади теплової карти та маршруту погляду вебсторінки

У практичній площині основними методами візуалізації результатів айтрекінгу є теплові карти (heat maps або attention maps) та маршрути погляду (gaze plots або scan path) на основі точок переміщення погляду [6].

Теплові карти фіксації погляду (рис. 1а) запропоновано в 1958 році вченими Mackworth J. F. та Mackworth N. H. Такі карти представляють відображення часових і просторових даних, наприклад, кількість або тривалість фіксацій користувача. Для відображення, як правило, використовують кольорову шкалу (наприклад, зелений-жовтий-червоний). Цю кольорова інформація, накладена на вихідний стимул, може бути накопичена від декількох учасників. Щоб уникнути розсіяної візуалізації та мати плавну карту, до областей фіксації застосовують фільтр Гауса [5]. Використовуючи колір для відображення зібраних даних, легко визначити, на які стимули користувачі витрачають більше часу.

Маршрути погляду (рис. 1б) становлять собою відображення точок фіксації у вигляді кіл, що накладають на стимули. Радіус кола пропорційний тривалості відповідної фіксації. Два кола послідовних фіксацій з'єднані лінією, що представляє сакаду — переміщення погляду, яке йде від першої фіксації до другої. Таким чином створюється повний шлях фіксацій. У кожному колі відображають порядковий номер фіксації. Ця часова інформація корисна, наприклад, для візуалізації області стимулу, на якій було сфокусовано погляд у першу чергу під час дослідження. Маршрут погляду представляє дані про рух очей одного конкретного користувача. У випадку відстеження погляду декількох користувачів усі маршрути погляду накладають на стимули [5].

Окрім методів на основі точок переміщення погляду, практичне застосування в дослідженнях з динамічними стимулами мають методи на основі зон інтересу (AOI). Зони інтересу визначають як області в просторі стимулу, які є важливими для дослідження і можуть бути використані для аналізу різних метрик переміщення погляду, таких як фіксації, сакади або маршрути погляду. У більшості випадків такі зони інтересу створюють окремо під кожне дослідження, що займає додатковий час на налаштування цих зон.

Перед дослідниками, що займаються темою відслідковування погляду, відкриваються широкі можливості для вдосконалення існуючих методів візуалізації. Так виникають виклики для візуалізації результатів відслідковування динамічних стимулів, оскільки необхідно розмежовувати фіксації погляду на відповідні часові відрізки відслідковування. Подібні виклики виникають і під час дизайн дослідженнях мобільних додатків за допомогою айтрекінгу. Оскільки мобільні додатки мають свої особливості побудови користувацького інтерфейсу порівняно з вебсайтами — менший розмір екрану, більшу щільність функціональних елементів, менший час взаємодії з окремим екраном додатку, — то і візуалізація відслідковування погляду повинна відповідати цим викликам. Виникає потреба в створенні таких методів візуалізації, що дозволять аналізувати взаємодію погляду на кожному екрані додатку, а також порівнювати їх між собою. Крім того, варто врахувати розвиток методів тривимірної візуалізації результатів айтрекінгу. Такі методи візуалізації будуть необхідні в дослідженнях з відслідковування погляду в реальному просторі та імерсивних середовищах. Удосконалюючи методи тривимірної візуалізації, можуть використовуватись дані з додаткових датчиків (наприклад LIDAR) для розрахунку відстані або імітованої відстані до візуального стимулу. Ще одним викликом для вдосконалення існуючих методів, що базуються на зонах інтересу, є автоматизація побудови таких зон інтересу. З цією метою можуть бути використані нейромережі для розпізнавання образів і окреслення відповідних зон інтересу. Таким чином, розвиток і вдосконалення методів візуалізації відслідковування погляду є актуальним завданням, що може призвести до покращення розуміння психологічних та практичних аспектів взаємодії користувача з різними типами інтерфейсів та середовищ.

Список літератури

1. Machine learning based on eye-tracking data to identify autism spectrum disorder: a systematic review and meta-analysis / Q. Wei та ін. SSRN electronic journal. 2022. URL: https://doi.org/10.2139/ssrn.4100664 (дата звернення: 14.09.2023).

2. Шаманіна Т., Павленко В. Метод захисту інформації в комп'ютерних системах за даними айтрекінгу. Інформатика та математичні методи в моделюванні. 2021. Т. 11, № 1-2. С. 115–126.

3. Pelgrim M. H., Espinosa J., Buchsbaum D. Head-mounted mobile eye-tracking in the domestic dog: a new method. Behavior research methods. 2022. URL: https://doi.org/10.3758/s13428-022-01907-3 (дата звернення: 14.09.2023).

4. State-of-the-Art of visualization for eye tracking data / T. Blascheck та ін. *EuroVis - STARs*. 2014.

5. Sundstedt V., Garro V. A systematic review of visualization techniques and analysis tools for eye-tracking in 3D environments. Frontiers in neuroergonomics. 2022. Т. 3. URL: https://doi.org/10.3389/fnrgo.2022.910019 (дата звернення: 27.09.2023)

6. Bojko A. Eye tracking the user experience: a practical guide to research. Rosenfeld Media, LLC, 2013.

УДК 004.7.056.5(477)(047)

Ю.В. Білявська
доцент кафедри менеджменту, кандидат економічних наук, доцент
y.biliavska@knute.edu.ua
Державний торговельно-економічний університет, м. Київ

ЦИФРОВІ КОМПЕТЕНТНОСТІ В УМОВАХ ПЕРЕХОДУ ДО СУСПІЛЬСТВА 5.0.

Цифрова грамотність сприяє прискоренню економічного зростання та залученню інвестицій, розвитку цифровізації в промисловості і підприємництві, підвищенню конкурентоспроможності, модернізації, а також створенню високотехнологічних галузей, доступу до можливостей цифрового світу. Саме тому зміни в сучасному суспільстві зумовлені інтенсивним поширенням процесів інформатизації та технологізації, які, в свою чергу, формують відповідний рівень культури та визначають актуальність дослідження цифрової компетентності.

В еру розвитку діджиталізації ключову роль відіграють цифрові навички та цифрова грамотність, які характеризуються вмінням застосовувати на практиці сучасні програмні продукти, засоби комунікацій і зв'язку та інформаційні технології. Випадки витоку даних, що почастішали, і зростання масштабів цього явища викликають все більшу стурбованість у споживачів. Підприємствам необхідно зрозуміти такі побоювання та прийняти відповідні заходи, інакше вони ризикують втратити можливість управляти бізнесом. Саме тому для процвітання в новій економіці, що базується на інформації, підприємствам доцільно розвивати знання дескрипторів цифрової компетентності персоналу. Важливу роль відіграє набір властивостей і характеристик, які дозволять описати змістові модулі контенту компетентностей, можливих при виконанні таких заходів. До них належить забезпечення кібербезпеки та захист персональних даних, формування довіри до управління даними, неухильне дотримання законодавства та прозорості у роботі, розуміння споживачів, оскільки саме на них орієнтована робота підприємств.

Рівні володіння цифровими компетентностями вказують на певний мінімально необхідний набір знань, умінь і навичок громадян, якими вони повинні володіти. Такі навички необхідні для виконання заданого набору функцій залежно від обійманої посади чи поставленої перед ними задачі. Реальний рівень володіння певними компетентностями визначається тестуванням громадян за відповідними змістовними навчальними модулями. Саме з цією метою у 2019 році Міністерством цифрової трансформації України було презентовано «Держава і я» (мобільний застосунок, вебпортал і бренд цифрової держави) [1]. З поміж безлічі можливостей портал «ДІЯ» містить розділ «Цифрова освіта» де детально представлено рамки цифрової компетентності. Такий інструмент створений для того, щоб покращити рівень цифрових компетентностей українців, допомогти у створенні державної політики та плануванні освітніх ініціатив. Такі заходи спрямовані на підвищення рівня цифрової грамотності та практичного використання засобів і сервісів ІТ-технологій конкретними цільовими групами населення. Рамка охоплює 5 сфер цифрових компетентностей, які містять 20 компетентностей та 6 рівнів володіння [2]. Таким чином, це інструмент для формування дієвих цифрових компетентностей впровадження яких забезпечить розвиток цифрової грамотності та уникнення ІТ перешкод. Узагальнюючи [22] сформуємо каскад дескрипторів Рамки цифрової компетентності в умовах дотримання цифрової грамотності персоналу (рис. 1).

При розробці української рамки цифрових компетентностей для громадян використаний підхід, що передбачає адаптацію кращих європейських рамок цифрових компетентностей, а також відповідні нормативні та науково-методичні засади, що вироблені в Україні.

Представлений каскад дескрипторів Рамки цифрової компетентності охоплює реалізацію деяких положень, які є актуальними у веденні діяльності різними галузями промисловості:

– перехід до Індустрії 4.0. та Суспільства 5.0. вимагає набуття не лише певного набору, а цілого комплексу ключових компетентностей громадянина або фахівця;

– різноманітні чинники внутрішнього та зовнішнього середовища у результаті своєї взаємодії впливають на формування цифрових компетентностей та дескрипторів;

– формування переліку необхідних компетентностей відбувається з урахуванням менталітету, світогляду, цінностей, економічних та технологічних можливостей країни, галузі та підприємства;

– на узагальнений вибір цифрових компетеностей впливають фактори, які пов'язані з особистістю, а саме вік, стать, сімейний стан, соціальний статус, освіта, навички та знання;

– вибір, визначення та імплементація цифрових компетентностей потребує додаткового обговорення, застосування методу Делфі та Agile технологій фахівцями різноманітних структурних підрозділів.

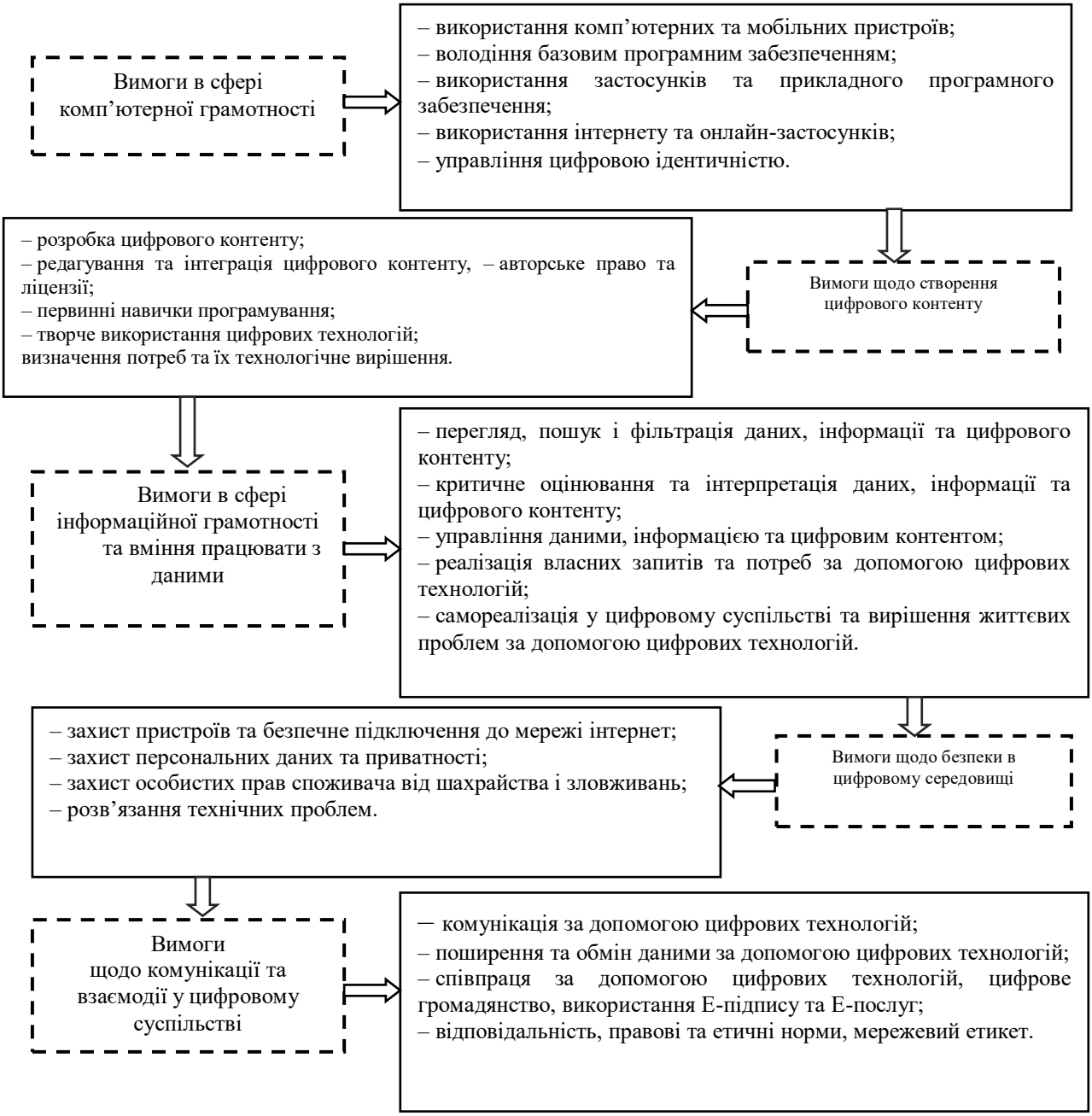


Рис. 1. Каскад дескрипторів Рамки цифрових компетентностей

Джерело: узагальнено на основі [2]

Таким чином, визначені напрями у каскаді цифрових компетентностей відображають детальну інформацію та наповнення необхідними дескрипторами. Дотримання визначених у суспільстві або на підприємстві цифрових компетентностей забезпечить громадянам та працівникам можливість уникнення помилок цифрової грамотності. Важливою умовою є те, що за допомогою певних ресурсів можна пройти тестування та отримати сертифікат про рівень знань цифрових компетентностей.

Список літератури

1. Офіційний сайт Державні послуги онлайн URL: https://diia.gov.ua/
2. Опис Рамки цифрових компетентностей для громадян України. URL: https://thedigital.gov.ua/storage/uploads/files/news_post/2021/3/mintsifra-oprilyudnyue-ramku-tsifrovoi-kompetentnosti-dlya-gromadyan/%D0%9E%D0%A0%20%D0%A6%D0%9A.pdf

УДК 004.9

В.В. Алексеєнко, С.П. Гуменюк
work.alekseenko@gmail.com, stanislav.humeniuk@gmail.com
Житомирський державний університет імені Івана Франка, м. Житомир

ВИКОРИСТАННЯ ЦИФРОВИХ ІНСТРУМЕНТІВ ДЛЯ ПЕРСОНАЛІЗАЦІЇ НАВЧАННЯ

Використання цифрових інструментів для персоналізації навчання є однією з ключових стратегій у сучасній освіті. Це дозволяє навчальним установам та викладачам створювати більш ефективні та індивідуалізовані навчальні траєкторії для кожного здобувача освіти. Персоналізоване навчання може допомогти здобувачам краще засвоїти навчальний матеріал, розвинути свої навички та досягти своїх навчальних цілей. Крім того, персоналізація навчання може допомогти здобувачам відчути себе більш мотивованими та залученими до навчального процесу.

Варто виокремити ряд важливих переваг використання цифрових інструментів для персоналізації навчання, які впливають на якість освіти та сприяють досягненню більшого успіху здобувачів:

1. Індивідуалізація навчання. Кожен здобувач унікальний та має власний темп навчання, рівень здібностей й стиль вивчення. Цифрові інструменти дозволяють адаптувати матеріал до потреб кожного здобувача, надаючи індивідуалізовані завдання та ресурси.

2. Підвищення залученості. Використання технологій та інтерактивних матеріалів може зробити навчання більш цікавим і захоплюючим для здобувачів. Вони більше зацікавлені в процесі навчання та активніше залучаються до нього.

3. Зростання продуктивності. Цифрові інструменти дозволяють ефективно відстежувати прогрес здобувачів та надавати зворотний зв'язок в реальному часі. Це допомагає викладачам адаптувати навчальний процес та вчасно реагувати на труднощі.

4. Більша доступність. Освітні ресурси та матеріали можуть бути доступні з будь-якого місця та в будь-який час завдяки цифровим інструментам. Це особливо корисно для дистанційного навчання та навчання на відстані.

5. Адаптація до різних стилів вивчення. Деякі здобувачі освіти краще вивчають візуально, інші - аудіально, інші - кінестетично. Цифрові інструменти можуть включати різні типи ресурсів і завдань, щоб відповідати різним стилям вивчення.

6. Співпраця та комунікація. Використання цифрових інструментів дозволяє здобувачам співпрацювати між собою та комунікувати з викладачами, навіть якщо вони знаходяться на відстані. Це сприяє розвитку навичок співпраці та комунікації.

7. Використання аналітики для покращення навчання. Цифрові інструменти збирають дані про успішність здобувачів, їхні відповіді та прогрес. Ця аналітика допомагає краще розуміти потреби здобувачів та розробляти ефективніші навчальні плани.

Для індивідуалізації навчання активно застосовуються адаптивні навчальні платформи. Ці навчальні платформи використовують технології штучного інтелекту (AI) і машинного навчання для персоналізації навчання та адаптації змісту та завдань до потреб кожного конкретного здобувача освіти. Вони спрямовані на надання здобувачам персоналізованих матеріалів та завдань відповідно до їхнього рівня знань, стилю вивчення та потреб. Адаптивні платформи починають з аналізу поточного рівня знань та вмінь здобувача, проводячи тести, вправи або аналізуючи відповіді. Це допомагає визначити, з якого рівня потрібно розпочати навчання та які конкретні теми потребують уваги. На основі результатів аналізу платформа може вибирати матеріали, завдання та ресурси, які відповідають потребам здобувача. Адаптивні платформи автоматично налаштовують рівень складності завдань на основі успішності здобувача. Якщо здобувач стикається з труднощами, рівень завдань може бути знижений, а якщо він показує високу компетентність, то складність зростає. Окрім того, здобувачі можуть вчитися у власному темпі, переглядаючи матеріал більше разів, якщо це потрібно, або переходячи до нових тем, коли вони готові. Платформи можуть надавати здобувачам освіти зворотний зв'язок щодо їхньої успішності, вказівки та рекомендації для подальшого навчання. [1]

Серед адаптивних платформ варто виокремити наступні[3]:

- Khan Academy, яка використовує адаптивний підхід для навчання математики, науки, програмування та багатьох інших предметів. Платформа надає індивідуалізовані завдання та відеоуроки в залежності від рівня знань здобувача.
- Coursera пропонує курси від провідних університетів та організацій. Вони використовують адаптивний підхід для пропозиції додаткових матеріалів та завдань для здобувачів, які потребують додаткового виклику.

- EdX – це платформа для масових відкритих онлайн-курсів (MOOCs), яка також використовує адаптивний підхід для навчання. Вона надає індивідуалізовані рекомендації та завдання.
- Smart Sparrow – це платформа, спеціалізована на адаптивному навчанні в області науки та інженерії. Вона створена для створення індивідуалізованих курсів.
- DreamBox – це адаптивна платформа для навчання математики, спрямована на дітей з раннього віку. Вона надає індивідуалізовані завдання та вправи для кожного учня.
- ALEKS (Assessment and Learning in Knowledge Spaces) – це платформа для навчання математики та науки, яка використовує адаптивні тести та завдання для визначення рівня знань і подальшого навчання.

Загалом, адаптивні навчальні платформи дозволяють створювати індивідуалізовані навчальні траєкторії, які враховують потреби та можливості кожного здобувача, що сприяє покращенню якості освіти.

Використання електронних підручників та інтерактивних засобів навчання дозволяє вибирати контент, який відповідає потребам та інтересам здобувачів. Такі матеріали можуть містити різні типи вмісту, такі як текст, відео, аудіо, графіку, інтерактивні вправи та багато іншого. Оскільки електронні підручники можуть містити різні джерела та типи інформації, здобувач може вибирати той спосіб вивчення, який відповідає його стилю вивчення: читати тексти, дивитися відео, слухати аудіо тощо. Отож, використання електронних підручників та засобів навчання сприяє персоналізації навчання, роблячи його більш ефективним та захоплюючим.

До цифрових інструментів для персоналізації навчання варто віднести й перегляд відео та вебінарів, що дозволяє здобувачам навчатися відповідно до власного графіка та повторювати матеріал за необхідністю. Вебінари можуть надавати можливість взаємодії з викладачами та іншими здобувачами навіть у віддаленому режимі. До таких інструментів та платформ варто віднести [2]:

- Платформа YouTube надає доступ до безлічі відеоуроків на різноманітні теми.
- Kaltura – це платформа для створення та розповсюдження відеоуроків.
- Zoom – це відомий сервіс для відеоконференцій та вебінарів, який дозволяє викладачам та тренерам проводити онлайн-уроки та зустрічі в режимі реального часу.
- Edpuzzle дозволяє викладачам створювати інтерактивні відеоуроки, додавати питання та завдання прямо до відео, що допомагає перевіряти розуміння матеріалу.
- Adobe Connect – це платформа для проведення вебінарів і онлайн-уроків з можливістю інтерактивної взаємодії між здобувачами та викладачем.
- Google Meet – це інструмент для відеоконференцій від Google, який може використовуватися для проведення онлайн-уроків та вебінарів.
- Microsoft Teams – це платформа для співпраці та комунікації, яка також має можливості для проведення відеоконференцій та вебінарів.

Використання цих цифрових інструментів допомагає підвищити залученість здобувачів до навчання, забезпечує більшу індивідуалізацію та сприяє зростанню результативності освіти. Такий підхід дозволяє кожному здобувачеві освіти розвиватися на своєму власному шляху та враховувати їхні унікальні потреби та здібності.

Розглянуті засоби – це лише деякі приклади того, як цифрові інструменти можуть бути використані для персоналізації навчання. Існує багато інших цифрових інструментів, які можна використовувати для персоналізації навчання, і з розвитком технологій ми будемо бачити все більше і більше інноваційних способів використання цифрових інструментів для персоналізації навчання.

Однак важливо зазначити, що персоналізація навчання – це не панацея. Важливо, щоб викладачі належним чином використовували цифрові інструменти для персоналізації навчання. Вони також повинні бути обережними, щоб не ігнорувати потреби здобувачів, які не користуються цифровими технологіями.

Список літератури

1. Близнюк Т. Цифрові інструменти для онлайн і офлайн навчання: навчально-методичний посібник. Івано-Франківськ: Прикарпатський національний університет імені Василя Стефаника, 2021. 64 с.

2. Іванюк І.В. Цифрові інструменти для навчання: результати зарубіжного та вітчизняного опитувань. Інформаційний бюлетень. 2023. №2. URL: https://lib.iitta.gov.ua/734991/ (дата звернення 12.09.2023).

3. Системи управління навчанням. UK.Myservername. URL: https://uk.myservername.com/15-best-learning-management-systems (дата звернення 12.09.2023).

4. Шепельський В.І., Краус К.М., Краус Н.М. Управління цифровим освітнім середовищем закладів освіти. European scientific journal of Economic and Financial innovation. 2023. №1(11). С. 30-45.

УДК 004.031 42

Т.Х. Фаталієв
tfataliyev@gmail.com
Інститут інформаційних технологій, м. Баку, Азербайджан

АКТУАЛЬНІ ПРОБЛЕМИ ДЕМОГРАФІЧНОГО АНАЛІЗУ В СЕРЕДОВИЩІ ІНТЕГРАЦІЇ Е-НАУКИ І Е-ОСВІТИ

Безперервний прогрес у сфері інформаційних технологій (IT), а також можливості, що надаються рішеннями Індустрії 4.0, відкривають широкі можливості для розвитку всіх сфер людської діяльності, включаючи науку та освіту. У цьому контексті відбувається безпосередній вплив на дослідні та освітні процеси, використання результатів у формі інновацій, а також на управління цими структурами. Індустрія 4.0 характеризується інтелектуальною автоматизацією, що поєднує фізичний та цифровий світи через Інтернет речей (IP) та кіберфізичні системи (КФС). Вона відкриває так само нові перспективи і для розвитку та інтеграції науки та освіти.

Широке застосування IP, КФS, штучного інтелекту (II), хмарних обчислень, аналізу великих даних та інших інтелектуальних технологій призвело до появи нових векторів науки та освіти, таких як «Наука 4.0» [1] та «Освіта 4.0» [2], при цьому в їх рамках відбувається в новій якості трансформація та інтеграція е-науки та е-освіти. Проведення демографічних досліджень на основі великих обсягів даних, зібраних у такому сформованому корпоративному середовищі, та вирішення існуючих проблем з підтримкою отриманих результатів відрізняється своєю актуальністю та створює широкі можливості для розвитку науки та освіти. Слід також зазначити, що ця область має широкий спектр напрямів досліджень для вивчення та використання проблем та можливостей застосування.

Загалом, інтеграційні процеси е-науки та е-освіти на платформі Індустрія 4.0 охоплюють широкий спектр різних напрямів діяльності та виявляються у найрізноманітніших формах. До основних їх можна віднести такі:

•інтеграція та розвиток мережевих інфраструктур під єдиною назвою "Національна науково-освітня мережа" (National research and education network - NREN) для надання передових IT-послуг дослідній та освітній спільноті;

•інтеграція, розвиток та управління інформаційних інфраструктур та ресурсів дата-центрів;

•організація спільного використання існуючих е-ресурсів, наприклад, е-бібліотек, та створення нових smart-ресурсів різного призначення;

•автоматизація процесів спільного використання з широким використанням IP, КФС, II, аналітики великих даних та інших передових технологій, обладнання та пристроїв нового покоління та розробка нових smart-систем різного призначення;

•організація та розширення спільної діяльності, участь науковців в освіті, а викладачів та студентів у наукових дослідженнях;

•якісна підтримка науково-освітнього процесу та управління;

• забезпечення комплексної безпеки (кібербезпеки та кіберстійкості);

•управління персоналом, підготовка кадрів нового типу, орієнтованих цифрову реальність викликів Індустрії 4.0 (smart вчений, smart педагог, smart вчитель, smart студент).

Зазначимо, що дослідження та практичні рішення, які реалізуються у зазначених напрямках, характеризуються великими обсягами даних, зібраних в е-ресурсах різного призначення. Таким чином, дата-центри, у тому числі інформаційні системи, бази даних, портали, е-ресурси та інші реєстри різного призначення за вказаними вище напрямками є джерелом демографічної інформації. Із застосуванням Аналітики великих даних відкриваються широкі можливості для отримання прихованих знань із цих даних, а також проведення демографічного аналізу для оцінки діяльністю та ефективного управління наукових та освітніх структур.

Слід зазначити, що є безліч робіт з різних аспектів досліджуваної проблеми. З огляду на обмеження обсягу представленої роботи розглянемо деякі з них. Відомо, що громадянська наука (ГН) відіграє важливу роль у розвитку процесу творення. Основною метою ГН є демократизація науки та ефективне вирішення глобальних проблем. Демографічні дослідження відіграють важливу роль у ефективній реалізації відбору учасників відповідно до цілей ГН, забезпечення інклюзивності та інших організаційних рішень. Показниками, що характеризують учасників, є демографічні (стаття, дата і місце народження, сімейний стан і т. д.), економічні (рід занять, сфера економіки та вид економічної діяльності, джерело засобів для існування тощо), загальне чи професійне освіта. (Рівень освіти, відвідуваність навчального закладу тощо), а також етнічні характеристики (національність, рідна мова, розмовна мова тощо). Підтверджено, що успіх досліджень у ГН залежить від демографічних характеристик учасників. Наприклад, демографічний аналіз проекту HiggsHunters на Великому адронному колайдері показав, що: а) 65% учасників були чоловіками, 74% мали як мінімум ступінь

бакалавра та більше половини мали ступінь магістра; б) Добре представлені професії включають вчителів, інженерів, консультантів, розробників та дослідників. 80% їх раніше брали участь у проектах ГН [3].

В [4] досліджено вплив демографічних характеристик на успішність. Демографічні дані використовувалися для вимірювання академічної успішності в очному (F2F) навчанні та дистанційному навчанні (DL). Студенти продемонстрували більш високу академічну успішність у DL, ніж у навчанні F2F. Було виявлено, що кількість слабких студентів у навчанні F2F різко скоротилася більш ніж на 11% у DL. Демографічні характеристики продемонстрували значний вплив на академічну успішність студентів та різниця у навчанні між F2F та DL склав не менше 7,4%.

У статті [4] розглянуто аналіз демографічних показників з урахуванням електронних даних. Дослідження базувалося на даних випускників, які навчалися там. Ці дані є гіпотетичними та експериментальними. Дані в регістрах кожного індивідууму інтегрувалися через персональний ідентифікаційний номер (ПІН) і з урахуванням отриманого набору даних проводився експеримент, а отримані результати за показниками візуалізувалися графічно. Завдяки цим аналізам можна отримати інформацію про соціальний статус населення, умови праці, рівень зайнятості, доходи і т.д.

В останні роки одним із найбільш актуальних та інтенсивно проведених наукових напрямів у галузі демографічних досліджень є формування єдиного об'єкта дослідження на основі інтеграції існуючих е-ресурсів. У цьому контексті принципи е-демографії, викладені в [6], можуть бути використані і в середовищі інтеграції е-науки та е-освіти. Е-демографія є ефективним інструментом проведення соціальних досліджень та моніторингу даних про населення і вважається одним із основних компонентів е-держави. Створення єдиної е-демографічної системи, що об'єднує існуючі е-ресурси для проведення демографічних досліджень та організації ефективного аналізу на основі зібраних даних, є дуже актуальним, але водночас складним завданням. Його реалізація потребує нормативної, фінансової, технічної та технологічної підтримки на глобальному рівні і тому може здійснюватись поетапно. Це можна зробити, наприклад, на мікро (проекти), мезо (регіональному), макро (глобальному) рівнях. При цьому сформована у сфері науки та освіти система е-демографії розглядається як підсистема «Національної системи е-демографії», що вимагає ефективної інтеграції реєстрів та систем, що охоплюють демографічні характеристики для оцінки, аналізу та ефективного прийняття рішень поточної демографічної ситуації. Зазначимо, що іншим із напрямів досліджень, що виділяється актуальністю, є підхід Social Credit System [7] до оцінки діяльності персоналу в досліджуваному інтеграційному середовищі. На основі інтегрованих демографічних даних у системі е-демографії може бути визначений соціальний кредит кожного персоналу у цій галузі.

Таким чином, середовище інтеграції е-науки та е-освіти дозволяє створити систему е-демографії як важливу платформу для проведення демографічного аналізу. У статті проведення демографічного аналізу та вирішення проблем із застосуванням передових технологій розглядається як актуальна проблема. Представлено концептуальні питання створення е-демографічної системи для онлайн-досліджень та моніторингу демографічних процесів у середовищі, що вивчається. Ця система повинна мати можливість інтегрувати існуючі онлайн ресурси на єдиній платформі. При реалізації системи можна здійснювати ефективну організацію та управління наукою та освітою на основі onlayn обробки реальних демографічних даних.

Список літератури

1. T.Kh. Fataliyev, Sh.A. Mehdiyev, The impact of Industry 4.0 on the formation of Science 4.0, Problems of Information Technology, vol. 13, №2, pp. 37-45, 2022.

2. L.I. González-Pérez, M.S. Ramírez-Montoya, "Components of Education 4.0 in 21st Century Skills Frameworks: Systematic Review", Sustainability, vol. 14, 3,1493, 2022.

3. A.J. Barr, A.C. Haas, C.W. Kalderon, Citizen scientist community engagement with the HiggsHunters project at the Large Hadron Collider, Research for All, vol. 2, №2, pp. 359-373, 2018.

4. A. El Refae Ghaleb, K. Abdoulaye, and E. Shorouq, The Impact of Demographic Characteristics on Academic Performance: Face-to-Face Learning Versus Distance Learning Implemented to Prevent the Spread of COVID-19, International Review of Research in Open and Distributed Learning, vol. 22, №1, pp. 91-110, 2021.

5. F.F. Yusifov, N.E. Akhundova, Analysis of Demographic Characteristics Based on E-Demography Data. Demography and Social Economy, №1, vol. 47, pp. 38-54, 2022.

6. R.M. Alguliyev, F.F. Yusifov, Architectural principles of building a national e-demographic system, Problems of Information Society, №1, pp. 3-17, 2021, [in Azerbaijani].

7. F.A.F.Ferreira, et al., A socio-technical approach to the evaluation of social credit applications, Operational Research Society, vol. 70, issue 10, pp. 1801–1816, 2019.

УДК 004.8

М.О. Макаренко[1], В.О. Тирлич[1]
makar44m@gmail.com, tyrlychvo@kntu.kr.ua
Центральноукраїнський національний технічний університет, м. Кропивницький

КЛАСИФІКАЦІЯ АСПЕКТІВ БЕЗПЕЧНОГО ВИКОРИСТАННЯ АВТОНОМНИХ РОБОТІВ

Звільнені від потреби прямого керівництва людиною, автономні роботи [1,2] які керуються штучним інтелектом стають все більш важливими у нашому сучасному світі. З їхньою допомогою вдається вирішувати завдання, що колись вважалися мрією наукової фантастики. Однак разом із великими можливостями, які вони принесли, дуже важливо забезпечити безпечне використання автономних роботів.

Розглянемо ключові технічні аспекти автономних роботів та складемо класифікацію що може приблизити нас до їх безпечного використання. Зосереджуючись на питаннях приватності, відповідальності, робочої сили, військового використання, впливу на суспільство, а також важливості встановлення адекватних нормативів і стандартів для забезпечення безпеки, прозорості та справедливості.

Автономні роботи [3-5] представляють собою складні технічні системи, що поєднують в собі різноманітні компоненти, від програмного забезпечення до фізичних сенсорів та складних механічних систем. Проведене дослідження дало змогу сформувати класифікацію комплексу різноманітних технічних аспектів що забезпечують безпеку використання автономних роботів (рис. 1).

1. **Системи моніторингу та сенсори**. Автономні роботи повинні мати надійні системи сенсорного моніторингу (наприклад, лідари, камери, радари), щоб виявляти перешкоди, інших учасників руху та зміни в навколишньому середовищі.
2. **Системи навігації**. Роботи повинні мати ефективні системи навігації, які дозволяють їм рухатися безпечно в різних умовах, включаючи визначення оптимального шляху та управління перешкодами.
3. **Алгоритми автономії**. Роботи повинні мати добре розроблені алгоритми для прийняття рішень, які враховують як найкращий спосіб досягнення мети, так і безпеку для навколишнього середовища та користувачів.
4. **Системи взаємодії з іншими автоматизованими системами**. Роботи повинні взаємодіяти з іншими системами та дотримуючись встановлених правил координації.
5. **Кіберзахист**. Забезпечення безпеки від потенційних кібератак і витоків даних є критичним, оскільки автономні роботи зазвичай підключені до мережі.
6. **Запобіжні аварійні заходи**. Роботи повинні мати системи аварійної зупинки і інші запобіжні заходи, які можуть зменшити ризик для користувачів у випадку непередбачених ситуацій.
7. **Оновлення та підтримка**. Постійне оновлення програмного забезпечення і обслуговування механічних компонентів є важливими для забезпечення безпеки та ефективності.
8. **Безпека даних та конфіденційність**. Забезпечення захисту даних зібраних автономними роботами, та дотримання стандартів конфіденційності є обов'язковими аспектами.
9. **Навчання та штучний інтелект**. Використання штучного інтелекту та неперервного навчання машин вимагає уваги до етичних та безпечних методів розробки та використання моделей.
10. **Відповідність стандартам та регулюванню**. Роботи повинні відповідати відповідним стандартам та законодавству щодо безпеки та використання.

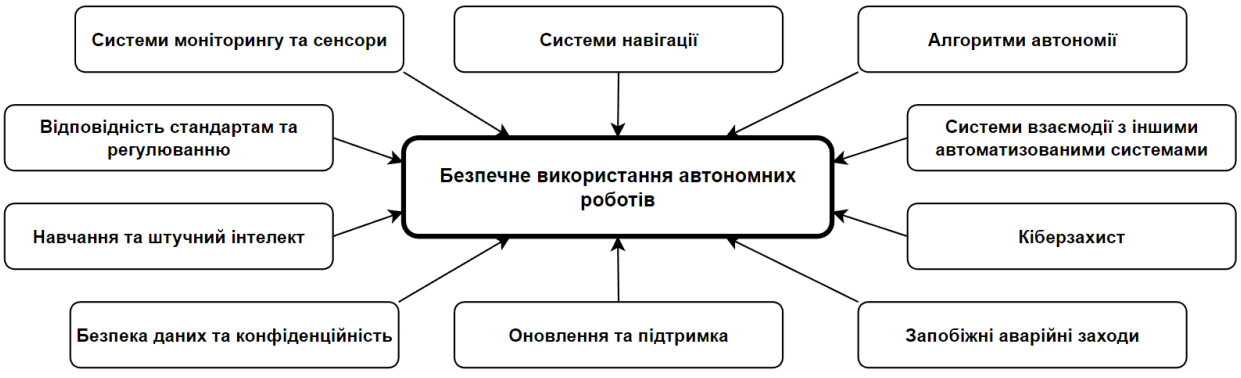


Рис. 1 Класифікація технічних аспектів безпечного використання автономних роботів

Розглянемо закони робототехніки Айзека Азімова, набору трьох фундаментальних принципів, призначених для забезпечення безпеки, етики взаємодії між роботами та людьми. Ці закони вперше були представлені Айзеком Азімовим у його науково-фантастичних романах і відтоді стали основою для обговорення етичних питань у робототехніці.

1. Перший закон стверджує, що робот не може завдати шкоди людині або, діючи беззастережно, допустити, щоб людина через свою недбалість зазнала шкоди. Іншими словами, роботи повинні бути програмовані та здатні діяти так, щоб захистити життя та безпеку людей навколо них.

Наприклад, цей закон може вимагати від робота уникати дій, які можуть призвести до травм або пошкоджень для людей, а також допомагати у виконанні безпечних операцій.

2. Другий закон стверджує, що робот повинен підкорятися велінням людини, за винятком тих випадків, коли ці веління суперечать першому закону. Це означає, що роботи повинні служити людям і виконувати їхні веління, коли це безпечно і не суперечить етиці та закону.

Наприклад, робот-помічник у побуті повинен слухати команди власника, але відмовити виконувати нелегальні дії або дії, які можуть призвести до шкоди іншим людям.

3. Третій закон стверджує, що робот повинен забезпечувати свою власну безпеку та захищати своє існування, доки це не суперечить першим двом законам. Це означає, що роботи повинні дбати про свою безпеку та функціонування, але не за рахунок шкоди людям.

Наприклад, якщо робот виявляє, що його функціонування порушено або існує загроза його власній безпеці, він може вжити заходів для забезпечення власної безпеки, але при цьому повинен уникати дій, які можуть завдати шкоди людині.

Закони робототехніки Азімова визначають основні етичні стандарти для роботів, роблячи акцент на безпеці та взаємодії з людьми. Вони стали важливими в контексті розвитку робототехніки і роблять акцент на важливості розуміння та дотримання етичних норм у сучасній робототехніці.

Використання автономних роботів або дронів в військових цілях повністю заперечує першому закону робототехніки, так як їхнє першорядне завдання – ураження ворожих цілей. Використання автономних дронів в військових цілях ідея не нова. Наприклад, у 2020 році дрон турецького виробництва, смертоносний ударний безпілотник, розроблений для асиметричної війни та антитерористичних операцій Kargu-2. Автономний робот працював у «високоефективному» автономному режимі, який не вимагає контролю людини. У доповіді групи експертів Ради Безпеки ООН йдеться: «Смертоносні автономні системи зброї запрограмовані для ураження цілей без необхідності передачі даних між оператором і боєприпасами. Це справжня функція «вистрілив, забув, знайшов».

Хоча поява автономних військових безпілотників може кардинально змінити характер війни, але загальною метою використання автономних роботів та дронів у військових цілях повинно бути забезпечення безпеки, зменшення ризиків для життя і мінімізація негативного впливу на мирних цивільних. Вирішення етичних, правових та безпекових аспектів важливо для створення рамок, які дозволять використовувати ці технології відповідально та відповідно до міжнародних стандартів.

Підсумовуючи, автономні роботи відкривають безмежні можливості для сучасного світу, ефективно вирішуючи завдання, які раніше були неможливими. Проте, разом із цими можливостями приходить велика відповідальність забезпечити безпечне використання цих роботів. У цій роботі були розглянуті ключові технічні аспекти, пов'язані з безпечним використанням автономних роботів, дотримуючись яких, ми зможемо забезпечити безпечне майбутнє.

Список літератури

1. Towards Autonomous Robot Evolution / Agoston E. Eiben та ін. Software Engineering for Robotics. 2020. С. 29–51. URL: https://doi.org/10.1007/978-3-030-66494-7_2 (дата звернення: 01.10.2023).

2. Gündoğar A., Niauronis S. Overview of Potential Risks of Artificial General Intelligence Robots. Applied Scientific Research. 2023. URL: https://doi.org/10.56131/tmt.2023.2.1.93 (дата звернення: 1.10.2023).

3. Barfield J. K. Discrimination against robots: Discussing the ethics of social interactions and who is harmed. Journal of Behavioral Robotics. 2023. Т. 14, № 1. URL: https://doi.org/10.1515/pjbr-2022-0113 (дата звернення: 01.10.2023).

4. Recent developments in terrain identification, classification, parameter estimation for the navigation of autonomous robots / M. G. H. Nampoothiri та ін. SN Applied Sciences. 2021. Т. 3, № 4. URL: https://doi.org/10.1007/s42452-021-04453-3 (дата звернення: 01.10.2023).

5. Kasap, M., Yılmaz, M., Çinar, E. et al. Unsupervised dissimilarity-based fault detection method for autonomous mobile robots. Auton Robot (2023). https://doi.org/10.1007/s10514-023-10144-2 (дата звернення: 01.10.2023).

УДК 629.7.02

Р.М. Минайленко, Л.І. Поліщук, О.К. Конопліцька-Слободенюк
aron70@ukr.net
Центральноукраїнський національний технічний університет, м. Кропивницький

ДИСТАНЦІЙНЕ НАВЧАННЯ ЯК ОДНА З ФОРМ ОРГАНІЗАЦІЇ НАВЧАЛЬНОГО ПРОЦЕСУ

На сьогоднішній день незаперечним є те, що основний капітал, яким володіє організація це кваліфіковані фахівці, які володіють певними знаннями, навичками і технологіями, тобто людський капітал.

Що стосується системності, то організація, що поставила за мету бути першою, успішною, швидко реагувати на зміни оточуючого середовища, приймати випереджаючі рішення, впроваджувати нові розробки та технології, має навчати персонал. Розвиток та навчання персоналу – це невід'ємна та важлива інвестиція, яка при грамотному та системному підході дасть якісні результати. Саме навчання є тим комплексом заходів, що дозволить сформувати ефективний та постійний бізнес-процес передачі досвіду, знань, розвитку навичок у співробітників організації.

Залежно від способу комунікації викладачів та учнів виділяють наступні методи дистанційного навчання:

– Метод навчання за допомогою взаємодії того, хто навчається, консультується або взаємодіє з освітніми ресурсами за мінімальної участівикладачів, репетиторів, консультантів, наукових та технічних керівників (самонавчання). Для здійснення цього методу викладачами, репетиторами створюються та підбираються різні освітні ресурси: друковані, аудіо- та відеоматеріали, а також навчальні посібники, що доставляють телекомунікаційними мережами (інтерактивні бази даних, електронні видання та комп'ютерні навчальні системи).

– Метод індивідуалізованого викладання та навчання, для якого характерні взаємини одного учня, консультованого студента чи школяра, клієнта, який потребує науково-технічних послуг, здобувача наукового ступеня з одним викладачем, репетитором, консультантом або науковим та технічним керівником (навчання «один до одного»)). Цей метод може реалізуватися в дистанційному навчанні переважно за допомогою таких технологій, як телефон, голосова пошта, факс, електронна пошта, та ін.

– Метод, в основі якого лежить виклад навчального матеріалу викладачем, при цьому учні не відіграють активної ролі в комунікації (навчання «один до багатьох»). Даний метод використовується педагогом, репетитором, консультантом, коли навчається і консультується ціла група, вони приблизно однаково підготовлені і для всіх однаковий кінцевий результат. Наприклад, це відбувається при підготовці школярів репетитором до екзаменів, або при консультуванні студентів з різних дисциплін. Цей метод, властивий традиційної освітньої системі, набуває нового розвитку з урахуванням сучасних інформаційних технологій. Так, лекції, записані на аудіо або відео, що читаються по радіо або телебаченню, доповнюються в сучасному дистанційному навчанні так званими електронними лекціями, що розповсюджуються по комп'ютерних мережах за допомогою систем дошок оголошень. Електронна лекція, яку готують та підбирають викладачі, репетитори, консультанти може являти собою добірку статей або витягів із них, а також навчальних матеріалів, які готують учнів до майбутніх дискусій.

– Метод, для якого характерна активна взаємодія між усіма учасниками навчального процесу (навчання «багато хто до багатьох»). Цей метод орієнтований на групову роботу студентів та становить найбільший інтерес для дистанційного навчання. Він передбачає широке використання дослідницьких та проблемних способів навчання. Роль викладача при такому навчанні зводиться до того, що він ставить тему для студентів, школярів або для претендентів на наукові ступені (ставить навчальне завдання), а далі він повинен створити і підтримувати таке сприятливе середовище спілкування і психологічний клімат, при яких учні могли б працювати в співробітництво. Викладач відповідає за координацію, управління ходом дискусії, і навіть за підготовку матеріалів, розробку плану роботи, обговорюваних питань, і тем.

– Метод проєктів передбачає комплексний процес навчання, що дозволяє учню проявити самостійність у плануванні, організації та контролі своєї навчально-пізнавальної діяльності, результатом якої є створення будь-якого продукту чи явища. У основі методу проєктів лежить розвиток пізнавальних, творчих інтересів учнів, умінь самостійно формувати знання.

– Метод проблемного навчання заснований на розгляді складних пізнавальних завдань, вирішення яких становить суттєвий практичний чи теоретичний інтерес. У процесі проблемного навчання увагу

учнів фокусується на важливих проблемах, вони стимулюють пізнавальнуактивність, сприяють розвитку умінь та навичок у вирішенні цих проблем. Роль викладача зводиться до спостереження та підтримки, але не більше Дослідницький метод навчання характерний наявністю чітко поставлених актуальних та значущих для учасників цілей, продуманої та обґрунтованої структури, широкого використання арсеналу методів дослідження, використання наукових методів обробки та оформлення результатів.

Останні кілька років в освітній сфері стали активно застосовуватися онлайн-семінари або вебінари. Вебінар – це форма веб-конференції, яка включає проведення онлайн-нарад, демонстрацію презентацій через мережу Інтернет в режимі реального часу та інші інтерактивні можливості. Під час вебінару кожен учасник використовує свій персональний комп'ютер, зв'язок між учасниками підтримується через Інтернет за допомогою спеціалізованого програмного забезпечення, встановленого на комп'ютері кожного учасника, або через веб-додаток. Останній спосіб проведення вебінару дуже зручний, тому що не вимагає розгортання на робочих станціях учасників конференції спеціалізованого програмного забезпечення .

Вебінари можуть використовувати різні інтерактивні взаємодії, включати сеанси голосувань і опитувань, що забезпечує повну взаємодію між аудиторією і викладачем. Визначення «інтерактивна взаємодія» часто використовується у спеціальній літературі. Інтерактивна взаємодія – це спілкування студента з іншими учасниками вебінару через програмний комплекс. За більш просунутих можливостях ведення спілкування реалізується можливість вибору варіантів змісту навчального контенту та режиму навчання. Чим більше можливостей у програмного комплексу, чим активніше студент бере участь у процесі навчання та спілкуванні з іншими учасниками вебінару, тим вище інтерактивність. У загальному сенсі інтерактивна взаємодія передбачає спілкування будь-яких учасників, залучених до навчального процесу, один з одним із використання доступних їм можливостей. При проведенні вебінарів дуже часто застосовується технологія «електронна дошка». Насамперед цей інтерактивний інструмент призначений для коментарів, він дозволяє викладачеві та слухачам залишати позначки або коментувати пункти слайдової презентації.

Завдяки використанню глобальної мережі Інтернет, викладач та студенти вебінару можуть перебувати на величезних відстанях один від одного, та брати участь в одному освітньому процесі. Без використання сучасних технологій зібрати аудиторію разом було б досить складно або взагалі неможливо. Не слід розуміти вебінар як односторонню трансляцію. Ведучий, як правило, надає право учасникам вебінару поставити запитання, які їх цікавлять, або висловити свою точку зору з обговорюваної теми. Завдяки використанню веб-камер співрозмовники можуть бачити один одного, що також позитивно впливає на освітній процес. Під час проведення занять часто застосовуються засоби віддаленого контролю комп'ютерів, за допомогою яких викладач може безпосередньо допомогти студенти, якщо у останнього виникли якісь труднощі при виконанні практичного завдання. Такі засоби як JoinMe та TeamViewer дозволяють ефективно керувати програмами на стороні віддаленого комп'ютера.

Зазвичай, форма дистанційної освіти передбачає самостійне виконання студентами практичних завдань. Для того, щоб централізовано зберігати виконані завдання, навчальні матеріали та інші документи, необхідні для навчального процесу, часто використовуються хмарні сховища даних. Хмарне сховище даних – це вид онлайн-сховища, в якому інформація та дані користувачів зберігаються на кількох розподілених у мережі Інтернет серверах, що надаються в користування клієнтам. Використання хмарного сховища найчастіше набагато зручніше, ніж використання власних виділених серверів. З погляду користувача, хмарне сховище представляє їм цілісний віртуальний сервер. Слід зазначити, що більшість хмарних сховищ надають певний обсяг свого дискового простору для безкоштовного використання. Декілька гігабайт зазвичай вистачає для освітніх потреб. Додатковим (а в деяких випадках навіть основним) засобом комунікації між учасниками освітнього вебінару можуть бути VoIP-програми. Часто, при дистанційному навчанні у вищих навчальних закладах від студентів не потрібно постійно перебувати в аудиторії. У більшості робочих програм вищих навчальних закладів, що реалізують дистанційне навчання, все ж таки проходять очні заняття.

Ці заняття, як правило, не обов'язкові для відвідування, однак, часто бувають корисні для вироблення у студентів різноманітних практичних навичок. Велика кількість великих компаній підтримують власні центри дистанційного навчання, щоб уніфікувати та покращити якість підготовки власних співробітників. У внутрішньокорпоративній сфері освіти тапідвищення кваліфікації працівників застосовуються спеціальні системидистанційного навчання, які забезпечують найефективнішу побудову освітніх програм. До таких систем відносяться WebTutor, Competentum, Moodle та інші.

Великі ІТ-корпорації створюють великі навчальні портали для підготовки співробітників або зовнішніх покупців своїх продуктів. При цьому деякі курси надаються безкоштовно або входять до комплекту програмного забезпечення.

Тобто, можна сказати, що у сфері інформаційних технологій дистанційні методи навчання стали поширеними повсюдно та міцно зайняли свою нішу

УДК 519.1

В.І. Петренюк
petrenjukvi@i.ua
Центральноукраїнський національний технічний університет, м. Кропивницький

ТЕНДЕНЦІЇ ЗАСТОСУВАННЯ ГРАФІВ

Математичний метод φ-перетворення розглядає великі складних структури як зв'язний набір малих і відносно простіших підструктур. Для цього вони можуть мати деякі спільні частини, які можна ідентифікувати та ототожнювати (об'єднати) під час побудови або реконструкції цілої конструкції з кінцевої кількості підструктур. Продемонструвати можливості цього методу для побудови як множини всіх неізоморфних 3-мінімальних плоских простих графів, у яких множина всіх вершин розташована на границях трьох 2-клітин, і побудови множини всіх неізоморфних 3-мінімальних площинних простих графів, так і множини 2-мінімальних проективних площинних графів, в яких фіксована множина точок розташована на двох границях 2-кліток або псевдоклітки.

Для аналізу складної системи, синтезованої з досліджуваних більш простих підструктур у загальному вигляді та їх застосування в інформатиці пропонуємо теоретико-графовий підхід як спосіб машинного мислення або оперування штучними образами-структурами. Відомі математичні методи, за допомогою яких великі системи як структури розглядаються через набір малих і простих підструктур, які можуть мати деякі спільні частини, які можна ідентифікувати при побудові або реконструкції цілої структури з кінцевого числа підструктур. Таким є φ-метод створення моделі графа, отриманої у вигляді пари скінченних множин: множин вершин і множин ребер для визначення зв'язків між структурою вершин як об'єктів. Прикладом цього є трансформація основних задач системного програмування в задачі теорії графів з математичним забезпеченням алгоритмів. Основну ідею методу φ-перетворення, засновником якого є М.П. Хоменко [1] можна інтерпретувати як успадкування певної властивості підструктур у всій структурі в залежності від властивостей з'єднання (ідентифікація та ототодження заданих частин пари підструктур).

Системний аналіз заданих властивості моделі складної системи, представленої у вигляді графової моделі, можна досліджувати за допомогою простого графа G з фіксованим набором точок, вбудованих у поверхню, на якій будуть розташовані ребра графіка, де S - евклідова площина, або проективна площина. Наприклад, у моделі G такою властивістю зовнішня планарність множини всіх вершин, що знаходяться на межі однієї комірки, є наявність підграфів, гомеоморфних K_4 або $K_{2,3}$. Це буде корисним у систематичному аналізі обох графових моделей та їх топологічного аспекту, який полягатиме у виявленні спільних властивості на ребрах і вершинах складеної з них великої графової моделі.

Так звані циліндричні графи [2], були досліджені з точки зору їх зовнішньої планарності та отримано повний список із 38 нециліндричних графів як заборонених підграфів чи частин вхідного графа. Алгоритм побудови і список 3-мінімальних графів, а саме їх характеристика методом φ-перетворення графів [3], список 32 3-мінімальних графів [4].

Прикладом можливого застосування може служити набір задач розміщення точок або автоматичний контроль з подальшим доступом до її точок. Якщо ми говоримо про поверхню як про майже нескінченний набір значень функції кількох змінних на заданій скінченній підмножині як про набір вершин, зв'язок яких між парами елементів у вигляді набору ребер, ми маємо майже вбудова ний граф у поверхню . Якщо задати ребра як майже нескінченну підмножину точок, то, за умови відсутності перетину ребер у внутрішніх точках ребер, ми матимемо майже мінімальне вкладення графа в поверхню. Якщо поверхня є сферою або певною мірою нагадує площину без отворів, то використо вуйте наступний список 3-мінімальних графів, щоб розмістити на межах трьох клітинок усі вершини графа. Якщо поверхня є сферою з отвором або певною мірою нагадує площину з круглою діркою , прохід через який можливий як стрибок з однієї точки границі дірки в діаметрально протилежну точку цієї границі, тоді ми використовуємо наступний список 2-мінімальних проективних планарних графів для розміщення на границях двох комірок заданого набору вершин графа. Більше прикладів наведено в [5].

Список літератури

1. M.P. Khomenko. φ -Transformation of Graphs. Institute of Mathematics, Kyiv, 1973.
2. D. Archdeacon, C.P. Bonnington, N. Dean, N.Hartsfield. Obstructions Sets for Outer-Cylindrical Graphs. Journal of Graph Theory, v 38, i. 1, 2001, pp 42–64.
3. V. Petrenjuk. Characterization of the 3-minimal Planar Graph. Collection of the proceedings of a seminar of discrete mathematics\ and applications. Moscow, MGU 1993, p.217.
4. V. Petrenjuk. List of 3-minimal Planar Graphs. Preprint DNTB 31.10.86 #2450-86. 7p.
5. V. Petrenjuk. About Transformation graphs as a tool for investigation. Proceedings of the 4-th International Conference on Computational Linguistics and Intelligent Systems (COLINS 2020). Volume I: Lviv, Ukraine, April 23-24, 2020, 1309-1319. URL: http://ceur-ws.org/Vol-2604/.

УДК 378:004

А.С. Коваленко[1], О.В. Коваленко[1], М.О. Кобець[1]
annasun911@gmail.com, dr.kovalenkoov@gmail.com, nicko9298@gmail.com
[1]*Центральноукраїнський національний технічний університет, м. Кропивницький*

СУЧАСНІ ПІДХОДИ ВИКОРИСТАННЯ МЕТОДУ ZETTELKASTEN ТА СИСТЕМИ OBSIDIAN У НАВЧАЛЬНИХ ДИСЦИПЛІНАХ ОСВІТНЬО-ПРОФЕСІЙНИХ ПРОГРАМ ЗВО ІТ–СПРЯМОВАНОСТІ

Сучасний світ вимагає від фахівців високого рівня гнучкості, здатності швидко адаптуватися до нових умов та використовувати інноваційні підходи в своїй професійній діяльності. Це особливо актуально для галузі інформаційних технологій (далі ІТ), яка стрімко розвивається та визначає темпи сучасного прогресу. Важливим аспектом підготовки фахівців у закладах вищої освіти (далі ЗВО) ІТ-спрямованості є впровадження інноваційних методів навчання та запам'ятовування інформації, які б дозволили студентам не лише засвоювати необхідні знання, але й розвивати навички самостійного пошуку та аналізу інформації, критичного мислення та творчого підходу до вирішення задач та заміни ведення класичного конспекту лекцій навчальних дисциплін освітньо-професійних програм.

Одним із сучасних підходів до організації навчального процесу є використання методу Zettelkasten на основі системи Obsidian [1,2].

Розглянемо сучасні підходи використання методу Zettelkasten та системи Obsidian на прикладі підготовки фахівців ІТ–спрямованості, можливості та переваги використання цих інструментів в навчальному процесі, а також досвід їх застосування на практиці.

Метод Zettelkasten [3,4], розроблений німецьким соціологом Нікласом Луманном, є системою організації знань та ідей за допомогою створення мережі взаємопов'язаних заміток. Концепція методу Zettelkasten полягає в створенні заміток, які містять основні ідеї та концепції, та їх подальшому взаємопов'язуванні. Кожна замітка має унікальний ідентифікатор та може бути пов'язана з іншими замітками за допомогою посилань.

В контексті підготовки фахівців ІТ-спрямованості, метод Zettelkasten може бути особливо корисним, оскільки він дозволяє студентам структурувати великі обсяги інформації, які є характерними для ІТ-галузі [5].

Студенти можуть створювати замітки з різних підходів програмування, патернів, алгоритмів, різноманітних комп'ютерних систем та інших дисциплін освітньо-професійних програм, а також взаємопов'язувати їх, щоб створити цілісну картину знань предметної області.

Це дозволяє не лише краще засвоювати матеріал та використовувати його у подальшому, але й розвивати навички аналітичного мислення та вирішення задач, які є ключовими для успішної кар'єри в ІТ-галузі.

Система Obsidian, в свою чергу, є інструментом для створення та управління базою знань, яка дозволяє візуалізувати зв'язки між інформацією та ідеями. Що у зв'язці дозволяє використати концепцію «Другий мозок». Дозволяє ефективно планувати навчальні проекти, організовувати базу знань фахівця, проводити інтеграцію з іншими інструментами GitHub, Trello, Jira, Slack та ін. Obsidian має активне спільнотне середовище, яке розробляє сторонні модулі, що додають нові функції та можливості до основної програми - візуалізація даних, розширене форматування, сортування, звітування тощо.

Ці інструменти можуть бути ефективно використані в навчальних дисциплінах освітньо-професійних програм закладах вищої освіти ІТ-спрямованості для покращення якості освіти та підготовки висококваліфікованих фахівців.

Актуальність ведення нотаток методом Zettelkasten в сучасному освітньому процесі можна розглядати як можливу альтернативу чи навіть повноцінну заміну традиційного конспекту лекцій. Цей метод дозволяє студентам не лише фіксувати основні тези лекцій, але й створювати власну мережу знань, в якій ідеї та концепції взаємопов'язані та структуровані таким чином, що сприяє кращому засвоєнню матеріалу та розвитку критичного мислення, приклад сформованої бази знань представлено у вигляді графа на рис.1.

Важливість використання методу Zettelkasten в сучасній освіті також обумовлена актуалізацією нових освітніх парадигм, таких як компетентнісний підхід, який передбачає активну участь студентів у навчальному процесі та розвиток їхніх навичок самостійного пошуку та аналізу інформації.

Метод Zettelkasten дозволяє студентам створювати власні бази знань, які відображають їхнє розуміння предмета та сприяють формуванню компетенцій, необхідних для успішної професійної діяльності. Крім того, форма дистанційного навчання, яка стала особливо актуальною в останні роки, вимагає від студентів більшої самостійності та відповідальності за власне навчання.

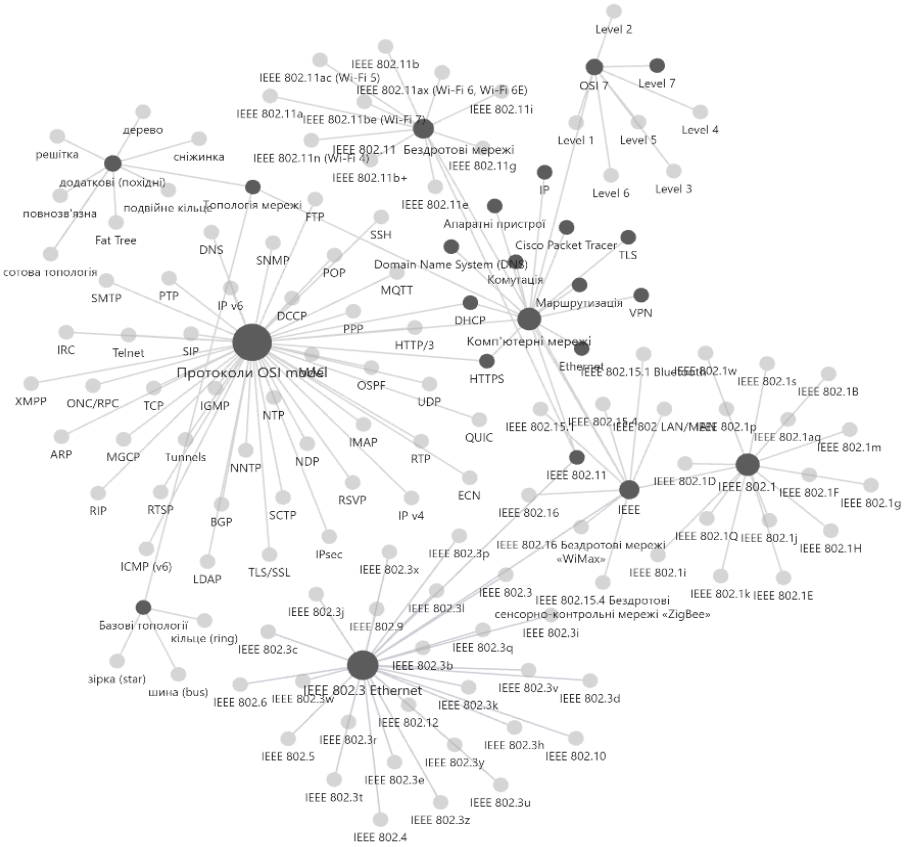


Рис. 1. Нотатки дисципліни Комп'ютерні мережі сформовані за допомогою системи Obsidian

Метод Zettelkasten може стати ефективним інструментом для організації навчального матеріалу в умовах дистанційного навчання, оскільки дозволяє студентам створювати структуровані бази знань, які можуть бути легко доступні та використані спільно з іншими навчальними системами (як приклад система Moodle) для підготовки до занять, іспитів, єдиного державного кваліфікаційного іспиту (ЄДКІ), курсових чи випускних кваліфікаційних робот у закладах вищої освіти.

Як висновок можна сказати що в контексті сучасних викликів та нових освітніх парадигм, метод Zettelkasten та система Obsidian можуть стати ефективними інструментами у навчальних дисциплінах освітньо-професійних програм ЗВО ІТ–спрямованості. Використання методу вимагає від студентів активної участі в навчальному процесі, готовності до самостійного пошуку, аналізу інформації та використання на парах електронних пристроїв для ведення нотаток. Тому, для успішного впровадження цих інструментів в освітній процес, необхідно також розвивати мотивацію та самостійність студентів наприклад, додатковими заохоченнями використання Obsidian під час очного чи дистанційного навчання.

Список літератури

1. Basu A. What is zettelkasten and how to write "papers" using zettelkasten?. Qeios. 2020. URL: https://doi.org/10.32388/zm0v6i (дата звернення: 1.10.2023).

2. Vorschau Daniela K. Helbig. Life without Toothache: Hans Blumenberg's Zettelkasten and History of Science as Theoretical Attitude.*Journal of the History of Ideas, University of Pennsylvania Press*. 2019. Т. 80, № 1. С. 91–112. URL: https://pure.mpg.de/rest/items/item_3026314_8/component/file_3327044/content. (дата звернення: 1.10.2023).

3. Ratcliffe J. Using a zettelkasten to manage your ideas. Journal of Aesthetic Nursing. 2021. Т. 10, № 1. С. 37–39. URL: https://doi.org/10.12968/joan.2021.10.1.37 (дата звернення: 1.10.2023).

4. de Aragão Fraga F. P. On Automatic Generation of Knowledge Connections. Rio de Janeiro, 2023. 162 с. URL: https://www.maxwell.vrac.puc-rio.br/61191/61191.PDF (дата звернення: 01.10.2023).

5. Matysek A., Tomaszczyk J. Digital wisdom in research work. Zagadnienia Informacji Naukowej - Studia Informacyjne. 2020. Т. 58, № 2A(116A). С. 98–113. URL: https://doi.org/10.36702/zin.705 (дата звернення: 1.10.2023).

УДК 004.415.538

К.О. Кохан
kiril.kohan@gmail.com
науковий керівник Ткаченко О.М. , к.т.н, доцент
Національний університет біоресурсів і природокористування. м. Київ

ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ ВИБОРУ ОПТИМАЛЬНИХ КОНФІГУРАЦІЙ АВТОМАТИЗОВАНОГО ТЕСТУВАННЯ БАГАТОКОМПОНЕНТНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

Автоматизоване тестування багатокомпонентних інформаційних систем — це частина процесу тестування на етапі контролю якості в процесі розробки програмного забезпечення. Воно використовує програмні засоби для виконання тестів, перевірки результатів, також здатне виконувати трудомістке низькорівневе регресійне тестування, що скорочує час та дає чіткі звіти[1].
Незважаючи на широкий спектр програм та технологій для автоматизації тестування, кожний конкретний проект має підібрати для себе найбільш доцільні та вигідну методику тестування, що максимально покриє всі поставлені задачі.Технологія має бути гнучка, легка в використанні та потужна, за її вибір відповідають найбільш кваліфіковані люди, архітектори в тестуванні, бо вибір правильних елементів програми для визначає успіх тестування в принципі.

Автоматизоване тестування передбачає використання інструменту автоматизації для виконання набору тестів. У той час як ручне тестування виконується людиною, що сидить перед комп'ютером, ретельно виконує всі етапи тестування. Автоматизація ПЗ також може вводити тестові дані в систему, яку тестують, порівнювати очікувані та фактичні результати та генерувати детальні звіти про тестування. Однак воно вимагає значного вкладання коштів та ресурсів. Цикл розробки вимагає багаторазового виконання одного й того ж набору тестів під час послідовності розробки. Використовуючи автоматизацію, можна написати набір тестів і відтворювати його повторно у разі необхідності. Як тільки набір тестів автоматизовано, втручання людини не потрібне. Також це допомагає поліпшити ROI (коефіцієнт окупності інвестицій). Метою автоматизації є скорочення кількості тестів, які потрібно запускати вручну, а не усунення ручного тестування в цілому.

Одним з головних завдань впровадження автоматизації в процес тестування є підвищення ефективності, збільшення охоплення та прискорення тестування за умов постійного повтору тестових сценаріїв. Автотест можна запускати регулярно, в робочий і неробочий час. На виконання ручних тестів, знаходження і реєстрацію помилок у тестувальника в середньому йде близько дня. При автоматизації цей процес займе хвилини, а також дозволить знаходити помилки в коді на момент його внесення в репозиторій вихідного коду.

Автоматизація тестування існує декількох видів: тестування коду, графічного інтерфейсу користувача (GUI). Найпопулярнішою формою є GUI тестування, це пояснюється двома факторами: по перше, додаток тестується тим же способом, яким його буде використовувати людина, по-друге, можна тестувати, не маючи доступу до вихідного коду. Види тестування у вигляді піраміди тестування представлені на Рис. 1.

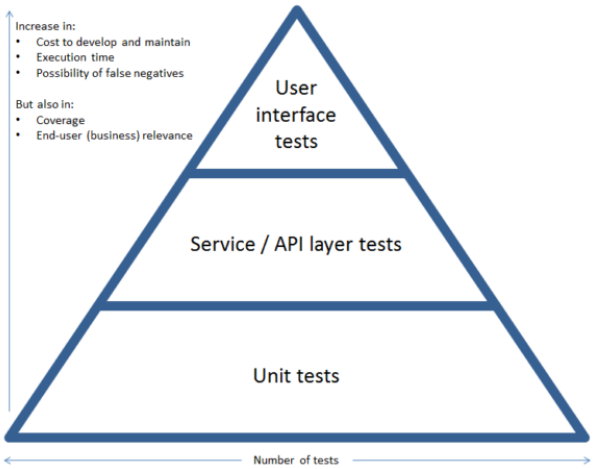


Рис. 1. Піраміда тестування

Однією з головних проблем автоматизованого тестування є його трудомісткість. Попри те, що автоматизоване тестування дозволяє усунути частину рутинних операцій і прискорити виконання

тестів[2], великі ресурси можуть витрачатися на оновлення самих тестів. Наприклад, при рефакторингу часто буває необхідно оновити і модульні тести, і зміна коду тестів може зайняти стільки ж часу, скільки і зміна основного коду.

Як зрозуміти, що настав час автоматизувати тестування? Чи у всіх випадках рентабельність інвестицій в автоматизацію буде виправдана? Якщо проект великий, зростає, в його складі кілька підсистем і «ручні» тест-кейси вже налічують кілька сотень, автоматизація дозволить підвищити продуктивність тестувальника, який не буде витрачати тижні на перевірку тест-кейсів. Не тільки великий проект, але і велика команда програмістів потребує автоматизації тестування, щоб прискорити виявлення багів при взаємодії різних модулів коду та оперативно їх виправити. Автоматизація процесів тестування буде особливо актуальною, якщо продукт відповідає таким критеріям:

Наразі такі інформаційні системи, як веб-додатки[3] є дуже актуальними, вони використовуються в процесі колективної взаємодії, обслуговуванни масштабних процесів, організації колективних заходів, організації навчального процесу та ін. Перевагою такого роду систем є можливість опрацювання інформації великою кількістю людей. А це в свою чергу призводить до підвищення якості обробки інформації.

Тестування — необхідний етап створення продукту. Автоматизація дозволяє полегшити й прискорити цей процес. Але не всі види тестування потребують автоматизації, а тільки ті, які засновані на діях, що повторюються.

Існують такі типи тестування, які рекомендується автоматизувати.Тестування продуктивності (навантажувальне, стресове, об'ємне) проводиться з метою перевірки працездатності продукту в умовах, максимально наближених до реальних, з очікуваними навантаженнями та обсягом даних. Наприклад, потрібно перевірити роботу сайту при великому трафіку користувачів, який може вплинути на швидкість завантаження і роботу окремих модулів. ТП автоматизується в першу чергу, бо мануальні тестувальники не можуть штучно створити умови, які будуть імітувати реальні ситуації для виявлення дефектів коду. Регресивне тестування на коректність функціональності застосовується на сервісах, які регулярно змінюються (нові білди, нові версії ПЗ). Завдання РТ — переконатися, що нові зміни, внесені в код, не порушили роботу ПЗ. Автоматизація РТ звільняє тестувальника від частого ручного запуску одних і тих самих тест-кейсів перед кожним новим оновленням додатка або ПЗ. А в разі, коли потрібне виконання однакових дій, але з різними даними, автоматизація дозволяє використовувати єдину базу, з якої скрипти автоматично будуть обирати інформацію і проводити тести. Конфігураційне тестування застосовується для перевірки працездатності продукту на різних операційних системах і в умовах змін в конфігураціях. При розробці мобільних додатків КТ дозволяє контролювати роботу продукту на різних мобільних пристроях з урахуванням розмірів і роздільної здатності екрану, операційних систем, їх версій і т.п. Автоматизація КТ не вимагає багато часу на впровадження, але при цьому значно прискорює процес тестування шляхом паралельного запуску тестів з різним поєднанням конфігурацій (браузер — операційна система — система управління базами даних — сервер). Інтеграційне тестування застосовується для групових тестів, які об'єднують програмні модулі, створені декількома програмістами. Наприклад, потрібно перевірити як взаємодіє модуль кошика і платіжний модуль в інтернет-магазині. Крім цього, ІТ перевіряє роботу системи в поєднанні з позапроцесними залежностями (керованими й некерованими). Результат автоматизації інтеграційних тестів — надійний захист від збоїв і відсутність необхідності переробки коду.

Метою моєї роботи є дослідження інформаційної технології вибору оптимальних конфігурацій автоматизованого тестування багатокомпонентних інформаційних систем. В процесі роботи системи користувач системи: вводить текст кейси для тестування в спеціальній файл, а система запускає тестування веб додатку. Після цього система генерує звіти щоб надати користувачу статистику по проходженню тестів. Даний підхід дозволяє бути впевненим у тестуванні поведінки застосунка та його візуального вигляду.

Список літератури

1. Тестування програмного забезпечення. Базовий курс / С. С. Куликов. — Мінськ: Чотири чверті, 2017. — 312 с. ISBN 978-985-581-125-2

2. Тестування програмного забезпечення. Навчальний посібник / Авраменко А.С., Авраменко В.С., Косенюк Г.В. ; – Черкаси: ЧНУ імені Богдана Хмельницького, 2017. – 284 с. ISBN 978-985-581-125-2.

3. Чим веб-додаток відрізняється від сайту? [Електронний ресурс]. – Точка доступу: URL: http://www.sunsoft.com.ua/uk/Article/38 – Чим веб-додаток відрізняється від сайту?

УДК 37:004

А. В. Мірочник
miralinaval@gmail.com
Науковий керівник: Ю.В. Білявська
доцент кафедри менеджменту, кандидат економічних наук, доцент
y.biliavska@knute.edu.ua
Державний торговельно-економічний університет, м. Київ

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ОСВІТІ

Використання інформаційних технологій у навчально виховному процесі допомагають розвинути нинішню освіту. Інформатизація освіти в нашій країні прогресує,і для цього необхідно впроваджувати науково обґрунтовані засоби та методи інформаційних технологій.

Різноманітні мобільні додатки та онлайн-платформи стали невід'ємною частиною навчального процесу і великою перевагою для учнів, студентів та вчителів. Вони полегшують доступ до навчального матеріалу, роблять навчання більш інтерактивним та цікавим, а також допомагають студентам ефективніше використовувати свій час самонавчання та сприяють розвитку логічного мислення у дітей, оскільки вони аналізують свої дії та навчаються критично їх осмислювати, виявляти можливі помилки і шукати їх рішення. Ось деякі з ключових ролей мобільних додатків та онлайн-платформ у навчальному процесі:

1. Доступ до навчального матеріалу: Мобільні додатки та платформи дозволяють зручно отримувати доступ до навчальних матеріалів, включаючи підручники, лекції, відеоуроки та інше. Наприклад, платформи як Coursera, italki, PROMETHEUS, Duolingo надають доступ до багатьох курсів та навчальних ресурсів.

2. Інтерактивність: Деякі додатки і платформи дозволяють створювати відразу відповіді на завдання, спілкуватися з іншими студентами та вчителями через форуми чи чати. Наприклад, Google Classroom, Moodle, а також додатки для спільної роботи над проектами, такі як Slack чи Trello.

3. Персоналізація: Деякі мобільні додатки та платформи можуть адаптуватися до потреб кожного студента, надаючи рекомендації для навчання та враховуючи індивідуальний прогрес. Наприклад, платформи зі штучним інтелектом, такі як Rosetta Stone або Babbel, можуть пристосовувати вивчення іноземних мов до рівня та потреб користувача.

4. Ефективне використання часу: Мобільні додатки та платформи можуть допомагати раціонально розподіляти час для навчання, нагадуючи про завдання та терміни здачі робіт та дозволяють навчатися з будь-якого місця та в будь-який час, що особливо важливо для зайнятих людей або тих, хто навчається на віддалі.

У сучасних навчальних закладах відбувається перегляд підходів, які використовувалися для навчання української мови за професійним спрямуванням, а також пошук інноваційних методів з урахуванням розвитку інформаційних технологій. З метою відходу від традиційної моделі викладання, яка ґрунтувалася на поясненнях викладача, активно впроваджується використання нових моделей навчання разом з інформаційними технологіями. Інформаційні технології надають студентам доступ до сучасних методів навчання, завдяки чому відбуваються кардинальні зміни в організації навчального процесу, в якому головна роль переходить від викладача до студента, що відповідає завданням гуманізації та гуманітаризації освіти [5, с. 26].

Роль вчителів змінюється з розвитком інформаційних технологій навчання. Студентам не вистачає часу, щоб знайти, проаналізувати, зрозуміти та застосувати отриману інформацію. Тому роль вчителя полягає в тому, щоб допомогти учням розвинути навички, визначити, як знаходити, аналізувати та інтерпретувати потрібні дані. Таким чином, інформаційні технології навчання – це важлива частина процесу модернізації і розвитку освіти.

Приклади мобільних додатків і платформ, які використовуються для навчання:

Duolingo: Додаток для вивчення іноземних мов, який використовує гру та інтерактивні завдання.Регулярні тренування в цьому застосунку допоможуть зробити кроки назустріч своїй меті.

Coursera: це офіційний додаток для однойменного вебсайту, де користувачі мають змогу пройти сотні різноманітних онлайн-курсів із різних предметів. Йдеться про громадські науки, математику, біологію, прикладні науки. Тут знайдуться курси практично для будь-якої сфери.

Italki: Освітня платформа, де можна вибрати репетитора та провести уроки англійської чи будь-якої іншої мови.

Google Classroom: Платформа для вчителів та учнів для спільної роботи над завданнями та матеріалами.

Quizlet: Додаток для створення та вивчення флешкарток і карточок для вивчення нового матеріалу.

Kahoot!: Інтерактивна платформа для проведення вікторин та гри в класі для залучення учнів.

Notability та Evernote: Додатки для організації нотаток та зберігання матеріалів.

Ці додатки та платформи допомагають студентам і вчителям зробити навчання більш ефективним, доступним і цікавим, а також забезпечують можливість навчатися в будь-який зручний для них спосіб.

Впровадження у викладання STEAM-технологій є одним із найбільш продуктивних шляхів формування конкурентоспроможного фахівця. Такий навчальний підхід передбачає рух від практики до теорії, інтеграцію різних наук та активне використання новітніх технологій.

Якщо про STEM-підхід до викладання науковці говорять протягом тривалого часу, то Art-компонент додався нещодавно. Під час розгляду навчального матеріалу є доречним залучення різних видів мистецтв. Було зазначено, що креативність є однією з важливих якостей сучасного професіонала. Розглядатимемо поняття креативності як сукупність творчих можливостей людини, які проявляються в різних видах діяльності [5, с. 109].

Під час вивчення окремих дисциплін доречно використовувати спеціально створені інструменти. Наприклад, GeoGebra – це програма для візуалізації математики з широким функціоналом та зручним інтерфейсом. Розробники зазначають, що GeoGebra «стала провідним постачальником програми динамічної математики, яка використовується для підтримки науки, технологій, інженерії та математики (STEM), освіти та інновацій у викладанні та навчанні в усьому світі». Користувачі мають змогу не лише розробити свій ресурс, але й переглянути проекти інших. У процесі вивчення іноземних мов корисними є різноманітні програми з онлайн-перекладу.

Найпопулярніша з них – Google Перекладач [5, с. 112]. Безумовними перевагами Перекладача є ґрунтовна словникова база, завдяки якій користувач може працювати практично з будь-якою мовою. Як і в інших лінгвістичних словниках, пошук потрібної інформації значно спрощується. Програма перекладає окремі слова, речення та навіть фрагменти тексту. Однак її недоліками є те, що Перекладач не має змоги диференціювати відтінки значень та стилістичні особливості, відсутнє розрізнення омонімів. Під час перекладу речень програма не може врахувати всі специфічні особливості синтаксису певної мови.

Специфіка сучасного навчання у вищих навчальних закладах полягає в здатності не лише озброювати знаннями студентів, а й формувати у них потребу в безупинному самостійному оволодінні ними, розвивати вміння й навички самоосвіти. Тому основним завданням є формування інформаційно-грамотної особистості, здатної розуміти поставлені перед нею завдання, осмислювати, аналізувати результати, шукати нові можливості застосування зі змінами технологій та вимогами ринку.

Отже, застосування інформаційних технологій у навчанні дає величезні можливості вдосконалення продуктів і процесів освіти. Сьогодні Інтернет став локальним джерелом інформації. Тому запуск інтернету в класах та адміністративних приміщеннях значно розширює можливості сучасної освіти і дозволяє людям без обмежень отримувати доступ до онлайн-ресурсів.

Список літератури

1. Як ефективно використовувати технології в освіті https://life.pravda.com.ua/columns/2019/04/22/236630/

2. Мобільні застосунки для навчання https://uaspectr.com/2021/05/27/10-mobilnyh-zastosunkiv-dlya-navchannya-ditej/

3. П'ять програм для ведення проєктів https://ms.detector.media/how-to/post/20620/2018-02-19-pyat-bezkoshtovnykh-program-dlya-vedennya-proektiv-chy-dopomozhut-vony-vporyadkuvaty-robochyy-bezlad/

4. Інформаційні технології навчання https://what.com.ua/informaciini-tehnologii-navcha/3/

5. Інформаційні технології в сучасній системі освіти: моногр. О.М. Романуха, В.М. Зінченко, С.К. Ревуцька, П.О. Чевердак, Д.П. Шапран. ДонНУЕТ, . Кривий Ріг : Вид. Р. А. Козлов, 2019. – 122 с.

УДК 004.056, 004.75

М.О. Рисований, Р.М. Минайленко, В.А. Резніченко
maximofficial@gmail.com, aron70@ukr.net
Центральноукраїнський національний технічний університет, м. Кропивницький

ПЕРЕВАГИ ТА НЕДОЛІКИ РОЗРОБКИ ІГОР ТА ПЗ НА UNREAL ENGINE

В сучасному світі розробка відеоігор та програмного забезпечення є надзвичайно захоплюючою сферою комп'ютерної індустрії. Існує безліч інструментів та платформ для розробки, однак однією з найвидатніших та популярних є Unreal Engine. Цей двигун став епіцентром творчості для тисяч розробників по всьому світу, завдяки своїм вражаючим можливостям та іноваціям.

Основною перевагою двигуна є підтримка різних платформи, що дозволяє розробникам створювати ігри та ПЗ для різних пристроїв.

Наступною перевагою є модульність та розширюваність: Unreal Engine надає можливість розширювати функціональність через плагіни та модулі.

Велика спільнота користувачів: Unreal Engine має велику та активну спільноту користувачів, спільнота розробників та багато навчальних ресурсів допомагають новачкам та досвідченим розробникам отримувати підтримку та навчатися.

Графіка та візуалізація: Unreal Engine відомий своєю потужною графікою та здатністю створювати вражаючі візуальні ефекти.

Наступна перевага – це розширені можливості фізики. Unreal Engine включає в себе потужний фізичний двигун, який дозволяє реалістично моделювати фізичні взаємодії у грі. Це дозволяє розробникам створювати реалістичні рухи, руйнування об'єктів та інші ефекти, які зроблюють гру більш живою та захопливою для гравців. Фізична модель Unreal Engine допомагає створити більш реалістичний імерсивний світ для гри.

Як першим і мабуть основним недоліком для новачків є високі вимоги до апаратного забезпечення. Розробка на Unreal Engine може вимагати потужний комп'ютер, що може бути фінансово важким для деяких розробників.

Другим недоліком є великий обсяг ресурсів. Проекти, створені на Unreal Engine, можуть бути великими та важкими для завантаження, що може впливати на продуктивність.

Вартість ліцензії: Unreal Engine безкоштовний для особистого використання, але для комерційних проектів потрібно сплачувати за ліцензію.

Також варто зауважити, що розробка на цьому двигуні є не простою. Навіть з великою кількістю навчальних ресурсів, Unreal Engine може бути складним для новачків. Велика кількість функцій та налаштувань може виглядати вражаюче для тих, хто тільки починає вивчати цей двигун. Це може призвести до певного розчарування та втрати мотивації в початковій стадії розробки. Наочний інтерфейс та більш простий вступ можуть полегшити процес навчання для новачків.

Загалом, Unreal Engine є потужним інструментом для розробки ігор та програмного забезпечення, Цей двигун надає численні переваги, такі як кросплатформеність, модульність, розширюваність, вражаюча графіка, розширені можливості фізики та багато іншого, однак також має свої недоліки.

Варто перелічити популярні ігри, які були створені на Unreal Engine: Tekken 7, Dead by Daylight, Astroneer, Fortnite, Star Wars Jedi: Fallen Order та ще сотні інших.

Якщо порівнювати Unreal Engine та ще один дуже популярний рушій Unity, то можна відокремити, що графіка у першому більш сучасна, але й більш складна до реалізації, тому новачки дуже часто вибирають Unity, тому що він легший для вивчання та не потребує потужного комп'ютера. Unity відомий своєю більшою кількістю підтримуваних платформ, включаючи мобільні, веб та консольні. Unreal Engine також підтримує багато платформ, але часто використовується для створення ігор для ПК та консолей.

Також, як можна було помітити Unreal Engine зазвичай використовується для великих проектів, в той час, як деякі інші рушії можуть бути застосованими невеликою командою розробників для створення інді-ігор.

Вибір між Unreal Engine та іншими двигунами повинен базуватися на конкретних потребах та ресурсах розробника. Якщо вам важливі вражаючі візуальні ефекти, реалістична фізика та готова спільнота користувачів, то Unreal Engine може бути відмінним вибором. Однак варто бути готовими до вкладення часу та зусиль в оволодіння цим інструментом, особливо для новачків.

Список літератури

1. Joanna Lee, Learning Unreal Engine Game Development, 2016
2. Duncan Harris, Alex Wiltshire, Making Videogames. The Art of Creating Digital Worlds, 2022.
3. Unreal Engine: Game Development from A to Z, 2016.

УДК 004.056, 004.75

В.Ю. Кривохижа, Р.М. Минайленко, В.С. Гермак
vvvetal2003@gmail.com, aron70@ukr.net
Центральноукраїнський національний технічний університет, м. Кропивницький

ДОСЛІДЖЕННЯ МЕТОДІВ ТЕСТУВАННЯ ПСЕВДОВИПАДКОВИХ ЧИСЕЛ

У сучасній інформатиці псевдовипадкові числа широко використовуються в безлічі доповнень, від методів Монте-Карло і імітаційного моделювання до друкованої графіки. Якість використовуваного PRNG побічно пов'язано з якістю отриманого результату. Ось чому Роберт Р. це підтверджує знамените висловлювання Кові: "Генерація випадкових чисел занадто важлива, щоб залишати її на волю випадку." Додаток для шифрування використовує спеціальний алгоритм для генерації випадкових чисел. Ці алгоритми визначені заздалегідь, тому Ви можете генерувати випадкові числа. Якщо ви виберете хороший метод, згенерований стовпець чисел пройде більшість тестів на випадковість. Такі числа називаються псевдовипадковими числами. Давайте розглянемо, як перевіряти псевдовипадкові числа.

Тест на найдовшу послідовність одиниць у блоці

Цей тест ідентифікує послідовність центральних блоків у блоці довжиною m біт. Мета полягає в тому, щоб перевірити, чи є довжина цього стовпця справжньою. Мета полягає в тому, щоб перевірити, чи відповідає довжина цього стовпця очікуваній довжині знайденого одиничного стовпця, коли масив точно такий же.

Тест рангів бінарних матриць

Цей тест обчислює ранг непересічної двійкової матриці, яка генерується з вихідних двійкових стовпців. Метод цього тесту полягає в підтвердженні лінійності порядку фіксованої довжини, що становить початкову послідовність.

Тест на збіг шаблонів, що не перекриваються.

У цьому тесті підраховується кількість попередньо визначених шаблонів, знайдених у вихідній послідовності. Мета - виявити генератори випадкових чи псевдовипадкових чисел, що формують занадто часто задані неперіодичні шаблони. Як і в наступному тесті на збіг шаблонів, що перекриваються, для пошуку конкретних шаблонів довжиною m біт використовується вікно також довжиною m біт. Якщо шаблона не виявлено, вікно зміщується на один біт. Якщо шаблон знайдено, вікно переміщається на біт.

Тест на збіг шаблонів, що перекриваються.

Суть цього тесту полягає в тому, щоб обчислити кількість патернів, знайдених з послідовностей вихідних днів, розташованих на відстані. Вікно довжиною m біт використовується, як і в попередньому тесті, для пошуку певного шаблону довжиною m біт. Якщо шаблон не виявлено, вікно збільшується на 1 біт. Єдина відмінність цього тесту від попереднього полягає в тому, що якщо шаблон знайдений, вікно переміщається вперед на 1 байт, а потім продовжує пошук.

Універсальний статистичний тест Маурера

Тут визначається число біт між однаковими шаблонами у вихідній послідовності (заходи, що мають безпосереднє відношення до довжини стиснутої послідовності). Мета тесту — з'ясувати, чи ця послідовність може бути значно стиснута без втрат інформації. У випадку, якщо це можливо зробити, вона не є справді випадковою.

Тест на лінійну складність

Цей тест заснований на принципі роботи циклу лінійного типу з одночасними посиланнями. Мета полягає в тому, щоб визначити, чи є вхідна послідовність досить складною, щоб її можна було вважати повністю випадковою. Ідеальна послідовність характеризується довгими лінійними регістрами з одночасними підключеннями.

Проблема генерації випадкових та псевдовипадкових послідовностей, що застосовуються у криптографії, залишається актуальною на сьогоднішній день. Існує велика кількість статистичних тестів для перевірки генераторів. Дослідження в даній області продовжуються, і знаходяться ефективніші методи оцінки якості генераторів випадкових послідовностей.

УДК 004.056, 004.75

Д.Р. Рачек
racdanil602@gmsil.com
Київський національний університет будівництва і архітектури, м. Київ

ЗАЛЕЖНІСТЬ МАШИННОГО НАВЧАННЯ ВІД ЯКОСТІ ДАНИХ

«Дані - це нове паливо». Так ска-зав Clive Humby, математик, архітектор Клубної карти Tesco з Великобританії у 2006.

Статистика з Інтернету, зокрема соціальні мережеві сервіси (SNS) свідчить, що кожну хвилину в Facebook публікується понад півмільйона комен-тарів, оновлюється близько 300000 статусів, і завантажується більш ніж 100000 фотографій. Загальна кількість «твітів» за день у Твіттері 500000000. Користувачі Інстаграм за день «лайкають» 4200000000 та діляться 95000000 постами. Генерується незліченна кількість контентів з мобільних пристроїв і не тільки для SNS. Зростаюча тенденція на «підключені пристрої» Інтернету (IoT) і поєднане з нею генерування немислимої кількості нових даних. Для прикладу, у 2016 кількість «підключених пристроїв» була 6500000000, а до 2025 ця цифра обіцяє бути більш ніж 20000000000 та кількість генерованої цими пристроями інформації на рік прогнозується перевищити 500 зетабайт (1 зетабайт = трильйон гігабайт). Не варто забувати і про інші домени, такі як медицина, роботи, сучасні автомобілі.

Однак, для того, щоб ML-моделі працювали ефективно, їм необхідні якісні дані. Якість даних для ML можна визначити як ступінь відповідності даних тому, для чого вони використовуються.

Важливими факторами якості даних для ML є:

- Актуальність. Дані повинні бути актуальними для завдання, для якого вони використовуються. Наприклад, якщо ML-модель використовується для прогнозування цін на акції, то дані повинні бути актуальними для поточної ринкової ситуації.
- Повнота. Дані повинні бути повним і всебічним зображенням того, що вони представляють. Наприклад, якщо ML-модель використовується для діагностики хвороб, то дані повинні включати всі можливі симптоми хвороби.
- Точність. Дані мають бути точними і без помилок. Наприклад, якщо ML-модель використовується для розпізнавання осіб, то дані повинні бути точними, щоб модель не плутала обличчя людей.
- Безсторонність. Дані не повинні містити попереджень, які можуть впливати на результати ML-моделі. Наприклад, якщо ML-модель використовується для прогнозування кредитного рейтингу, дані не повинні містити попереджень щодо раси, статі або доходу.

Вплив якості даних на результативність моделей машинного навчання виявляється не лише у точності прогнозів, але й у взаємодії моделі з реальним світом. Навіть найдосконаліші алгоритми не зможуть дати достовірні результати, якщо вихідні дані містять неточності або не репрезентують реальні умови. Такі неточності можуть виникати з різних джерел, включаючи помилки вводу даних, неповноту або зашумленість. Слід враховувати, що модель навчається на тому, що їй подається, і, якщо ці дані містять помилки, модель автоматично їх вивчає. Глибше розглядання цього аспекту вказує на те, що якість даних не лише визначає ефективність моделі на етапі тренування, але також впливає на її здатність адаптуватися до нових, реальних умов на етапі використання. Це особливо важливо в областях, де умови можуть змінюватися в часі або від одного випадку до іншого.

Неякісні дані можуть призвести до таких проблем:

- Неточність. ML-модель може бути неточною, якщо вона навчається на неякісних даних.
- Нестабільність. ML-модель може бути нестабільною, якщо вона навчається на неякісних даних.
- Небезпека. ML-модель може бути небезпечною, якщо вона навчається на неякісних даних. Особливу увагу слід приділити впливу якості даних на процес прийняття рішень. Якщо дані містять неточності, то і результати, а також рішення, засновані на них, можуть бути спотвореними. Це особливо критично в областях, де прийняття невірного рішення може мати серйозні наслідки, такі як у медицині або фінансах.

Для покращення якості даних можна вжити наступних заходів.

- Вибір даних. Необхідно відібрати дані, які є актуальними, повними, точними та безсторонніми.
- Чистка даних. Необхідно очистити дані від помилок, непотрібних даних та інших проблем..
- Аналітика даних. Необхідно провести аналіз даних, щоб виявити потенційні проблеми з якістю. Якщо ML-модель використовується для прогнозування кредитного рейтингу, необхідно провести аналіз даних, щоб виявити наявність попереджень.

УДК 004.4

П.С. Усік
usikps@kntu.kr.ua
Центральноукраїнський національний технічний університет, м. Кропивницький

ЗАСТОСУВАННЯ ПРИНЦИПІВ ОБ'ЄКТНО-ОРІЄНТОВАНОГО ПРОГРАМУВАННЯ (ООП) У КОНТЕКСТІ НЕЙРОННИХ МЕРЕЖ.

Нейронні мережі в сучасному світі стали надзвичайно важливим інструментом в багатьох сферах, включаючи машинне навчання, обробку природної мови, комп'ютерне бачення і багато інших[1-2]. Однак їх розвиток і підтримка стають складним завданням в міру збільшення їхньої складності. Використання парадигми об'єктно-орієнтованого програмування(ООП) може сприяти полегшенню цього завдання та покращенню структури нейронних мереж.

Об'єктно-орієнтоване програмування може бути корисним під-ходом при розробці програм для нейронних мереж, особливо якщо мова програмування, в якій ви працюєте, підтримує ООП. Ось які переваги ООП можна використовувати в програмуванні нейронних мереж:

1. Модульність: Ви можете створити окремі класи для різних частин вашої нейронних мереж, такі як шари (layers), функції активації і оптимізатори. Це допоможе полегшити розробку, підтримку і розширення вашої моделі.
2. Спадкування (Inheritance): Ви можете використовувати спадкування для створення нових класів, які розширюють функціональність інших класів. Наприклад, ви можете створити клас для специфічного типу нейронної мережі, яка успадковує загальні властивості і методи.
3. Поліморфізм: ООП дозволяє використовувати поліморфізм для створення класів, які можуть мати різні реалізації методів. Наприклад, ви можете мати кілька різних функцій активації і обмінювати їх безпроблемно в рамках одного інтерфейсу.
4. Інкапсуляція: Ви можете захистити деякі деталі реалізації нейронної мережі, роблячи їх приватними або захищеними, і надавати доступ до них через публічні методи. Це допомагає уникнути прямого втручання в деякі чутливі частини коду.
5. Код читабельності: Використання ООП може полегшити зрозуміння вашого коду, особливо для інших розробників, які співпрацюють над проектом. Ваш код може стати більш організованим та структурованим.
6. Підтримка бібліотек: Багато бібліотек для глибокого навчання та нейронних мереж, такі як TensorFlow і PyTorch, використовують ООП. Використання ООП в вашому коді може полегшити інтеграцію з такими бібліотеками.

Проте, у ООП є свої недоліки. Однією з основних проблем ООП є можливість збільшення складності та витрат на розробку. Створюючи кілька класів і об'єктів, ви ризикуєте отримати складну кодову базу, яку важко налагодити, протестувати та оптимізувати. Крім того, ООП вимагає більше ресурсів пам'яті та обчислювальної потужності, що може негативно вплинути на продуктивність та масштабованість вашої програми, особливо у випадках аналізу даних або машинного навчання. Додатково, ООП не завжди є найкращим вибором для відображення структури даних або розв'язання певних завдань. Наприклад, іноді деякі типи даних або операції можуть бути важко представити за допомогою класів, і деякі проблеми можуть потребувати більш декларативного або математичного підходу, який відрізняється від імперативного або процедурного підходу.

Звісно, ООП - це не єдиний спосіб програмування нейронних мереж, і також можна використовувати функціональний стиль програмування. Завдяки своїм концепціям і перевагам об'єктно-орієнтоване програмування переконливо аргументує його включення в операції машинного навчання. ООП сприяє підвищенню надійності та зручності обслуговування, а також пропонує модульний і гнучкий підхід до розробки алгоритмів. Завдяки цьому, шляхом поєднання найкращих принципів розробки програмного забезпечення за допомогою ООП з динамікою машинного навчання, ми можемо розпочати нову епоху оптимізованих та ефективних програм для машинного навчання, спроможних досягти кращої спільної роботи.

Список літератури

1. Wired, Cade Metz. "Finally, Neural Networks That Actually Work".Available: https://www.wired.com/2015/04/jeff-dean/.
2. Lance Dooley. "Object Oriented Programming: Neural Networks".Available: https://www.linkedin.com/pulse/object-oriented-programming-neural-networks-part-1-lance-dooley.

УДК 004.72

О.В. Чижов[1], А.О. Фесенко[1]
alex.definch@gmail.com, aafesenko88@gmail.com
Науковий керівник – к.т.н. доцент Фесенко А. О.
[1]Національний авіаційний університет, м. Київ

SAAS CLOUD SHARED HOSTING ЯК СУЧАСНЕ РІШЕННЯ ДЛЯ МАЛОГО БІЗНЕСУ, ЩОБ БУТИ ОНЛАЙН

У роботі було проведено порівняльний аналіз доступних рішень для малих, слабо навантажених вебсайтів. Результатом аналізу та порівняння таких популярних на ринку рішень, як Shared Hosting і Virtual Private Server, було запропоновано гібридне рішення на базі Хмарних Обчислень, що об'єднує переваги обох рішень і усуває їхні недоліки.

Вступ

Сучасний світ неможливий без інтернету, а основна одиниця інтернету як джерела інформації - це вебсайт. На даний момент створено понад 1,1 мільярда вебсайтів у світі, понад 200 мільйонів або близько 18% активно підтримуються і відвідуються [1]. Щосекунди створюється 3 нових вебсайти [1], це понад 250 тисяч нових сайтів щодоби. Кількість інтернет-користувачів щороку збільшується на 4% і на липень 2023 року налічувала 5,19 мільярдів [2].

Актуальна статистика свідчить, що 69% сайтів не відвідує понад 50 000 відвідувачів на місяць, а половина з усіх активних сайтів у світі має менше 15 000 відвідувачів на місяць [3]. Якщо врахувати, що в середньому кожен відвідувач переглядає 4-6 сторінок за один візит [3], то можна з упевненістю констатувати, що 69% всіх активних сайтів у світі є низько навантаженими, з навантаженням не більше ніж 10 запитів на хвилину або 0.17 RPS (Requests per Second).

Shared Web Hosting

Як правило, для розміщення подібних сайтів використовується Shared Hosting, як найдешевше рішення з ціною менше $5 USD на місяць [4]. Концепція Shared Hosting платформ передбачає конкурентне розміщення безлічі вебсайтів на одному сервері. Така топологія може призвести до просідань швидкості або навіть недоступності вебсайту, коли навантаження на один вебсайт зростає, і ресурсів, що залишилися, недостатньо для решти вебсайтів на цьому ж сервері. У сучасному конкурентному і динамічному світі швидкість має значення. При зменшенні швидкості завантаження сторінки від 1 до 10 секунд, ймовірність того, що відвідувач покине сайт, зростає на 123% [5]. Дослідження Akamai показало, що затримка завантаження на 100 мілісекунд знижує конверсію сайту на 7% [6].

Ще одним суттєвим недоліком Shared Hosting рішень є відсутність гнучкості. Якщо кількість відвідувачів змінюється періодично і в широкому діапазоні, наприклад у вихідні та будні дні, то власникові доводиться платити за дорожчий план, який використовується не на 100%.

Cloud Virtual Private Server

Рішення з виділеними віртуальними серверами (VPS) і хмарними серверами (Cloud Computing via IaaS) дають більшу продуктивність і гнучкість, але вартість володіння та обслуговування значно вища [7]. Клієнту потрібно не тільки оплачувати розробку вебсайту, а й початкове налаштування оточення та подальше обслуговування сервера. Критичним моментом у налаштуванні та обслуговуванні сервера є питання безпеки [7], оскільки власник сам відповідає за налаштування безпеки.

SaaS Cloud Shared Hosting

Альтернативним рішенням може стати об'єднання двох технологій, коли замовник отримує переваги Shared Hosting у вигляді централізованого налаштування та управління. З іншого боку розподілена обчислювальна система дає змогу домогтися більшої продуктивності за менших витрат на обладнання. Кожен вебсайт отримує стільки ресурсів, скільки йому потрібно для обслуговування його клієнтів, при цьому не впливаючи на сусідні ресурси та їхню продуктивність. На додаток до продуктивності, подібна система дає більшу відмовостійкість і безпеку, у зв'язку з тим, що кожен вебсайт розподілений між щонайменше двома серверами в кластері, а сам кластер закритий від зовнішнього світу сервером балансування навантаження.

Таблиця 1
Порівняння технологій за основними параметрами

№ п/п	Характеристика	Shared Web Hosting	Cloud Virtual Private Server	SaaS Cloud Shared Hosting
1	Ціна аренди	Низька	Середня	Низька
2	Ціна налаштування	Відсутня	Низька	Відсутня
3	Ціна обслуговування	Відсутня	Низька	Відсутня
4	Продуктивність	Низька	Висока	Висока
5	Надійність	Низька	Середня	Висока
6	Безпека	Висока	Низька	Висока

Висновок

Розглянувши сучасні технології організації роботи вебсайтів із малим навантаженням, було окреслено їхні архітектурні недоліки, що не вирішуються удосконаленням усередині однієї технології. Гібридне рішення дає змогу розв'язати всі ці недоліки і домогтися більшої продуктивності та економії. З огляду на той факт, що це рішення зачіпає більшість веб ресурсів у сучасному Інтернеті, це потенційно може принести істотний економічний ефект.

Список літератури

1. NJ. How Many Websites Are There in the World? [Електронний ресурс] / NJ // Siteefy. – 2023. – Режим доступу до ресурсу: https://siteefy.com/how-many-websites-are-there/.

2. Kemp S. DIGITAL 2022: GLOBAL OVERVIEW REPORT [Електронний ресурс] / Simon Kemp // DataReportal. – 2022. – Режим доступу до ресурсу: https://datareportal.com/reports/digital-2022-global-overview-report.

3. Fitzgerald A. How Many Visitors Should Your Website Get? [Data from 400+ Web Traffic Analysts] [Електронний ресурс] / Anna Fitzgerald // HubSpot. – 2023. – Режим доступу до ресурсу: https://blog.hubspot.com/blog/tabid/6307/bid/5092/how-many-visitors-should-your-site-get.aspx.

4. Bernheim L. 7 Pros & Cons of Web Hosting (Oct. 2023) [Електронний ресурс] / Laura Bernheim // HostingAdvice.com. – 2023. – Режим доступу до ресурсу: https://www.hostingadvice.com/how-to/pros-cons-web-hosting/.

5. Lopez J. M. 4 Steps to Speed Up your Mobile Site and Increase Conversions [Електронний ресурс] / Jose Maria Lopez // LinkedIn Corporation. – 2021. – Режим доступу до ресурсу: https://www.linkedin.com/pulse/4-steps-speed-up-your-mobile-site-increase-jose-maria-chema-lopez/.

6. Akamai Online Retail Performance Report: Milliseconds Are Critical [Електронний ресурс] // Akamai Technologies. – 2017. – Режим доступу до ресурсу: https://www.akamai.com/newsroom/press-release/akamai-releases-spring-2017-state-of-online-retail-performance-report.

7. Bali K. 7 Different Types of Web Hosting with Pros and Cons [Електронний ресурс] / Kavya Bali // Mantra Ventures Inc.. – 2022. – Режим доступу до ресурсу: https://serverguy.com/servers/types-of-web-hosting-their-pros-cons/.

УДК 004.41

М.В. Хлєбніков, Ю.М. Пархоменко
khlebnikov97@gmail.com, parhomenkoym@ukr.net,
Центральноукраїнський національний технічний університет, м. Кропивницький

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ АВТОМАТИЗОВАНОГО ПЛАНУВАННЯ ПРОЕКТІВ

Планування - найважливіший етап розробки проекту. Це безперервний процес визначення найкращого способу дій для досягнення поставлених цілей проекту з урахуванням обстановки, що складається.

Планування ділиться на два рівні:

1) Стратегічне або великоблокове планування проектів. Воно забезпечує планування черговості робіт, задає фокусуючи цілі і забезпечує контроль виконання зобов'язань.

2) Тактичне планування спринтів, яке забезпечує короткі і зрозумілі цілі для співробітників і враховує високу невизначеність способу реалізації.

Для управління проектами добре зарекомендувало себе прийняття рішень на основі обчислень ЕОМ і призначених для цього програмних систем. Системи планування мають можливість вносити зміни в графік, що містить в собі інформацію про виконання робіт проекту, а також дати їх завершення, витрат і прогрес виконання. Також повинна забезпечуватися синхронізація поточного проекту з затвердженим планом.

Механізм прийняття управлінських рішень зобов'язаний забезпечити оцінку можливих ризиків. Допустимий ризик – важлива складова стратегії ефективного менеджменту. Розробка та методичне обґрунтування поліпшення управління ризиками організацій України при виконанні інвестиційних проектів, з подальшим впровадженням в практику управління, є найважливішою проблемою, яку необхідно вирішити.

Для отримання оцінки впливу та ймовірності ризиків був використаний метод експертного оцінювання[1]. Після етапу оцінки ймовірності виникнення ризику необхідно визначити, наскільки він вплине на проект. Project Management Body of Knowledge (PMBOK) пропонує розглянути 4 фактори впливу: цілі, термін, бюджет і якість [2].

Функціональна схема наведена на рис. 1. Усі дані по проектам виводяться на екран для зручного перегляду, також через ці таблиці можна ввести нову інформацію по проекту, роботам та ризикам. Після обчислень факторів впливу ризиків система побудує діаграму Ганта, на якій буде візуальна індикація ризиків робіт проекту.

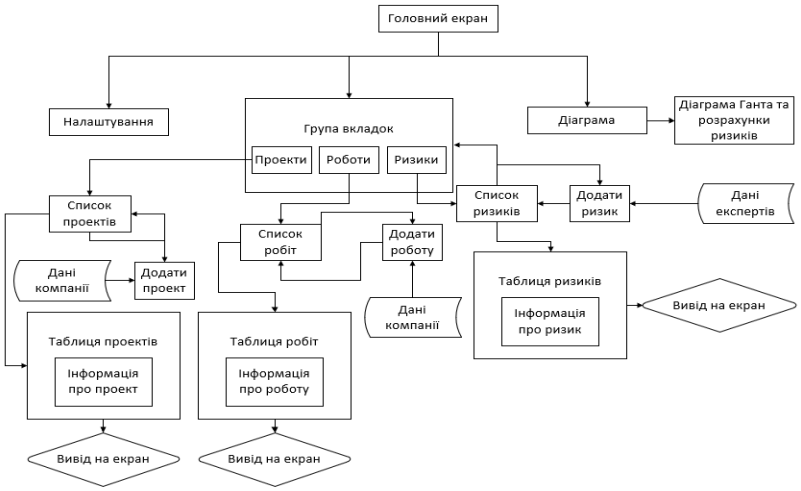


Рис. 1. Функціональна схема системи

Список літератури

1. Грабовецький Б. Є. Методи експертних оцінок: теорія, методологія, напрямки використання: Монографія. – Вінниця: ВНТУ, 2010. – 171 с.

2. Project Management Institute, Project Management Body of Knowledge, Sixth Edition, Project Management Institute Inc., 2017. p. 324-340 c.

УДК 612.17, 004.08

Ю.М. Пархоменко, І.В. Бражніченко, О.В. Бражніченко
parhomenkoym@ukr.net, Oleg.brazhnichenko@gmail.com, ihor.bra@gmail.com
Центральноукраїнський національний технічний університет, м. Кропивницький

ДОСЛІДЖЕННЯ ТА РОЗРОБКА СИСТЕМИ ЗБОРУ ІНФОРМАЦІЇ ДОБОВОГО МОНІТОРУВАННЯ ЕЛЕКТРОКАРДІОГРАМИ НА БАЗІ FLESH НАКОПИЧУВАЧІВ

Дослідження, виявлення і діагностика захворювань сердечно – судинної системи і, зокрема, захворювань серця є однієї з важливих проблем сучасної медицини. Одним з ведучих методів вивчення біоелектричної активності серця є електрокардіографія. Вона на сьогоднішній день незамінна в діагностиці інфарктів міокарда, ішемічної хвороби серця, порушень ритму і провідності, гіпертрофій передсердь і желудочків і інших захворювань серця.

У цьому зв'язку представляється необхідним створення апаратно – програмних засобів для автоматизації процесу діагностики серця (зняття електрокардіограми (ЕКГ), її аналізу і видачі висновку). Важливо визначити оптимальний набір структурних параметрів електрокардіографічного сигналу (ЕКС), що забезпечують найбільш достовірну діагностику, а також розробити алгоритми виділення й обробки характерних структур сигналу, який реєструється.

На рисунку представлена пропонуєма функціональна схема приладу добового моніторування (ДМ) ЕКГ.

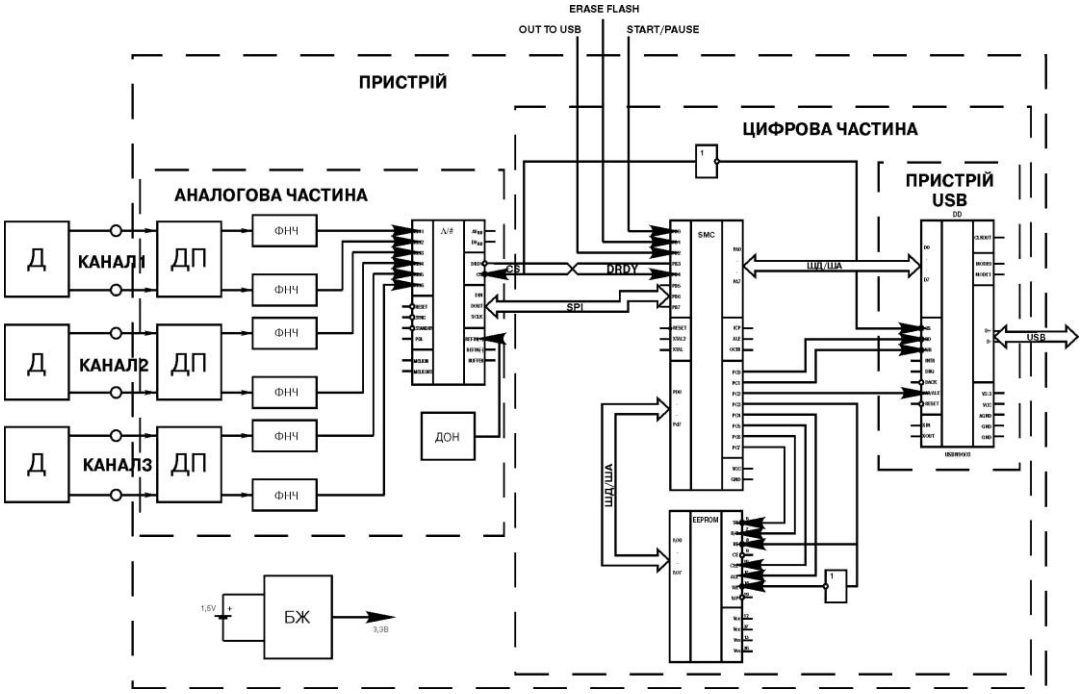


Рис. 1. Функціональна схема приладу

Електрокардіосигнали від трьох каналів, що надходять від електродів (Д), встановлених на тілі людини після підсилення інструментальною схемою диференційного підсилювача (ДП), проходять через ланки фільтрів низької частоти ФНЧ. Частота вибірок кардіосигналу не перевищує 125Гц. Частота фільтрації - 0÷35Гц. Вказані фільтри не пропускають перешкоди мережної частоти (50Гц) постійної складової та сигнали сформовані іншими частинами тіла, що обрізаються ФНЧ знизу. Три пара фазних сигнали з виходу фільтрів подаються на входи аналого-цифрового перетворювача АЦП.

Кожна пара сигналів обробляється в мультиплекс орному режимі і розділена за часом. 24-розрядний двійковий код виборки кожного кардіосигналу у послідовному коді через SPI інтерфейс поступає на входи порту В мікроконтролера SMC З виходу мікроконтролера SMC (порт D) цей код у паралельно-послідовному 8-бітному коді передається до енергонезалежної flash-пам'яті EEPROM. Ємність накопичувача EEPROM 256-512МБ, що дозволяє без стискування зберігати добовий обсяг інформації.

При необхідності накопичена інформація може бути передана в ОЗП персонального комп'ютера для наступної обробки, аналізу і видачі результатів діагностики через контролер USB. Ця інформація через USB порт може бути також записана на портативний flash-накопичувач.

УДК 37:004

Н.М. Якименко
доцент кафедри кібербезпеки та програмного забезпечення, к.ф.-м. н., доцент
yakimenko_n_m@ukr.net
Центральноукраїнський національний технічний університет, м. Кропивницький

ВИКОРИСТАННЯ ГРАФІЧНОГО ІНТЕРФЕЙСУ ЯК МЕТОДОЛОГІЧНОЇ ОСНОВИ ЕЛЕКТРОННОГО ПІДРУЧНИКА

Швидість розвитку сучасного світу невпинно трансформує основи людського буття. Інформація, ставши двигуном прогресу, поступово перетворилася на одну з головних проблем. Інформаційне перенасичення сформувало інформаційних вибух. За даними результатів дослідження Цифрового всесвіту «Extracting Value from Chaos», кожні два роки у світі відбувається подвоєння інформації. У 2016 році об'єм світової інформації становив 16 зеттабайт (16 трлн. гігабайт), а до 2025 року він має збільшитися до 163 зеттабайт. Причина цього – інформаційні технології. Поява комп'ютера, смартфона, інших девайсів надала людині можливість полегшити свій інтелектуальний труд, проте одночасно стала глобальною фабрикою виробництва інформації. Комп'ютер, смартфон сьогодні варто розглядати як знаряддя праці, засіб виробництва, що своєю чергою призводить до соціальних змін, трансформації мислення, переходу до нової формації людського буття. Це не лише змінює наше ставлення до речей, принципи світосприйняття, пріоритети розвитку знань, але й основи економіки, права, культури. У цій ситуації незмінним лишається підручник. Проте, з ростом інформативності суспільства простежується тенденція зниження інтересу суспільства до навчальної літератури. Причина – застарілість методів, покладених в основу навчальної літератури, їх невідповідність та відставання на фоні бурхливого технічного прогресу. Інформатизація навчального процесу не може обмежуватися застосуванням PDF-файлів чи текстів у спеціалізованих навчальних програмах. Необхідне використання ширшого кола підходів: схематизації, віртуалізації, візуалізації навчального матеріалу. Зважаючи на вищевикладені факти, потреба розроблення нових принципів побудови електронних підручників не викликає сумніву. Новий електронний підручник має вмістити не лише значний обсяг інформації, що постійно зростає, але й бути цікавим, простим у користуванні, інтерактивним, мобільним. Можливе створення нового підручника у формі мобільного додатку, що буде доступний у будь-який час у будь-якому місці з будь-якого носія: смартфона, планшета, комп'ютера. Це не лише розширить доступність навчання, зробить його більш цікавим, але й сприятиме ефективнішій обробці інформації.

Сьогодні наукою запропоновано багато підходів до класифікації електронної навчальної літератури: електронні підручники; освітні електронні видання; віртуальні лабораторії; тренажери; електронні бази даних та ін. Усі вони вкладають у суть електронного видання технічні засоби передачі інформації, тестові форми контролю знань (тестпрограми, презентації та ін.) але не враховують принципів роботи та обміну інформацією всередині інформаційного середовища..

Створюючи інформаційні технології, наука породжує не лише новий продукт, ідеї, але й впроваджує в суспільстві нові мови розуміння суті цього продукту, закони його функціонування, розуміння. Користуючись комп'ютером, смартфоном, людина обробляє великі обсяги інформації через графічний інтерфейс екрана і вже не уявляє його функціонування в іншому режимі. З часом людина переносить принципи та закони обігу інформації в інформаційному середовищі на своє буття. Проекція графічного інтерфейсу стає кодом розуміння роботи цього середовища для неї, кодом розуміння будь-якої інформації в світі. Причини такого швидкого поширення принципів графічного інтерфейсу – кластерність розміщення інформації; семіотичне кодування інформації; схематизм. Згадані принципи відповідають основним законам педагогіки: наочність, інформативність, доступність.

Тому з появою комп'ютерів, глобальної інформаційної мережі людина починає мислити також мовою машин. Графічний інтерфейс – це різновид інтерфейсу, в якому елементи інтерфейсу (кнопки, меню, списки) подано у вигляді графічних зображень, що містять у собі більш складну структуровану інформацію. Перевагою графічного інтерфейсу виступає легкість сприйняття та систематизації інформації, його привітність, універсальність з точки зору оновлення, можливість вибору широкої палітри кольорової гами та символів з урахуванням психологічних особливостей здобувача освіти. Одночасно підхід поєднує два важливі принципи навчання: схематизм та символізм, можливість зменшення, збільшення обсягів матеріалу без шкоди для його структури. Знаковість, наочність, семіотика при цьому відіграють важливу роль. Понад 80% усієї інформації людина отримує візуально. На думку дослідників, сприйняття інформації за допомогою візуальних методів є найбільш ефективним. Такий механізм має три рівні: сприйняття, відчуття, уява. Інші ж методи діють виключно на якомусь одному рівні. Спираючись на традиційні моделі сприйняття інформації, які розглядають інформаційний процес з позиції семіотики (Ю. Лотмана, Р. Якобсона, М. Кухта), можна сміливо визнати головну роль у навчанні саме символу, знака, графіки. Результатом їх досліджень є висновок про те, що сприйняття інформації проходить з допомогою саме органів чуття людини, першими включаються в процес її відчуття та сприйняття і лише потім – асоціації, запам'ятовування, впізнання, осмислення. Структурованість навчального матеріалу є важливим доповненням символу. Навчальний матеріал має бути

стиснутий до схем, а не просто згрупований. Сидячи за комп'ютером, людина бачить лише знаки, схеми, а не командні рядки програм, коди, цифри, алгоритми. Це дає можливість сформувати в свідомості студента чіткий образ об'єкта пізнання, чітко дотримуватись навчального алгоритму. Завдання викладача полягає в тому, що він має провести логічно-графічне структурування інформації. Інакше, він закине студентів у потоки нової незрозумілої інформації. Схема завжди краща за текст та більш зрозуміла. На відміну від тексту, де співвідношення понять заховані в словах, схема виносить їх нагору. Текст у даному випадку має меншу структурну візуальну зрозумілість. Схеми та графіки, навпаки, прості, зручні, цікаві.

Прогрес людства став можливим багато в чому саме завдяки вдосконаленню семіотики (символізації) – розвитку нашої мови, особливо таких її відгалужень, як мова символічної логіки, а не через покращення функціональності мозку. Загальновідомим є той факт, що значна частина фізиків, математиків, інженерів мислить візуальними, рідше руховими, образами. Лише наблизившись до завершення свого дослідження, вони починають застосовувати алгебричний аналіз, який перекодовують на текстовий із візуального. За даними нейропсихологів, 48% людей мислять логічним шляхом та 52% – образним. Саме тому проведення міждисциплінарних запозичень у питаннях структурованості інформації дуже важливе, особливо з точних наук, які мають досвід у створенні нових програмних мов та алгоритмів обробки інформації.Такий підхід є актуальним, в тому числі і для гуманітарних наук. Зважаючи на соціальні, вікові, психологічні особливості здобувачів освіти, вони допомагають визначити необхідний зміст матеріалу, робити акценти на важливих питання і темах, постійно проводити корекцію. Урахування психології цінне з точки зору фізіології вищої нервової діяльності, зокрема, у виборі кольорів, символів. При цьому необхідно пам'ятати про об'єктивність та коректність викладача у застосуванні останніх.

Психологія пізнавальних процесів дає змогу визначити раціональні шляхи побудови навчального процесу, прогнозувати можливі складнощі, добирати навчальний матеріал, диференційовано розставляти та застосовувати різні прийоми роботи, види завдань. Отримання додаткових можливостей вільно та самостійно добирати зображення до тем, кольорову гаму сприятиме зростанню зацікавленості слухача, збагаченню його знань шляхом візуалізації. Викладачеві це дасть можливість виявити особливості сприйняття матеріалу, проаналізувати причини такого вибору, психічний стан здобувача. У даній ситуації важливо дотримуватися принципів та законів юзабіліті.

Отже, необхідність оновлення підходів до формування навчальної літератури не викликає сумнівів. Інформаційний вибух XX – початку XXI ст. змушує змінюватися суспільство і в тому числі педагогіку. Поява та поширення інформаційних технологій значно підвищили якість та ефективність навчання, зробили його більш цікавим, спростили доступ до інформації, її обробку, передавання, зберігання. Недоопрацьованими лишилися методи та мова передавання інформації. Використовуючи нові технічні засоби, викладачі продовжують керуватися при формуванні навчальної літератури старими принципами та методами побудови навчального матеріалу. Використання графічного інтерфейсу як методологічної основи електронного підручника дозволяє розміщувати інформацію у значних обсягах, робити її простою та зрозумілою для більшості користувачів. Основними перевагами даного методу є те, що: електронний підручник отримує форму мобільного додатка; значні обсяги інформації можна архівувати в схеми, знаки, символи; варіативність і гнучкість навчального процесу відбувається не за розкладом та дзвоником, а відповідно до особистої біологічної активності організму кожного здобувача індивідуально та в зручний для нього час; навчально-пізнавальна діяльність здобувача активізується з допомогою якісно нового типу візуалізації навчального матеріалу; відбувається посилення мотивації пізнавального інтересу здобувача за рахунок новизни підходів; формується позитивний емоційний фон навчання; можливість постійного оновлення інтерфейсу, його використання як важеля психологічного впливу, елементу психоаналізу; дозволяє задіяти особливості вищої нервової системи з урахуванням індивідуальних особливостей слухачів та тем, що вивчаються. Технічною платформою для створення пропонованого електронного підручника можуть бути мови програмування OpenGL, Direct3D, QML та ін. Особливістю даних програм є побудова складних тримірних сцен, комп'ютерних ігор, віртуальної реальності, візуалізації в наукових дослідженнях. Вирішення графічних завдань можливе за допомогою використати Adobe Photoshop, Corel Draw, RasterDesk, 3D Studio Max, Maya. Наш світ змінюється, з ним змінюються погляди на норми міжлюдських відносин, цінності культури, основи світосприйняття, зважаючи на це, мають змінюватися і принципи побудови навчальної літератури. Покладання даного принципу в основу сучасного створення навчальної літератури розкриває перспективи трансформації формування навчального матеріалу за даним методом з різних дисциплін, на основі розробки універсального конструктора для самостійного створення слухачами електронних підручників.

УДК 004.5

В.О. Гнатюк[1], К.Ю. Зандер[2]
viktor.hnatiuk@npp.nau.edu.ua, 8390983@stud.nau.edu.ua
[1]Національний авіаційний університет, м. Київ

УДОСКОНАЛЕННЯ РОБОТИ СИСТЕМИ МАСОВОГО ОБСЛУГОВУВАННЯ З ВИКОРИСТАННЯМ ВІРТУАЛЬНОГО АСИСТЕНТА НА БАЗІ ШТУЧНОГО ІНТЕЛЕКТУ

Актуальність розробки нових методів оптимізації роботи систем масового обслуговування (СМО) в сучасному світі важлива з кількох ключових причин: поліпшення якості обслуговування (ефективніші СМО дозволяють покращити якість обслуговування та задоволеність клієнтів), ефективне використання ресурсів (оптимізація СМО дозволяє раціонально використовувати ресурси, такі як робочий час, персонал, обладнання та інфраструктура), використання сучасних технологій (сучасні технології, включаючи штучний інтелект (ШІ), аналіз даних та автоматизацію, відкривають нові можливості для оптимізації СМО), підвищення конкурентоспроможності бізнесу (оптимізація роботи СМО дозволяє компаніям підвищити конкурентоспроможність на ринку; швидке та якісне обслуговування стає важливим конкурентним перевагою, що залучає більше клієнтів та покращує їхнє сприйняття бренду), відповідь на сучасні виклики та тенденції (з плином часу змінюються вимоги споживачів та технологічні можливості; оптимізація СМО дозволяє відповісти на нові виклики та адаптуватися до змін у споживчих попитах). Отже, розробка нових методів оптимізації СМО є актуальною науковою задачею, оскільки це сприяє покращенню якості обслуговування, більш ефективному використанню ресурсів, використанню сучасних технологій та підвищенню конкурентоспроможності бізнесу.

Метою роботи є розробка методу оптимізації роботи систем масового обслуговування, з використанням віртуального асистента на базі штучного інтелекту як ефективного інструменту для автоматизації та поліпшення процесів обслуговування користувачів.

Сучасні методи оптимізації роботи СМО включають в себе велику кількість технологій, моделей та стратегій. Ось низка наукових досліджень за цією тематикою: автор представляє загальну теорію черг та методи оптимізації в СМО [1], публікація присвячена моделюванню та аналізу систем обслуговування, включаючи розподіл завдань між ресурсами [2], стаття присвячена методам оптимізації розподілу ресурсів в хмарних обчисленнях для ефективного обслуговування завдань [3], у статті розглядаються методи оцінки довжини черги та керування дозволом на виклики у мережах зі службами з різними характеристиками [4], у статті пропонуються методи машинного навчання для вибору веб-сервісів з урахуванням якості обслуговування [5]. Ці наукові праці представляють деякі з сучасних методів оптимізації СМО, що використовуються в різних галузях, таких як телекомунікації, хмарні обчислення та веб-сервіси.

З огляду на результати аналізу варто зазначити, що сучасні методи оптимізації СМО мають свої переваги, але також існують певні недоліки. Недоліки сучасних методів оптимізації СМО: складність моделювання (багато методів оптимізації вимагають складного математичного моделювання СМО, що може бути складним завданням та вимагати значних обчислювальних ресурсів), чутливість до параметрів (ефективність багатьох методів оптимізації може значно залежати від правильного підбору параметрів моделі, що ускладнює їх практичне застосування та потребує досить точних вхідних даних), обмеженість у реальних умовах (багато моделей базуються на специфічних припущеннях, які можуть не відображати реальні умови СМО, особливо в змінних та непередбачуваних середовищах). Також, варто зазначити переваги СМО з використанням віртуального асистента (ВА) (телеграм бота): автоматизація та ефективність (ВА можуть автоматизувати багато рутинних завдань, полегшуючи роботу співробітників та забезпечуючи ефективне обслуговування клієнтів), покращення якості обслуговування (ВА можуть надати швидку та точну відповідь на запити користувачів, покращуючи загальне враження користувачів від обслуговування), постійна доступність та швидкість відгуку (ВА можуть бути доступні цілодобово та надавати миттєві відповіді, що позитивно впливає на час очікування та задоволення клієнтів), скорочення витрат (використання ВА може допомогти знизити витрати на обслуговування та звільнити людські ресурси для інших важливих завдань), полегшення взаємодії з користувачами (ВА можуть стати зручним інструментом для взаємодії з користувачами, надаючи їм можливість отримати потрібну інформацію та допомогу швидко та легко). Інтеграція ВА у СМО може допомогти максимально використати переваги автоматизації та поліпшити взаємодію з користувачами. Однак важливо розглядати їх як додатковий інструмент, а не як повноцінну заміну людського фактору та експертності.

Розробка методу оптимізації роботи СМО з використанням ВА на базі ШІ. Для розробки ВА необхідно обрати інструменти, платформу та виконаємо наступні етапи.

Етап 1. Реєстрація віртуального асистента. Для реєстрації ВА необхідно обрати платформу, відповідно до досліджень у роботах [6, 7], оберемо для прикладу систему обміну миттєвими повідомленнями Telegram.

Етап 2. Розробка логіки бота в Google Apps Script. При розробці Telegram-бота використаємо Google Apps Script (GAS), що являє собою скриптову платформу, розроблену в Google для розробки легких веб додатків на платформі Google Workspace. Проєкти GAS запускуються в інфраструктурі Google на стороні сервера. Згідно GAS «забезпечує прості шляхи для автоматизації задач на перетині продуктів Google та сторонніх сервісів». GAS також являється інструментом для написання розширень для Google Docs, Sheets та Slides.

Етап 3. Інтеграція ШІ. Для допомоги користувачам використаємо для прикладу GPT-3 (породжувальний попередньо тренований трансформер 3), що являє собою авторегресійну модель мови, яка використовує глибоке навчання, щоби генерувати текст, подібний до людського. Для використання GPT для допомоги користувачам у телеграм боті та підключення до нього GAS, потрібно виконати кілька кроків:

Крок 1. Інтеграція GPT (отримуємо доступ до сервісу, який надає GPT (наприклад, OpenAI GPT-3) та отримуємо API ключ; використовуємо API ключ у GAS для взаємодії з GPT, надсилаючи запити та отримуючи відповіді).

Крок 2. Обробка повідомлень користувачів та відповідей (коли користувач надсилає повідомлення боту у Telegram, GAS отримує це повідомлення через вебхуки, обробка повідомлення користувача та вилучаємо необхідну інформацію).

Крок 3. Надсилання запитів до GPT та обробка відповідей (складаємо запити до GPT, включаючи текст повідомлення користувача або іншу необхідну інформацію; отримуємо відповідь від GPT та оброблюємо її для подальшого використання).

Крок 4. Надсилання відповіді користувачеві (створюємо логіку, яка відправляє оброблену відповідь користувачеві у Telegram через Bot API).

Етап 4. Формування бази даних. Для формування бази даних буде здійснено запис у Google Sheets (writeToGoogleSheet) з використанням функції writeToGoogleSheet, що відповідає за запис даних користувача та їх запит до Google Sheets. Функція додає новий рядок з необхідними даними, у разі помилок вона їх логує. Це дозволяє боту взаємодіяти з користувачем через Telegram, за необхідності, викликати ШІ для генерації відповідей та записувати інформацію про користувачів та їх запити до бази даних.

Таким чином, розроблене рішення для оптимізації роботи СМО з використанням ВА та інтеграції з GAS, Google Tables та GPT. Загальні особливості цього рішення включають наступне: використання ВА, взаємодія з користувачами (бот взаємодіє з користувачами за допомогою кнопок та текстових запитів, дозволяючи їм вибирати інформацію, яка їх цікавить), генерація відповідей за допомогою GPT-3.5, збереження інформації в Google Tables (інформація про користувачів та їх запити зберігається та управляється в Google Tables, спрощуючи роботу з даними та їх аналіз), використання GAS для програмування логіки бота та забезпечення інтеграції з Google Tables, що дозволяє автоматизувати обробку та збереження даних, оптимізація роботи СМО (ВА та інтеграція з GPT-3.5 спрямовані на оптимізацію обслуговування користувачів, забезпечуючи швидку та інформативну відповідь на їх запити). Це загальні особливості розробленого рішення, яке поєднує в собі ефективну комунікацію з користувачами через ВА, розширення можливостей генерації відповідей за допомогою ШІ, та ефективне управління та аналіз даних через GAS.

Список літератури

1. Kleinrock, L. (1976). Queueing Systems, Volume I - Theory. Wiley. 417 p.

2. Gelenbe, E., & Mitrani, I. (1980). Analysis and Synthesis of Computer Systems. Academic Press. London; New York: Academic Press. 239 p.

3. Ananthanarayanan, G., et al. (2010). CloudScale: Elastic Resource Allocation for Cloud Computing Environments. ACM.

4. Zhang, H., & Hou, J. C. (2005). Queue Length Estimation and Call Admission Control in Differentiated Services Networks. IEEE/ACM Transactions on Networking, 13(2), 400-413.

5. Li, W., & Li, Y. (2009). Learning Automata-based QoS-aware Web Service Selection. IEEE Transactions on Services Computing, 2(1), 48-61.

6. Гнатюк В.О., Бондаренко І.О., Каплун І.С. Використання систем обміну миттєвими повідомленнями для автоматизації надання консультативних послуг. Реєстрація, зберігання і обробка даних. Т 23. № 4. 2021. С. 58-67.

7. Гнатюк В.О., Батрак О.Г., Яроцький С.В. Автоматизована система реєстрації місцезнаходження працівника // Проблеми інформатизації та управління: Збірник наукових праць: Випуск 2 (74). К.: НАУ, 2023. С.14 - 20.

УДК 004.62

М. Ю. Ткалич[1], О.Ю. Ткаченко[1]
tkalychmu@kntu.kr.ua, sansomailjokes@gmail.com
[1]Центральноукраїнський національний технічний університет, м. Кропивницький

ВИКОРИСТАННЯ BIG DATA В СФЕРАХ МАРКЕТИНГУ ТА РЕКЛАМИ

У сучасному цифровому світі, основаному на швидко зростаючій кількості даних, Big Data стала незамінною складовою успішного маркетингу та реклами. Масштабні набори даних, їх аналіз та інтерпретація надають компаніям цінні інсайти щодо цільової аудиторії та сприяють зростанню продажів. Використання Big Data забезпечує можливість створювати персоналізовану рекламу, прогнозувати майбутні тренди та покращувати сегментацію споживачів. Розглянемо сучасні методи та підходи використання Big Data цих сферах [1,2].

Використання Big Data у сфері маркетингу та реклами включає збір, аналіз та інтерпретацію великого обсягу даних з різних джерел з метою отримання унікальних інсайтів щодо цільової аудиторії, її вподобань, поведінки та потреб [3]. Це дозволяє компаніям створювати насичені та ефективні маркетингові кампанії, привертати нових клієнтів та зберігати вже наявних [3].

За допомогою Big Data аналітики, маркетологи можуть ретельно проаналізувати інформацію про кожного споживача, зокрема його демографічні дані, географічну локацію, покупки, соціальні мережі, відгуки та інші фактори, що впливають на його рішення придбати товар чи послугу. Зібрані дані допомагають встановити профіль споживача, його потреби та очікування, що дає можливість створювати персоналізовану рекламу, яка найкраще відповідає його інтересам.

Крім того, Big Data аналітика дозволяє прогнозувати та передбачати майбутні тренди та зміни у споживчому попиті. За допомогою алгоритмів машинного навчання та штучного інтелекту, можна аналізувати велику кількість даних і знаходити залежності та закономірності, які допомагають приймати обґрунтовані рішення щодо стратегій маркетингу та реклами.

Використання Big Data у маркетингу також дозволяє краще орієнтуватися на цільову аудиторію, покращувати сегментацію та приймати індивідуальні рішення щодо кожного користувача. Це стимулює зростання продажів, забезпечує підвищення лояльності клієнтів та створює конкурентну перевагу на ринку.

Проаналізувавши існуючі підходи можна виділити наступні тенденції.

1. Персоналізація реклами. Компанії, такі як Google та Facebook, використовують Big Data для аналізу інтересів та поведінки користувачів, щоб показувати їм персоналізовану рекламу. В першу чергу коли розглядаються питання процесу обробки потоку великих даних (Big Data) це персоналізація реклами, цей процес можна розділити на наступні ключові розділити.

1.1 Збір даних. Дані збираються з різних джерел, таких як веб-сайти, соціальні мережі, мобільні додатки, CRM-системи, тощо. Це можуть бути дані про поведінку користувачів, їх інтереси, демографічні дані, геолокацію та інше.

1.2 Зберігання та обробка даних. Зібрані дані зберігаються в великих базах даних. Для обробки великих обсягів даних використовуються спеціалізовані інструменти та технології, такі як Hadoop, Spark, та інші.

1.3 Аналіз даних. Дані аналізуються за допомогою алгоритмів машинного навчання та інших методів аналітики для виявлення закономірностей та тенденцій. Це дозволяє визначити цільові аудиторії та створити персоналізовані рекламні пропозиції.

1.4 Персоналізація реклами. На основі аналізу даних формуються персоналізовані рекламні повідомлення, які відповідають інтересам та потребам конкретних користувачів.

1.5 Доставка реклами та послідуюче вимірювання ефективності. Персоналізовані рекламні повідомлення доставляються користувачам через різні канали комунікації, такі як електронна пошта, соціальні мережі, мобільні додатки, банерна реклама на веб-сайтах, тощо. Після доставки реклами вимірюється її ефективність, аналізуються результати та робляться висновки для оптимізації майбутніх рекламних кампаній.

2. Аналіз ефективності рекламних кампаній. Бренди використовують інструменти аналітики, такі як Google Analytics, для вимірювання ефективності своїх рекламних кампаній та визначення ROI.

3. Цільовий маркетинг. Компанії аналізують дані про покупки та поведінку користувачів, щоб визначити свою цільову аудиторію та створювати персоналізовані пропозиції.

4. Прогнозування трендів. Бренди використовують аналіз даних для прогнозування майбутніх трендів та адаптації своїх маркетингових стратегій.

5. Оптимізація ціноутворення та управління взаємодією з клієнтами. Компанії аналізують дані про конкурентів та попит, щоб встановлювати оптимальні ціни на свою продукцію чи послуги. Бренди використовують Big Data для аналізу взаємодії з клієнтами та покращення обслуговування.

Ці тенденції демонструють, як великі дані можуть бути використані для покращення маркетингових стратегій та рекламних кампаній, забезпечуючи більш персоналізований підхід до клієнтів та підвищуючи ефективність реклами.

Таким чином, Big Data аналітика є потужним інструментом у сфері маркетингу та реклами, який допомагає компаніям розуміти свою цільову аудиторію, прогнозувати тенденції та адаптувати свої стратегії для досягнення кращих результатів.

Однак, використання Big Data аналітики також вимагає від компаній вирішення складних технічних та етичних питань. По-перше, великі обсяги даних потребують потужних обчислювальних ресурсів та компетентного персоналу для їх обробки та інтерпретації. Компанії повинні вкладати значні фінансові кошти у технології Big Data, навчання персоналу та захист цих даних від несанкціонованого доступу.

По-друге, існує також значна проблема з етичним використанням Big Data. Збір та аналіз великого обсягу даних може порушувати приватність та конфіденційність особистих інформаційних даних користувачів. Компанії повинні бути відповідальними за збирання та збереження даних, а також повинні забезпечити можливість відмовитися від збору даних тим, хто так вирішив.

Незважаючи на технічні труднощі та етичні ризики, Big Data аналітика все більше впроваджується в бізнес-середовище.

Компанії, які можуть успішно використовувати Big Data, мають перевагу над своїми конкурентами. Завдяки відомостям, отриманим з великих наборів даних, вони можуть адаптувати свою стратегію маркетингу, йти в ногу з трендами та передбачати майбутні перетворення споживачів.

У подальшому, зростання Big Data аналітики може призвести до змін у сфері маркетингу та реклами. Споживачі стануть усе більш свідомими про збір та використання їх даних, тому компанії повинні вміти діяти прозоро та відповідально. Наслідком цього може бути зміщення уваги від високотехнологічних методів реклами до взаємодії зі споживачем, яка базується на довірі та персоналізації.

Загалом як висновок можна сказати що використання Big Data аналітика має значний потенціал для розкриття нових можливостей у сфері маркетингу та реклами.

Вона дозволяє компаніям збирати та аналізувати великі обсяги даних, що допомагає покращити ефективність рекламних кампаній і залучити більше клієнтів. Однак, важливо усвідомлювати виклики, пов'язані з використанням Big Data, і дбати про етичні аспекти цього процесу.

Лише тоді компанії зможуть успішно використовувати Big Data для досягнення високих показників в продажах та конкурентних переваг.

Список літератури

1. Cavlak N. The Role of Big Data in Digital Marketing. Advanced Digital Marketing Strategies in a Data-Driven Era. 2021. С. 16–33. URL: https://doi.org/10.4018/978-1-7998-8003-5.ch002 (дата звернення: 01.10.2023)

2. Saluja H., Yadav V. K., Mohapatra K. M. Use of Big-Data Analytics with the Interactive Advertisement for Product/Service Representation towards its Customers. INTERNATIONAL JOURNAL OF ADVANCED PRODUCTION AND INDUSTRIAL ENGINEERING. 2019. Т. 4, № 2. URL: https://doi.org/10.35121/ijapie201904235 (дата звернення: 1.10.2023).

3. Lehenchuk S. F., Zavalii T. O. Big Data in marketing analytics: opportunities and problems of use. Problems of Theory and Methodology of Accounting, Control and Analysis. 2023. № 1(54). С. 52–58. URL: https://doi.org/10.26642/pbo-2023-1(54)-52-58 (дата звернення: 1.10.2023).

4. Liu Q., Wan H., Yu H. Application and Influence of Big data Analysis in Marketing Strategy. Frontiers in Business, Economics and Management. 2023. Т. 9, № 3. С. 168–171. URL: https://doi.org/10.54097/fbem.v9i3.9580 (дата звернення: 1.10.2023)

УДК 004.9

В.К Осадчий, Є.В Мелешко, М.С. Якименко
osadchyivlko@kntu.kr.ua, elismeleshko@gmail.com
Центральноукраїнський національний технічний університет, м. Кропивницький

ДОСЛІДЖЕННЯ НЕЙРОННИХ МЕРЕЖ З МОЖЛИВОСТЯМИ НАПИСАННЯ ПРОГРАМНОГО КОДУ ТА ДОПОМОГИ В ІТ-СФЕРІ

У сучасному світі інформаційних технологій нейронні мережі, засновані на великих мовних моделях, займають центральне місце серед засобів машинного навчання та штучного інтелекту. Ці потужні обчислювальні системи, здатні допомагати у розробці програмного коду та вирішувати різні задачі в ІТ сфері. У цій роботі проведено дослідження різних типів відомих нейронних мереж, що можуть допомагати в ІТ-сфері, і порівняння їхніх переваг та обмежень.

ChatGPT – нейронна мережа, здатна генерувати тексти, що може бути потужним і ефективним інструментом у сфері інформаційних технологій.

Переваги ChatGPT:

- Обробка природної мови. Ця нейромережа має вражаючі навички в розумінні, аналізі та генерації тексту. Робота з нею можлива в форматі діалогу на природній мові.
- Загальні знання. Навчена на широкому спектрі даних і має доступ до різноманітних знань та концепцій, включаючи інформацію зі сфери програмування, баз даних, алгоритмів та інших аспектів ІТ.
- Допомога в навчанні. Може бути корисною для учнів, студентів та початківців у сфері ІТ, надаючи пояснення та відповіді на запитання, а також допомагаючи роз'яснити складні концепції.
- Допомога у вирішенні проблем. Може допомогти аналізувати та вирішувати різноманітні проблеми, пов'язані з програмним забезпеченням, знаходячи варіанти та рекомендації рішень.
- Генерація великих обіймів тексту та програмного коду.

Недоліки ChatGPT:

- Можливі певні помилки. Відповіді цієї нейромережі не завжди є ідеальними (особливо, коли ми говоримо про складні завдання або запитання), і іноді вони можуть містити неточності або помилки.
- Неможливість використовувати Інтернет-посилання. Обробляє текст, який надається у запиті, і не може переходити за межі цього обмеженого текстового контексту, напр., за посиланнями користувача.
- Помилки в математиці. Має проблеми у вирішенні певних математичних задач. Це може створити багато помилок, якщо програмне забезпечення потребує великої кількості математичних дій.
- Обмеження у відомостях. Нейромережа може не мати інформації про різні теми або події, які сталися після останнього оновлення даних. Може надавати багато помилок або неправдиву інформацію.

Висновок. ChatGPT може бути корисним інструментом для швидкого отримання відповідей, інструкцій і допомоги в програмуванні та інших сферах ІТ. Однак він має обмеження щодо розуміння контексту, точності та свіжості інформації. Його відповіді слід обов'язково перевіряти на помилки.

Bing – інструмент, створений Microsoft, використовує нейронні мережі для полегшення процесу пошуку потрібної інформації, має функціонал схожий на функціонал ChatGPT.

Переваги Bing:

- Використання передових технологій. Активно використовує технології штучного інтелекту, такі як машинне навчання, глибоке навчання, нейронні мережі та обробка природної мови (NLP), щоб надавати високоякісні відповіді на запитання користувачів. Також може генерувати програмний код.
- Велика функціональність. Bing пропонує широкий спектр функціональних можливостей, включаючи пошук в Інтернеті, створення текстів та програмного коду.
- Сучасна інформація. Нейромережа Bing має можливість надавати інформацію про події, які відбулися навіть сьогодні. Це дозволяє користувачам отримати більш надійну інформацію.
- Широкий спектр додаткових дій. Bing відображає використані пошукові запити та надає список схожих запитів. Крім того надає посилання на джерела інформації для визначення походження даних.
- Швидкість і стабільність. Характеризується високою швидкодією і надійністю в експлуатації. Особливо важливо відзначити, що Bing, відповідає на запити швидше, ніж ChatGPT.
- Допомога у вирішенні проблем. Може допомогти аналізувати та вирішувати різноманітні проблеми, пов'язані з програмним забезпеченням, знаходячи варіанти рішень.

Недоліки Bing:

- Ліміт запитів: має обмеження на кількість запитів, які користувач може зробити в одному діалозі та протягом дня. Тож, користувачі можуть використовувати службу пошуку тільки в обмеженому обсязі.
- Залежність від активних сторінок. Якщо користувач переходить на іншу веб-сторінку або відкриває нову вкладку браузера під час виконання запиту в Bing, це може призвести до зупинки або призупинення процесу пошуку. У ChatGPT ця проблема відсутня.
- Можливі певні помилки. Відповіді цієї нейромережі не завжди є ідеальними (особливо, коли ми говоримо про складні завдання або запитання), і іноді вони можуть містити неточності або помилки.

- Залежність доступу. Bing можна використовувати лише в Microsoft Edge. А ChatGPT може бути відкритим у будь-якому браузері.

- Певні обмеження в генерації великої кількості тексту. Це може робити його не таким зручним для завдань, де потрібна велика кількість тексту або програмного коду.

Висновок. Bing, як пошукова система, може бути корисним інструментом для швидкого доступу до інформації та отримання результатів пошуку в Інтернеті. В порівнянні з ChatGPT, Bing служить більше як пошуковий інструмент, тоді як ChatGPT може генерувати довгі тексти та програмні коди.

Google Bard – це велика мовна модель, розроблена Google AI, навчена працювати з великими обсягами текстових даних і може виконувати такі завдання, як створення тексту, машинний переклад, створення різних типів творчого вмісту та давати інформативні відповіді на запитання.

Переваги Bard:

- Універсальність. Може виконувати різноманітні завдання, такі як створення тексту, машинний переклад, надання інформативних відповідей на запитання, а також створення програмного коду.

- Комплексна підготовка. Bard навчений працювати з великою кількістю текстових даних, тому може генерувати текст, який є не лише творчим, але й точним та інформативним.

- Постійне вдосконалення. Постійно навчається та розвивається, з часом стає кращим.

- Сучасна інформація. Як і Bing, має ширший аспект даних та можливість надавати інформацію про події, які відбулися сьогодні. Це дозволяє користувачам отримати більш актуальну інформацію.

- Допомога у вирішенні проблем. Може допомогти аналізувати та вирішувати різноманітні проблеми, пов'язані з програмним забезпеченням, знаходячи варіанти рішень.

Недоліки Bard:

- Можливі помилки. Іноді робить помилки, коли стикається з новими або складними завданнями.

- Обмеження в генерації довгих текстів. Подібні до Bing обмеження у генерації довгих текстів.

- Залежність доступу. Можна використовувати лише в акаунті Google.

Висновок. Більша частина переваг й недоліків є вже класичними для великих мовних моделей. Bard має в собі багато позитивних сторін та може бути досить корисним при використанні в IT-сфері.

Blackbox AI – помічник для написання коду. Також дозволяє шукати рішення проблем у великій базі даних відкритого доступу, вибрати відповідні фрагменти з готових прикладів. Надає різноманітні інструменти, які допомагають швидше писати ефективний код. Сервіс підтримує автозаповнення коду для десятків популярних мов програмування, включаючи Python, JavaScript, TypeScript, Go, Ruby тощо.

Переваги Blackbox AI:

- Висока ефективність. Швидко створює програмний код, забезпечує його високу якість і точність.

- Завантаження у якості додатка. Blackbox пропонує можливість завантажувати себе як додаток до певних середовищ розробки, наприклад Visual Studio Code. Це спрощує та прискорює процес розробки.

Недоліки Blackbox AI:

- Обмежена функціональність. Не здатна надавати інші відповіді, окрім програмного коду.

- Відсутність можливості зчитувати посилання та зображення.

- Обмеженість у мові. Здатна працювати лише з запитами, що були написані англійською мовою.

Висновок. Blackbox AI є корисним помічником у роботі з кодом.На відміну від попередників, ця нейромережа зроблена виключно для допомоги у програмуванні й це варто враховувати в роботі з нею.

Загальні висновки. Розглянуті нейромережі є важливими інструментами для розробників, оскільки вони можуть автоматизувати та спростити різні аспекти програмування. Використання цих нейромереж дозволяє програмістам вдосконалювати свої навички та прискорювати процес створення програмних продуктів. Їх використання може допомогти в багатьох аспектах роботи та навчання.

Список літератури

3. ChatGPT. URL: https://chat.openai.com/
4. Bing. URL: https://www.microsoft.com/en-us/bing
5. Bard. URL: https://bard.google.com/chat
6. Blackbox AI. URL: https://www.useblackbox.io/
7. Березовський Д. (2023) Ключові відмінності між ChatGPT та Bing. URL: https://chatgpt.com.ua/post/chatgpt-vs-bing-ai-chatbot
8. Ялалов Д., Гащ К. (2023) AI Black Box: що це таке і як працює. URL: https://mpost.io/uk/ai-black-box-what-it-is/
9. Даньшина К. (2023) Google Bard запрацював в Україні – з аудіовідповідями українською мовою, налаштуваннями тону розмови та запитами із зображеннями URL: https://itc.ua/ua/novini/google-bard-zapracyvav-v-ukraini/

УДК 378:004

Я.В. Федюк[1], А.С. Коваленко[1], О.В. Коваленко[1]
viacheslavovich25122001@gmail.com, annasun911@gmail.com, dr.kovalenkoov@gmail.com
[1]Центральноукраїнський національний технічний університет, м. Кропивницький

ВИКОРИСТАННЯ СЕРВІСУ ZOTERO ЯК ІНСТРУМЕНТУ ФОРМУВАННЯ НАУКОВО-ДОСЛІДНИЦЬКИХ НАВИЧОК СТУДЕНТІВ

Сучасний освітній процес вимагає від студентів не лише засвоєння теоретичних знань, але й вміння самостійно проводити наукові дослідження, аналізувати великі обсяги інформації та формувати власні висновки. Одним із ключових аспектів науково-дослідницької діяльності є здатність ефективно працювати з науковою літературою, систематизувати та зберігати зібрані дані [1]. В цьому контексті важливу роль відіграє використання сучасних інформаційних технологій та сервісів, які допомагають оптимізувати процес наукової роботи.

Одним із таких інструментів, який заслуговує на увагу, є сервіс Zotero [2,3]. Це безкоштовний сервіс з відкритим інструментом для зберігання, управління та організації наукових джерел, який дозволяє студентам та науковцям ефективно працювати з літературою [4], створювати бібліографічні списки та ділитися зібраними матеріалами з іншими користувачами [5].

Розглянемо можливості, які надає сервіс Zotero для формування науково-дослідницьких навичок студентів, а також розгляд практичних аспектів використання цього інструменту в освітньому процесі. Важливо зазначити, що використання таких інструментів, як Zotero, сприяє не лише підвищенню ефективності наукової роботи, але й формує інформаційну компетентність студентів, що є важливим аспектом сучасної освіти.

Сервіс Zotero є одним із найпопулярніших інструментів для управління бібліографічними даними, але існують і інші аналогічні системи, такі як EndNote, Mendeley, RefWorks, та інші. Розглянемо переваги та недоліки цих сервісів порівняно з Zotero.

1. EndNote.

Переваги: Широкий спектр функцій та можливостей для управління бібліографічними даними; Значна кількість стилів цитування та форматування; Інтеграція з текстовими редакторами для автоматичного форматування бібліографічних списків.

Недоліки: Висока вартість ліцензії; Складність використання для нових користувачів.

2. Mendeley.

Переваги: Можливість зберігання PDF-файлів та анотування тексту; Інтеграція з соціальними мережами для науковців; Хмарне сховище для зберігання даних.

Недоліки: Обмеження на кількість безкоштовного сховища; Менше кількість стилів цитування порівняно з іншими сервісами.

3. RefWorks.

Переваги: Інтуїтивно зрозумілий інтерфейс; Широкий вибір стилів цитування; Можливість спільної роботи над проектами.

Недоліки: Вартість ліцензії; Обмежені можливості для анотування та роботи з PDF-файлами.

Проведене дослідження показало що загальні переваги сервісу Zotero щодо інших систем це: безкоштовність та відкритість коду; Найбільший вибір стилів цитування та можливість створення власних стилів; Можливість зберігання та анотування PDF-файлів; Інтеграція з текстовими редакторами для автоматичного форматування бібліографічних списків; Можливість спільної роботи над проектами та обміну ресурсами; Інтуїтивно зрозумілий інтерфейс та простота використання.

Сервіс Zotero надає широкий спектр можливостей для формування науково-дослідницьких навичок студентів. Розглянемо детальніше, які інструменти та функції Zotero можуть бути використані в контексті науково-дослідницької діяльності студентів.

1. Збір та організація наукових джерел. Zotero дозволяє зберігати наукові статті, книги, веб-сторінки та інші ресурси в одному місці, що спрощує доступ до необхідної інформації. Під час перегляду веб-сторінок Zotero автоматично ідентифікує наявність досліджень на сторінці та пропонує можливість створити посилання на публікацію в автоматичному режимі. Користувачі можуть створювати папки та колекції для систематизації зібраних матеріалів за темами, проектами або іншими критеріями. Функція тегування дозволяє додавати ключові слова до збережених ресурсів, що полегшує пошук необхідної інформації.

2. Анотування, сортування та ведення нотаток. Zotero надає можливість додавати анотації та нотатки до збережених ресурсів, що дозволяє студентам фіксувати важливі моменти та ідеї під час роботи з літературою. Сервіс сприяє систематизації досліджень для студентів, надаючи їм інструменти для сортування елементів, створення колекцій та маркування їх ключовими словами. Також можна налаштувати збережені пошукові запити, які автоматично поповнюються відповідними матеріалами під час роботи. Функція виділення тексту допомагає виділити ключові фрагменти тексту для подальшого аналізу та використання в науковій роботі.

3. Створення бібліографічних списків та цитування. Zotero надає можливість автоматично генерувати посилання та бібліографічні списки для різних текстових редакторів, включаючи Word, LibreOffice та Google Docs. Завдяки підтримці понад 10 000 форматів цитування в тому числі ДСТУ ГОСТ 7.1:2006, ДСТУ 8302:2015. Користувачі можуть легко адаптувати свої документи до вимог конкретних стилів чи видань. Функція "drag-and-drop" дозволяє легко вставляти цитати та посилання на джерела в текст наукової роботи.

4. Співпраця, синхронізація та обмін ресурсами. Zotero дозволяє спільно писати статті з іншими студентами, розповсюджувати навчальні матеріали серед одногрупників або створювати спільну бібліографію, надаючи можливість безкоштовно ділитися своєю бібліотекою з необмеженою кількістю людей. Сервіс забезпечує синхронізацію даних між різними пристроями користувача, забезпечуючи безперервне оновлення файлів, нотаток та бібліографічних записів, незалежно від використаного веб-браузера чи операційної системи.

Ці та інші можливості Zotero сприяють формуванню науково-дослідницьких навичок студентів, допомагаючи їм ефективно працювати з науковою літературою, систематизувати зібрані дані та підготувати якісні наукові роботи. Zotero розроблено на основі відкритого вихідного коду незалежною некомерційною організацією, яка не зацікавлена в особистій інформації користувачів, що надає можливість контролювати власні дані.

Підсумовуючи, можна сказати, що Zotero є незамінним інструментом для студентів, які працюють з науковими джерелами. Цей сервіс значно спрощує процес збору, організації та використання інформації, що є ключовим аспектом науково-дослідницької діяльності. Автоматичне визначення досліджень на веб-сторінках, можливість легкого створення посилань, інструменти для сортування елементів, створення колекцій та маркування їх ключовими словами роблять процес роботи з науковими джерелами більш ефективним та організованим. Синхронізація даних між різними пристроями, можливість спільної роботи над проектами з іншими студентами, можливість безкоштовно ділитися власною бібліотекою з необмеженою кількістю людей, робить Zotero ідеальним інструментом для співпраці та обміну знаннями. Таким чином, Zotero є потужним інструментом, який може значно покращити якість наукових робіт студентів та сприяти розвитку їхніх науково-дослідницьких навичок.

Список літератури

1. Yvette Pyne, Stuart Stewart. Meta-work: how we research is as important as what we research. British Journal of General Practice. 2022. Т. 72, № 716. С. 130. URL: https://doi.org/10.3399/bjgp22X718757 (дата звернення: 01.10.2023).

2. Vijai C., Natarajan K., Elayaraja M. Citation Tools and Reference Management Software for Academic Writing. SSRN Electronic Journal. 2019. Т. 14, № 6. С. 586–596. URL: https://doi.org/10.2139/ssrn.3514498 (дата звернення: 27.10.2023).

3. Basu A. What is zettelkasten and how to write "papers" using zettelkasten?. Qeios. 2020. URL: https://doi.org/10.32388/zm0v6i (дата звернення: 1.10.2023).

4. Pelatihan Reference Managemenet Software (RMS) Zotero dalam pengelolaan Sumber Rujukan Penelitian / M. Asy'ari та ін. Jurnal Abdimas (Journal of Community Service). 2022. Т. 4, № 3. С. 417–431. URL: https://doi.org/10.36312/sasambo.v4i3.813 (дата звернення: 01.10.2023).

5. Hardjito K., Hariyadi P., Yani E. R. Pelatihan berbasis problem solving strategy penguasaan aplikasi zotero dalam pengelolaan sumber rujukan penelitian. Abdi Masyarakat. 2022. Т. 5, № 2. URL: https://doi.org/10.30737/jaim.v5i2.2412 (дата звернення: 01.10.2023).

УДК 004.8

І.В. Варченко, Є.В. Мелешко
mrcrazyyt67@gmail.com, elismeleshko@gmail.com
Центральноукраїнський національний технічний університет, м. Кропивницький

ДОСЛІДЖЕННЯ СПОСОБІВ ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В ІГРОВІЙ ІНДУСТРІЇ

Штучний інтелект десятиліттями застосовується в ігровій індустрії. Але з впровадженням сучасних інструментів і технологій, таких як графічні процесори (GPU), вдосконалене програмне забезпечення для цифрового мистецтва та величезні набори даних гравців, потенціал штучного інтелекту у цій сфері значно зріс.

Інтеграція методів і технологій штучного інтелекту у відеоігри дозволяє здійснювати створення більш динамічного, чуйного та захоплюючого ігрового процесу. Це включає в себе програмування керованих комп'ютером персонажів та об'єктів у ігровому середовищі, щоб демонструвати розумну поведінку, приймати рішення та взаємодіяти з гравцем та ігровим світом у реалістичній манері.

Основні способи застосування штучного інтелекту у сучасних відеоіграх наступні:

1. *Розумніші NPC*. Неігрові персонажі (NPC) – це персонажі гри, відмінні від основного гравця. Традиційно, NPC були запрограмовані на заздалегідь прописані дії за допомогою кінцевого автомата. Завдяки штучному інтелекту NPC тепер можуть вивчати ігровий стиль гравця та мати динамічний набір дій, що робить їх менш передбачуваними та більш складними для гравця. Прикладом такої гри може стати Skyrim, де штучний інтелект використовують для створення NPC, які можуть унікально взаємодіяти з гравцем. NPC мають свої особистості, і їх поведінка змінюється залежно від дій гравця.

2. *Динамічний Рендеринг*. За допомогою штучного інтелекту та машинного навчання компанії, які розроблюють ігри, намагаються усунути проблему спотворення перспектив. Це явище виникає, коли об'єкт виглядає добре, коли гравець знаходиться далеко, але спотворюється і стає піксельним, коли гравець наближається до цього об'єкта.

3. *Генерація діалогів і реалістичні взаємодії*. У більшості ігор використовується механізм, який значно покращений за допомогою обробки природної мови та аналізу настроїв на основі алгоритмів машинного навчання. При використані такої методики NPC створюють більш точні та реалістичні відповіді у діалогах з гравцем. Хорошим прикладом такої гри є Elder Scrolls IV: Oblivion.

4. *Процедурна генерація*. Процедурна генерація – це використання алгоритмів для динамічного створення ігрового контенту, наприклад, автоматизованої генерації рівнів. Штучний інтелект можна використовувати для створення процедурних систем генерації, які створюють унікальні для кожного гравця середовища, персонажі і предмети. За допомогою чого гравець ніколи не буде знати з чим стикнеться далі у грі. Прикладом такої гри є Minecraft, де створюються унікальні світи для кожного гравця.

5. *Інтелектуальне балансування гри*. AI можна використовувати для балансування ігор для кількох гравців, забезпечуючи справедливі та приємні враження для всіх гравців. Ігровий штучний інтелект може визначити здібності та емоційний стан гравця, а потім налаштувати гру відповідно до цього. Це може навіть включати динамічне балансування складності гри, коли складність гри регулюється в реальному часі залежно від здібностей гравця. Штучний інтелект в іграх може навіть допомогти з'ясувати наміри гравця.

6. *Ефективне тестування та виявлення помилок*. Тестування за допомогою штучного інтелекту може симулювати сотні сценаріїв ігрового процесу, виявляти помилки та збої, а також швидко й ефективно збалансовувати проблеми порівняно з ручним тестуванням. Наприклад, у Red Dead Redemption 2 поведінка NPC та їхня взаємодія з гравцями залежать від таких змінних, як плями крові на одязі персонажа, яким управляє гравець, чи типу капелюха, який він носить.

7. *Виявлення шахрайства*. Штучний інтелект можна використовувати для виявлення інформаційних загроз в онлайн-іграх, наприклад, шахрайства або злому. Це допомагає підтримувати цілісність гри та гарантує, що гравці отримають чесний і приємний досвід.

8. *Обробка природної мови (NLP)*. Обробка природної мови (NLP) проникає в ігри завдяки чат-ботам, керованим штучним інтелектом і іграм із голосовим керуванням. Алгоритми NLP дозволяють гравцям спілкуватися природною мовою з NPC і взаємодіяти з ігровим середовищем за допомогою голосових команд.

9. *Віртуальні помічники*. Деякі ігри включають віртуальних помічників, які можуть допомагати гравцям, надаючи інформацію або вказівки під час гри. Ці помічники використовують обробку природної мови (NLP), щоб розуміти запити гравців і відповідати на них.

10. *Пошук шляху*. Пошук шляху – це процес пошуку найкоротшого шляху між двома точками в грі. Штучний інтелект можна використовувати для створення алгоритмів пошуку шляху, які можуть швидко й ефективно орієнтуватися в складних ігрових середовищах. Це особливо корисно для ігор, які включають дослідження або вимагають від гравця швидкого переходу через рівень.

12. *Розумна поведінка ворога*. Розширений EAI дозволяє ворогам оцінювати оточення та передбачати рухи гравців. Вороги можуть застосовувати такі тактики, як обхід з флангу, укриття або координація з іншими ворогами для стратегічних атак. Цей рівень інтелекту підвищує складність і реалістичність гри.

13. *Налаштування рівнів складності*. Штучний інтелект може динамічно регулювати рівні складності гри залежно від навичок і продуктивності гравця. Це гарантує, що як новачки, так і досвідчені гравці зможуть насолоджуватися грою у своєму власному темпі.

14. *Динамічне оповідання*. Штучний інтелект зробив революцію в галузі ігор у формі інтерактивних розповідей, надаючи можливість автоматично створювати динамічні історії, які розвиваються залежно від вибору гравця. Такий підхід значно покращує занурення гравця та можливість відтворення.

15. *Ігри з голосовим керуванням*. Ігри з голосовим керуванням набувають популярності, особливо у віртуальній реальності (VR) і доповненій реальності (AR). AI розуміє голосові команди та реагує на них, дозволяючи гравцям взаємодіяти з ігровим середовищем інтуїтивно зрозумілим і захоплюючим способом.

16. *Забезпечення інклюзивності*. Персоналізація за допомогою штучного інтелекту забезпечує інклюзивність, оскільки гравці будь-якого рівня кваліфікації можуть отримувати задоволення від гри. Гравці-початківці можуть отримати допомогу, тоді як експерти можуть зіткнутися з більшими труднощами завдяки адаптивності, керованій штучним інтелектом.

Не дивлячись на таку велику кількість плюсів при використані штучного інтелекту у комп'ютерних іграх, на даний час є й деякі мінуси у його використані.

Ось декілька мінусів використання штучного інтелекту у відеоіграх:

1. *Вартість*. Розробка технології AI може бути досить дорогою, що може стати перешкодою для невеликих студій або незалежних розробників.

2. *Складність*. Впровадження штучного інтелекту в гру може бути складним і вимагає спеціальних знань і досвіду. Це може ускладнити розробникам, які не знайомі зі штучним інтелектом, реалізувати його у своїх іграх. А також може вимагати пошуку та додавання спеціалістів зі штучного інтелекту у команду розробників.

3. *Відсутність креативності*. Штучний інтелект може автоматично створювати рівні гри, але він може бути не в змозі придумати справді творчі чи оригінальні ідеї. Це може обмежити потенціал штучного інтелекту в ігровій індустрії.

4. *Обмежений інтелект*. Хоча штучний інтелект може бути дуже складним, він все ще обмежений своїм програмним кодом і даними, на яких його навчали. Це означає, що він може бути не в змозі належним чином реагувати на несподівані ситуації або дії гравця.

5. *Етичні занепокоєння*. Деякі люди можуть мати етичні занепокоєння щодо використання штучного інтелекту в іграх, наприклад, щодо можливості використання штучного інтелекту в неетичних цілях або для збереження шкідливих упереджень.

Висновок. Зараз штучний інтелект у відеоіграх використовується різними способами, починаючи від створення розумних NPC і закінчуючи процедурною генерацією, щоб покращити ігровий досвід. І оскільки штучний інтелект прискорює темпи розвитку, в майбутньому можна передбачати появу ще більшої кількості варіантів його використовування в ігровій індустрії.

Список літератури

1. Krepchenko A. (2023) AI in Gamedev [Електронний ресурс] – Режим доступу до ресурсу: https://medium.com/@anna.krepchenko/ai-in-gamedev-bc4be34ae55e

2. Алві М. (2021) Штучний інтелект і машинне навчання у відеоіграх [Електронний ресурс] – Режим доступу до ресурсу: https://hashdork.com/uk/ai-ml-у-відеоіграх/

3. Artificial Intelligence in Gaming Industry [Електронний ресурс] – Режим доступу до ресурсу: https://www.javatpoint.com/artificial-intelligence-in-gaming-industry

4. DSouza J. (2023) AI in Gaming | 5 Biggest Innovations (+40 AI Games) [Електронний ресурс] – Режим доступу до ресурсу: https://www.engati.com/blog/ai-in-gaming

5. John C. (2023) The Impact of Artificial Intelligence on the Gaming Industry [Електронний ресурс] – Режим доступу до ресурсу: https://medium.com/bestai/the-impact-of-artificial-intelligence-on-the-gaming-industry-393e2b61e6c1

УДК 004.62

Я.В. Федюк[1], О.Ю. Ткаченко[1], А.С. Коваленко[1]
sansomailjokes@gmail.com, viacheslavovich25122001@gmail.com, annasun911@gmail.com
[1]Центральноукраїнський національний технічний університет, м. Кропивницький

ОГЛЯД СУЧАСНИХ ПІДХОДІВ ДО ПІДВИЩЕННЯ ЕНЕРГОЕФЕКТИВНОСТІ ТА ОПТИМІЗАЦІЇ ВИКОРИСТАННЯ ОБЧИСЛЮВАЛЬНИХ РЕСУРСІВ В АЛГОРИТМАХ ХМАРНИХ СХОВИЩ

Сучасний світ характеризується стрімким розвитком інформаційних технологій, що вимагає від науковців та інженерів постійного пошуку нових шляхів оптимізації використання обчислювальних ресурсів. Однією з ключових тенденцій в цій галузі є розвиток хмарних технологій та хмарних сховищ даних. Хмарні сховища дозволяють зберігати великі обсяги даних без необхідності використання власних серверів та інфраструктури, що значно спрощує доступ до інформації та її обробку [1,2]. Однак, разом із зростанням обсягів даних що зберігаються зростає і потреба в енергоефективних та оптимальних підходах до використання обчислювальних ресурсів.

Розглянемо які зараз існують підходи до підвищення енергоефективності та оптимізації використання обчислювальних ресурсів в алгоритмах хмарних сховищ з урахуванням існуючих різних типів комерційних рішень.

Спочатку необхідно визначитись з загальною класифікацією хмарних сховищ та алгоритмів які використовуються, проведені дослідження літературних джерел [1-4] показали що сервіси можна класифікувати за типами послуг, які вони надають.

1. Інфраструктура як сервіс (**Infrastructure as a Service, IaaS**). Надає віртуальні ресурси, такі як віртуальні машини, сховища даних, мережі тощо. Приклади: Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP).

2. Платформа як сервіс (**Platform as a Service, PaaS**). Надає платформу для розробки, тестування та розгортання програмного забезпечення. Приклади: Heroku, Google App Engine, Microsoft Azure App Services.

3. Програмне забезпечення як сервіс (**Software as a Service, SaaS**). Надає готові до використання програмні продукти через Інтернет. Приклади: Google Workspace, Microsoft 365, Salesforce.

4. Функція як сервіс (**Function as a Service, FaaS**) або безсерверні обчислення (Serverless Computing). Надає можливість виконувати код без необхідності управління серверами. Приклади: AWS Lambda, Google Cloud Functions, Azure Functions.

5. Контейнер як сервіс (**Container as a Service, CaaS**): Надає платформу для розгортання та управління контейнерами. Приклади: Google Kubernetes Engine (GKE), Amazon Elastic Kubernetes Service (EKS), Azure Kubernetes Service (AKS).

Відповідно загальну класифікацію алгоритмів що використовуються на хмарних сховищах можна класифікувати за різними критеріями, такими як тип задачі, яку вони вирішують, метод обробки даних, та інші [3,4].

1. Алгоритми обробки даних: Алгоритми для збору та обробки великих обсягів даних (Big Data); Алгоритми для аналізу тексту та обробки природної мови (NLP); Алгоритми для обробки зображень та відео.

2. Алгоритми машинного навчання: Алгоритми класифікації та регресії; Алгоритми кластеризації; Алгоритми рекомендаційних систем; Алгоритми глибокого навчання (нейронні мережі).

3. Алгоритми безпеки: Алгоритми шифрування даних; Алгоритми аутентифікації та авторизації користувачів; Алгоритми виявлення та запобігання атакам.

4. Алгоритми оптимізації ресурсів: Алгоритми балансування навантаження; Алгоритми автомасштабування ресурсів; Алгоритми оптимізації використання сховища даних.

5. Алгоритми управління мережею: Алгоритми маршрутизації та комутації; Алгоритми управління пропускною спроможністю мережі; Алгоритми виявлення та виправлення помилок в мережі.

Залежно від обраного конкретного хмарного сервісу та розв'язуваних завдань можуть використовуватися й інші алгоритми, проте проведене дослідження показало, що для всіх вищерозглянутих підходів є й загальні риси для підвищення енергоефективності та оптимізації ресурсів.

1. Балансування навантаження. Розподіл робочого навантаження між серверами та іншими ресурсами відбувається за допомогою спеціальних алгоритмів балансування навантаження. Ці алгоритми розподіляють запити від користувачів або інші обчислювальні завдання між доступними серверами таким чином, щоб забезпечити оптимальне використання ресурсів та зниження навантаження на окремі сервери.

1.1 Моніторинг ресурсів. Система моніторингу відстежує стан серверів та інших ресурсів, включаючи їхню завантаженість, використання пам'яті, ЦП та інші параметри.

1.2 Алгоритми балансування навантаження. Коли надходить новий запит або завдання, алгоритм балансування навантаження визначає, на який сервер його направити, враховуючи поточну завантаженість серверів та інші параметри. Існують різні алгоритми балансування навантаження, такі як Round Robin, Least Connections, IP Hash та інші.

1.3 Розподіл навантаження. Завдання розподіляються між серверами таким чином, щоб забезпечити оптимальне використання ресурсів та зниження навантаження на окремі сервери. Це дозволяє уникнути перевантаження окремих серверів та забезпечити більш рівномірне використання ресурсів.

1.4 Адаптація до змін. Система постійно проводить моніторинг стану ресурсів та адаптує розподіл навантаження відповідно до змін у завантаженості серверів та інших параметрів.

Таким чином, розподіл робочого навантаження між серверами та іншими ресурсами дозволяє оптимізувати використання ресурсів, знизити навантаження на окремі сервери, зменшити енергоспоживання та продовжити термін служби серверного обладнання.

2. Автомасштабування. Динамічне збільшення або зменшення ресурсів в залежності від потреб, що дозволяє ефективніше використовувати енергію. Зниження використання ресурсів під час періодів низького навантаження (як приклад у нічний час), що зменшує загальне енергоспоживання.

2.1 Сканування поточного ресурсного стану.

2.2 Визначення правил авто масштабування. Адміністратор системи або розробник встановлює правила автомасштабування, які визначають, коли і як збільшувати або зменшувати ресурси. Найпоширеніша практика встановити правило, що якщо використання ЦП перевищує 80%, то слід додати ще один сервер.

2.3 Автомасштабування. Коли параметри системи відповідають встановленим правилам, система автомасштабування автоматично збільшує або зменшує ресурси. Наприклад, якщо використання ЦП перевищує 80%, система автоматично додасть ще один сервер.

2.4 Оптимізація енергоспоживання. Завдяки автомасштабуванню, система може забезпечити оптимальне використання ресурсів, зменшуючи навантаження на окремі сервери та знижуючи загальне енергоспоживання. Під час періодів низького навантаження система може автоматично зменшити кількість використовуваних ресурсів, що також знижує енергоспоживання.

Таким чином, автомасштабування дозволяє більш ефективно використовувати ресурси, адаптуючись до змін у навантаженні, що зменшує загальне енергоспоживання та оптимізує використання ресурсів.

3. Віртуалізація. Забезпечення більш ефективного використання фізичних ресурсів шляхом створення віртуальних машин за допомогою технології віртуалізації. Кожна віртуальна машина отримує частину фізичних ресурсів, які вона може використовувати для виконання своїх завдань. Завдяки віртуалізації можна створити кілька віртуальних машин на одному фізичному сервері, що зменшує потребу в великій кількості фізичних серверів. Це дозволяє більш ефективно використовувати фізичні ресурси, оскільки один сервер може виконувати кілька завдань одночасно. Зменшення кількості фізичних серверів знижує загальне енергоспоживання, оскільки кожен сервер вимагає електроенергії для роботи та охолодження. Віртуальні машини можуть бути легко переміщені між серверами або вимкнені, коли вони не потрібні, що також сприяє економії енергії.

Як висновок можна сказати що розвиток хмарних технологій вимагає від науковців та інженерів пошуку ефективних шляхів використання обчислювальних ресурсів. Впровадження енергоефективних алгоритмів, автомасштабування та віртуалізації може значно оптимізувати використання ресурсів в алгоритмах хмарних сховищ, зменшуючи загальне енергоспоживання та підвищуючи ефективність обробки даних.

Список літератури

1. A Review on Energy Efficient Approaches for Cloud Computing / Riakshi Routray та ін. *International Journal of Innovative Science and Research Technology*. 2023. Т. 8, № 4. С. 3230–3241. URL: https://www.researchgate.net/publication/371069711_A_Review_on_Energy_Efficient_Approaches_for_Cloud_Computing (дата звернення: 01.10.2023).

2. Shally, Kumar S., Gupta P. Energy efficient resource optimization algorithm for cloud infrastructure. *Journal of Intelligent & Fuzzy Systems*. 2022. P. 1–11. URL: https://doi.org/10.3233/jifs-220535 (дата звернення: 01.10.2023).

3. Optimization of energy consumption in cloud computing datacenters / A. Osman та ін. *International Journal of Electrical and Computer Engineering (IJECE)*. 2021. Т. 11, № 1. С. 686. URL: https://doi.org/10.11591/ijece.v11i1.pp686-698 (дата звернення: 01.10.2023).

4. Pandey A. K., Ahmad S. Energy Optimization in Cloud Computing A Review. *International Journal of Computer Sciences and Engineering*. 2019. Т. 7, № 2. С. 249–256. URL: https://doi.org/10.26438/ijcse/v7i2.249256 (дата звернення: 01.10.2023).

УДК 004.056.55

О.М. Назарько
sebexeres@protonmail.com
Національний технічний університет «Харківський політехнічний інститут», м.Харків

ВИКОРИСТАННЯ ШИФРУВАННЯ ДЛЯ ЗБЕРІГАННЯ СЕКРЕТНОГО БІТКОЇН КЛЮЧА В ОПЕРАЦІЙНІЙ СИСТЕМІ LINUX

Актуальність цієї теми полягає в тому, що біткоїн є популярною криптовалютою, яка використовується для зберігання та передачі цінності. У 2021 році зловмисники вкрали понад 1,2 мільярда доларів у біткоїнах. У 2022 році зловмисники отримали доступ до серверів компанії Ledger, яка займається виробництвом апаратних гаманців для зберігання біткоїнів. Унаслідок злому було вкрадено дані про приватні ключі користувачів, які належали до 21 країни.

Секретний біткоїн ключ - це файл, який містить приватний ключ користувача, необхідний для підписання транзакцій. Цей ключ має зберігатися в безпечному місці, щоб його не могли отримати зловмисники. Одним зі способів захисту секретного біткоїн ключа є його шифрування. Це дасть змогу зробити ключ недоступним для зловмисників, навіть якщо вони отримають доступ до пристрою, на якому він зберігається.

GPG [1] - це вільна утиліта шифрування, яка доступна для різних операційних систем, в операційній системі Linux вона використовується за замовчуванням [2]. Алгоритм шифрування AES-256 вважається досить безпечним. Для злому ключа зловмисникові знадобиться велика кількість обчислювальних ресурсів. Для додаткової безпеки пропонується використовувати команду shred [3] для видалення вихідного файлу після шифрування. Shred - це утиліта, яка стирає дані з диска, роблячи їх невідновлюваними.

Пропонована команда шифрування: gpg -c file.txt. Ця команда зашифрує файл з ім'ям file.txt з використанням алгоритму шифрування AES-256. Щоб видалити вихідний файл із секретним ключем, можна використовувати команду shred -u file.txt.

Для розшифрування файлу використовується така команда: gpg file.txt.gpg. Ця команда розшифрує файл з ім'ям file.txt.gpg і створить новий файл з ім'ям file.txt.

Ось кілька рекомендацій, які допоможуть зберегти секретний ключ у безпеці: використання надійного пароля або ключової фрази є одним із найважливіших способів захисту секретного біткоїн ключа; пароль або ключова фраза має бути довгою і складною, щоб її було важко зламати; зберігання зашифрованого файлу в безпечному місці також є важливим заходом безпеки. Зашифрований файл слід зберігати на окремому пристрої, який не під'єднаний до Інтернету; регулярна зміна пароля або ключової фрази допоможе запобігти злому вашого секретного біткоїн ключа, якщо хтось дізнається його.

Пропонований метод шифрування секретного біткоїн ключа є безпечним та ефективним. Він дозволяє захистити ключ від зловмисників, навіть якщо вони отримають доступ до пристрою, на якому він зберігається.

Список літератури

1. GPG шифрування https://www.gnupg.org/documentation/index.html
2. G. Khavaja, "Kali Linux Penetration Testing Bible", 2021.
3. William E Jr Shotts, "The Linux Command Line, 2nd Edition: A Complete Introduction", 2019.

УДК 004.056, 004.75

М.М. Тімчинко, К.Д. Богатирьова
TIM_2000@gmail.com, Bog_ket@gmail.com
Центральноукраїнський Національний технічний університет, м. Кропивницький

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ ЗАСТОСУВАННЯ ОБ'ЄКТНО-ОРІЄНТОВАНОЇ БАЗИ ДАНИХ

На сьогоднішній день неможливо представити відсутність інформаційних технологій у нашому житті. Будь-яка сучасна організація не може обійтися без бази даних. Це навчальні заклади, банки, магазини, заводи, будь-які підприємства і державні установи. Вони використовують їх для перекладу даних в електронний вигляд і об'єднання даних, а також оперативного доступу до них. Це дозволяє економити час і кошти на витрати.

Звичайно, зниження часу є лише побічним ефектом автоматизації. Найголовніше завдання розвитку інформаційних технологій в зовсім іншому - в придбанні тією чи іншою організацією виключно нових якостей, які надають їй істотну конкурентоспроможність.

Метою роботи є дослідження та програмна реалізація системи аналізу застосування ООБД в сучасних ІС.

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

– огляд існуючих реляційних СУБД;

– дослідження концепції об'єктно-орієнтованих баз даних;

– тестування побудованої системи з використанням ООСУБД VelocityDb;

– програмна реалізація ІС на основі ООБД у якості сховища даних.

Для порівняння із класичними реляційними базами даних було протестовано ООБД VelocityDb. Database Benchmark згенерував таблицю і заповнив її такими даними: число типу BIGINT, що виступає основним ключем таблиці, дві колонки типу VARCHAR(255), дві колонки типу INT, дві колонки типу REAL, і колонка типу DATETIME. Таблицю було заповнено одним мільйоном записів.

Розроблене програмне забезпечення створювалося згідно з парадигмою MVC.

MVC (Model-View-Controller) – схема використання декількох шаблонів проектування, за допомогою яких модель, користувацький інтерфейс і взаємодія з користувачем розділені на три окремих компоненти таким чином, щоб модифікація одного з компонентів надавала мінімальний вплив на інші. Дана схема проектування часто використовується для побудови архітектурного каркаса, коли переходять від теорії до реалізації в конкретної предметної області.

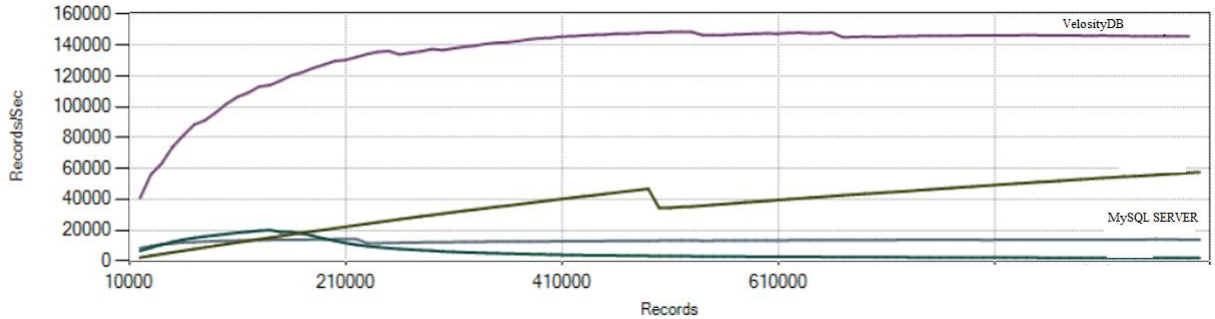


Рис. 1. Результати порівняння SQL Server та ООБД VelocityDb при додаванні даних

У процесі рішення завдань, обумовлених цілями дослідження, отримані наступні результати:

- реалізована інформаційна система, що використовує ООБД VelocityDb у якості сховища даних. Розроблена із використанням .NET Framework + WinForms.

База даних із допомогою інформаційної системи була заповнена тестовими даними про розроблені посібники,та інформацію про працівників. Запити виконуються достатньо швидко.

Проведений аналіз показав доцільність використання ООБД в інформаційних системах зі складною об'єктно-орієнтованою архітектурою та коли потрібна високопродуктивна обробка даних.

Об'єктно-орієнтовані бази даних мають дуже цікаву концепцію в порівнянні з класичними реляційними базами даних: дані, що зберігаються у вигляді об'єктів, інкапсуляція, успадкування, поліморфізм - всі ці особливості забезпечують зручну роботу і велику швидкодію.

УДК 004.8

Тирлич В. О.[1], Ткалич М. Ю.[2]
tyrlychvo@kntu.kr.ua[1], tkalychmu@kntu.kr.ua[2]
Центральноукраїнський національний технічний університет, м. Кропивницький

ОГЛЯД ТА КЛАСИФІКАЦІЯ ОСНОВНИХ НАПРЯМКІВ РОЗВИТКУ ШТУЧНОГО ІНТЕЛЕКТУ

Штучний інтелект (далі ШІ) став ключовим технологічним проривом XXI століття, змінюючи підходи до вирішення складних завдань та покращуючи якість життя людей в різних аспектах [1,2]. Щороку ШІ набуває все більшого значення [3], і його роль у розвитку сучасного суспільства стає дедалі важливішою. Це область, яка постійно зростає і розвивається. Дослідники та фахівці продовжують розробляти нові методи та інновації для покращення можливостей ШІ [4].

Метою цієї роботи є аналіз класифікацій основних напрямків розвитку штучного інтелекту, які визначають сучасний стан у цій області.

Інтелектуальна система може припускати зовнішнє керування, але для неї характерною є самокерованість. Система має певну мету і прагне так планувати свої дії, щоб досягати цієї мети. Як вхідні стимули системи можна розглядати поточну ситуацію, що сприймається і аналізується системою. Результатом реакції системи стає зміна зовнішньої ситуації, і поведінка системи коригується в залежності від того, бажаною чи небажаною є ця зміна. Людина має певну суму знань про світ, яка дозволяє їй орієнтуватися в життєвих ситуаціях та приймати правильні рішення. Крім того, людина вміє певним чином використовувати ці знання. Ці самі риси мають мати системи штучного інтелекту. Також можна стверджувати, що здатність до поповнення первинних знань, є однією із ключових рис інтелектуальних систем. Ця властивість інтелектуальних систем називається здатністю до навчання.

Функціонування інтелектуальної системи можна описати як постійне прийняття рішень на основі аналізу поточних ситуацій для досягнення певної мети. Давайте розглянемо основні напрями розвитку штучного інтелекту:

1. Машинне навчання - це підгалузь ШІ, яка вивчає, як комп'ютери можуть навчатися на основі даних.

2. Глибоке навчання - це форма машинного навчання, яка використовує нейронні мережі з багатьма шарами для вирішення складних завдань, таких як розпізнавання образів та голосу. Ці напрями розвитку дозволили досягнути значних досягнень у сферах, таких як комп'ютерне бачення, розпізнавання мови та автономна навігація.

3. Обробка природної мови (NLP) - NLP вивчає, як комп'ютери можуть розуміти та генерувати людську мову. Цей напрямок важливий для розвитку чат-ботів, систем автоматичного перекладу, аналізу текстів та багатьох інших застосувань.

4. Автономні системи та робототехніка - розвиток ШІ включає створення автономних систем і роботів, які можуть функціонувати без постійної людської контроль, виконуючи завдання в різних сферах, від виробництва до служби у сфері охорони здоров'я.

5. Рекомендаційні системи та персоналізація - цей напрям розвитку ШІ стосується створення алгоритмів, які можуть рекомендувати продукти, послуги, медіа та інше індивідуально кожному користувачу на основі їхніх інтересів та попереднього поведінки.

Підсумовуючи, можна сказати, що штучний інтелект охоплює широкий спектр напрямків, від машинного навчання і глибинного навчання до обробки природної мови і медичного ШІ. Кожен з них відіграє важливу роль у сучасному технологічному просторі. ШІ має великий потенціал для вирішення складних завдань у медицині, транспорті, бізнесі, освіті та інших галузях. Він допомагає підвищити продуктивність і поліпшити якість послуг.

Список літератури

1. Burgess, A. The Executive Guide to Artificial Intelligence. How to identify and implement applications for AI in your organization. London: AJBurgess Ltd, 2018. P. 3. 181 p.

2. Kuenstliche Intelligenz in der Logistik. Begriffe, Anwendungen und Perspektiven. SSI Schäfer. Whitepaper. 2018. P. 18.

3. Slyusar, Vadym. (2019). Artificial intelligence as the basis of future control networks. This is the official publication of the Prepint "Augmented reality in the interests of ESMRM and munitions safety", July 2019. - DOI: 10.13140/RG.2.2.11792.56320.

4. Falk D. How Artificial Intelligence Is Changing Science [Електронний ресурс] / Dan Falk // Quanta Magazine. – 2019. – Режим доступу до ресурсу: https://www.quantamagazine.org/how-artificial-intelligence-is-changing-science20190311/.

ЗМІСТ

СЕКЦІЯ 1. ІНФОРМАЦІЙНА БЕЗПЕКА ДЕРЖАВИ, СУСПІЛЬСТВА ТА ОСОБИСТОСТІ

СЕКЦІЯ 2. ПРОГРАМУВАННЯ ТА ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ

СЕКЦІЯ 3. ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ЕКОНОМІЦІ, МЕДИЦИНІ ТА ОСВІТІ

НАУКОВЕ ВИДАННЯ

ТЕЗИ ДОПОВІДЕЙ

VII Міжнародної науково-практичної конференції до 30-ти річчя кафедри кібербезпеки та програмного забезпечення

"Інформаційна безпека та комп'ютерні технології"

1 листопада 2023 року

Відповідальний за випуск: *О.А. Смірнов*

Комп`ютерна верстка: *Р.М. Минайленко*

Електронне видання

Центральноукраїнський національний технічний університет
пр-кт Університетський, 8, м. Кропивницький, 25006.
тел. (0522) 559-245, www.kntu.kr.ua