ІНФОРМАЦІЙНА БЕЗПЕКА ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Збірник тез доповідей
VII Всеукраїнської
науково-практичної конференції

27 листопада 2025 року

м. Львів

МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

ДЕРЖАВНА СЛУЖБА УКРАЇНИ З НАДЗВИЧАЙНИХ СИТУАЦІЙ

ЛЬВІВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ БЕЗПЕКИ ЖИТТЄДІЯЛЬНОСТІ

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЛЬВІВСЬКА ПОЛІТЕХНІКА»

ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА»

ПРИВАТНИЙ ЗАКЛАД ВИЩОЇ ОСВІТИ «ІТ СТЕП УНІВЕРСИТЕТ»

ІНФОРМАЦІЙНА БЕЗПЕКА ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Збірник тез доповідей
VII Всеукраїнської науково-практичної конференції

27 листопада 2025 року

Львів – 2025

ББК 32.81+78.362

Інформаційна безпека та інформаційні технології: збірник тез доповідей VII Всеукраїнської науково-практичної конференції, м. Львів, 27 листопада 2025 року. Львів, ЛДУ БЖД, 2025, 499 с.

За точність наведених фактів, самостійність наукового аналізу та нормативність стилістики викладу, а також за використання відомостей, що не рекомендовані до відкритої публікації відповідальність несуть автори опублікованих матеріалів.

Секція 1
ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

УДК 004.92:37.018.43

АЛГОРИТМИ КОЛЬОРИСТИКИ І ОСВІТЛЕННЯ В АКЦЕНТУВАННІ ПРОЦЕСІВ ВІЗУАЛІЗАЦІЇ ВЗАЄМОДІЇ ЕЛЕМЕНТІВ ІНФОРМАЦІЙНОЇ ОСВІТНЬОЇ СИСТЕМИ

Андрухів Д.І., Мартин Є.В.
Львівський державний університет безпеки життєдіяльності

Анотація. *Запропоновані підходи до розробки і використання засобів кольористики та освітлення для акцентування процесів візуалізації елементів інформаційної освітньої системи управління закладами зі специфічними умовами навчання. Проведено аналіз математичних моделей та алгоритмічних методів, які забезпечують адаптивне відображення даних розроблюваної системи з урахуванням психофізіологічних особливостей сприйняття освітніх модулів.*

Ключові слова: *інформаційна освітня система, специфічні умови навчання, комп'ютерна графіка, алгоритми освітлення та кольору.*

Abstract. *Proposed approaches to the development and use of coloristics and lighting tools to emphasize the visualization processes of elements of the information educational management system for institutions with specific learning conditions. An analysis of mathematical models and algorithmic methods that provide adaptive display of data from the system under development, taking into account the psychophysiological characteristics of the perception of educational modules, is carried out.*

Keywords: *information educational system, specific learning conditions, computer graphics, lighting and color algorithms.*

Інформаційні технології управління освітніми закладами підготовки фахівців для роботи в надзвичайних ситуаціях потребують використання специфічного програмного забезпечення з подальшою їх модельною реалізацією. Потреба ефективної візуалізації даних має вагоме теоретичне та практичне значення.

Проблема раціонального подання освітньої інформації через використання алгоритмів колористики та освітлення набуває особливої актуальності у зв'язку з підвищеними вимогами до ергономіки й читабельності інтерфейсів, що використовуються як у повсякденному освітньому процесі, так і в сучасних реаліях організації проведення навчального процесу в закладах зі специфічними вимогами.

Відомі математичні моделі кольористики, такі як RGB, HSV, LAB, та алгоритми освітлення, наприклад, модель Фонга, трасування променів, карти тіней, складають базис для результативної візуалізації елементів інформаційної технології управління такими закладами. Пропонована інформаційна освітня система базується на складових елементах, які забезпечують її розвиток та подальше вдосконалення (рис. 1). Реалії сьогодення

потребують реалізації відповідних підходів до структури навчального процесу. На відміну від діяльності закладів вищої освіти в довоєнний період реалії вимагають адаптації до сучасних умов.

Розроблена нами узагальнена схема інформаційної освітньої системи відображає ключові складові елементи і зовнішні та внутрішні фактори, що визначають ефективність її функціонування в умовах специфічних вимог до навчального процесу та соціальних викликів. Центральним елементом освітнього середовища виступає блок «Інформаційна освітня система» (див. рис. 1). Він інтегрує сукупність алгоритмічних, архітектурних і соціальних компонентів у єдину платформу для забезпечення освітнього процесу в закладах освіти системи ДСНС України.

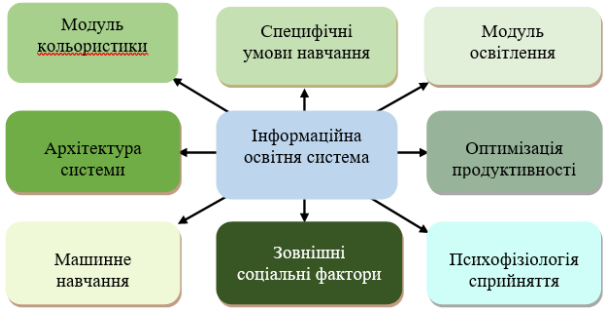

Рисунок 1 – Інформаційна освітня система та її елементи

Запропонована схема є системною моделлю освітнього середовища, де кожен компонент відіграє роль у забезпеченні комплексного управління освітнім процесом у закладах зі специфічними умовами навчання. Вона дозволить:

- здійснювати інтеграцію технологій в єдиній платформі;
- враховувати як технічні, так і психофізіологічні та соціальні фактори;
- підвищити ефективність навчання майбутніх фахівців ДСНС України.

Основи комп'ютерної графіки забезпечують теоретичний фундамент для створення алгоритмів, що здатні автоматично адаптувати колористичні параметри (див. рис. 1) відповідно до специфіки відображуваної інформації. Взаємодія користувача з комп'ютером вимагає врахування психофізіологічних особливостей сприйняття кольору та освітлення, що робить дослідження у цій галузі міждисциплінарним. Розвиток технологій змішаної реальності та графічних інтерфейсів користувача створює нові виклики для традиційних підходів до візуалізації.

Математичні моделі кольористики базуються на векторному представленні просторів кольорів, де кожен колір визначається координатами у тривимірному просторі RGB або альтернативних системах координат HSV, LAB. Алгоритмічна реалізація перетворень між кольоровими просторами використовує матричні операції виду

$$C' = M \times C, \quad (1)$$

де матриця С подає вектор кольорових компонентів,
М - матриця трансформації.

Для забезпечення плавних переходів між кольорами застосовуються інтерполяційні функції типу

$$f(t) = (1-t)C_1 + tC_2, \quad (2)$$

де параметр t визначає позицію на градієнтній кривій між кольорами C_1 та C_2.

Математичні основи теорії кольору включають розрахунок колірної температури та моделювання хроматичних адаптацій через трансформації. Алгоритми автоматичного вибору колірних палітр використовують евклідові метрики у перцептивних колірних просторах для забезпечення максимального контрасту та читабельності інформації.

Важливу роль відіграє освітлення в сприйнятті інформації: через освітлення яскраві барви одразу акцентують увагу (див. рис. 1). Алгоритми освітлення в комп'ютерній графіці грунтуються на фізичних моделях розповсюдження світла та його взаємодії з поверхнями об'єктів.

Для реального часу застосовуються апроксимаційні техніки, включаючи карти тіней та алгоритми відкладеного затінення. Адаптивні алгоритми освітлення автоматично коригують параметри відповідно до семантичного змісту відображуваних даних та контексту використання інформаційної системи (рис. 2).

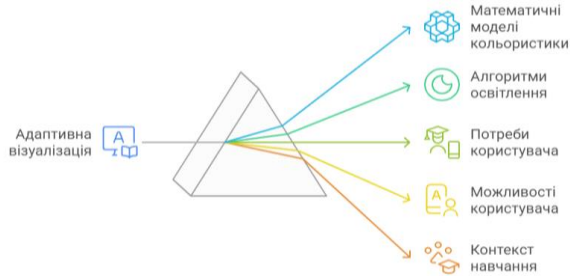

Рисунок 2 – Розкриття адаптивної візуалізації в освіті

Інтеграція алгоритмів кольористики та освітлення в інформаційній системі вимагає створення спеціалізованих рішень, що забезпечують ефективну обробку великих масивів візуальної інформації, властивих для закладів зі спе-

цифічними умовами навчання. Тоді використання мов програмування для перетворення структур графічних інтерфейсів дозволяє створювати гнучкі системи налаштування візуальних параметрів. Алгоритми рендерингу інтерфейсів в мобільних додатках вимагають оптимізації продуктивності через обмежені апаратні ресурси. Методи синхронізації візуальних елементів з потоками даних, властивих для розроблення інформаційної технології управління освітніми закладами зі специфічними умовами навчання забезпечують консистентність відображення інформації у реальному часі. Психологічні аспекти сприйняття кольору важливі при порівнянні розроблюваних елементів інформаційної освітньої технології та враховуються при розробці адаптивних інтерфейсів, що автоматично змінюють колірні схеми відповідно до практичних завдань та реалій сьогодення.

Архітектуру взаємодії основних модулів розроблюваної інформаційної освітньої системи подано на рис. 3. Блок-схема відображає структуру взаємодії модулів кольористики та освітлення в інформаційній освітній системі, де інтегруються дані для візуалізації, алгоритми машинного навчання та інтерфейс користувача. Центральною є інформаційна освітня система, яка генерує вихідні дані про сцену й об'єкти, які надходять у модулі кольористики та освітлення. Вони забезпечують формування колірних схем і динамічного освітлення як це показано на рис. 3. Водночас модуль машинного навчання здійснює адаптивний вибір палітр та оптимізацію параметрів освітлення на основі поведінкових даних користувача, що повертаються з інтерфейсу. Така структура створює замкнений цикл адаптації, завдяки якому досягається індивідуалізація відображення інформації, підвищується ергономічність та ефективність сприйняття освітнього контенту, особливо враховуючи специфічні умови навчання у реаліях сьогодення.

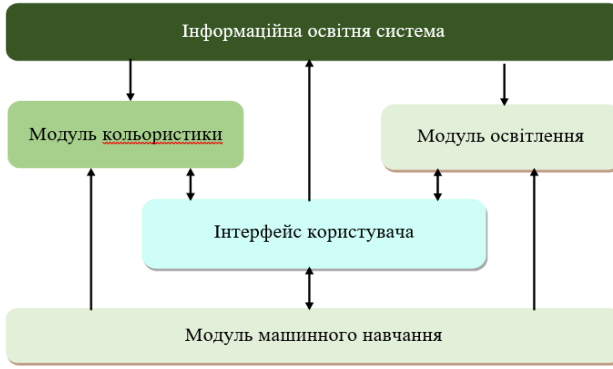

Рисунок 3 – Блок-схема взаємодії модулів кольористики та освітлення в інформаційній освітній системі.

Проведене дослідження показало, що алгоритми кольористики та освітлення є ключовими елементами у забезпеченні якісної та адаптивної візуалізації в інформаційних освітніх системах. Запропонована структура системи дозволяє інтегрувати алгоритмічні, архітектурні та соціальні чинники в єдину платформу, що особливо важливо для закладів зі специфічними умовами навчання. Створюється гнучке освітнє середовище, яке забезпечує адаптивність, індивідуалізацію навчання та підвищення ефективності підготовки майбутніх фахівців ДСНС України.

Література

1. Придатко О., Андрухів Д., Кобко Є. Інформаційні системи управління освітнім процесом, архітектура та оптимізація за допомогою комп'ютерних технологій. Львів: ЛДУБЖД, 2024. 589-594 с.

2. Соломія Лясковська, Євген Мартин. Математичні та алгоритмічні основи комп'ютерної графіки. Львів: ЛДУ БЖД, 2024. 183 с.

3. Edward R. Tufte. Envisioning Infomation: підручник. [Електронний ресурс]. – Доступний з https://coollib.com/b/423601-tafti-edvard-predstavlenie-informatsii/image/

УДК 004.056

ІНТЕГРАЦІЯ БЛОКЧЕЙН-ТЕХНОЛОГІЙ У СИСТЕМИ КОМПЛЕКСНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Валерія БАЛАЦЬКА[1], Андрій ІВАНУСА[1], Василь ПОБЕРЕЖНИК[2]
1. Львівський державний університет безпеки життєдіяльності
2. Національний університет «Львівська політехніка»

Розглянуто інтеграцію блокчейн-технологій у структуру КСЗІ як інноваційний підхід до підвищення довіри, прозорості та стійкості інформаційних систем. Запропоновано гібридну модель на основі permissioned blockchain, яка дозволяє забезпечити простежуваність подій і зменшити ризики внутрішніх порушень. Проаналізовано практичні переваги та напрями впровадження.

Ключові слова: *блокчейн, КСЗІ, довіра, permissioned blockchain, консенсус, ризик, кібербезпека, аутентифікація.*

The paper investigates blockchain technology integration into complex information security systems (ISPS) as an innovative approach to enhance trust, transparency, and resilience. A hybrid permissioned blockchain model is proposed, ensuring event traceability and reducing insider risks. Practical advantages and implementation prospects in critical information infrastructures are discussed.

Keywords: *blockchain, ISPS, trust, permissioned blockchain, consensus, risk, cybersecurity, authentication.*

Сучасна цифрова екосистема, у якій взаємодіють державні, комерційні та освітні структури, функціонує в умовах постійного зростання обсягів даних, кількості користувачів і кіберзагроз. Глобальні тенденції цифрової трансформації – електронне врядування, хмарні сервіси, смарт-контракти, електронна ідентифікація – вимагають не лише технічних, а й концептуально нових підходів до забезпечення безпеки інформації. Водночас посилюються загрози внутрішніх інсайдерів, які мають легітимний доступ до ресурсів і здатні змінювати або видаляти критичні дані.

Класичні системи комплексного захисту інформації (КСЗІ), побудовані на централізованих принципах, уже не відповідають вимогам прозорості та довіри, оскільки значна частина інцидентів виникає не через технічні, а через організаційні та поведінкові фактори [1]. У таких умовах актуальним є створення середовища цифрової довіри, де автентичність і достовірність операцій підтверджуються не адміністраторами, а алгоритмами [2]. Одним із найбільш ефективних підходів є впровадження блокчейн-технологій у структуру КСЗІ, що дозволяє забезпечити незмінність журналів подій, децентралізований аудит, стійкість до внутрішніх маніпуляцій [3] і повну простежуваність життєвого циклу даних.

Блокчейн виступає як архітектура колективного контролю, у якій довіра до системи не потребує довіри до її окремих учасників. На відміну від централізованих баз даних, де єдина точка відмови створює ризики

втрати або спотворення інформації, блокчейн забезпечує консенсусне підтвердження подій між усіма вузлами мережі. Це формує нову парадигму безпеки – розподілену довіру, яка не залежить від людини чи організації, а підтримується математичними та криптографічними механізмами.

Використання permissioned blockchain забезпечує контрольований доступ, автентифікацію вузлів і гнучке управління ролями, що критично важливо для державних або корпоративних інформаційних систем, де відкриті публічні мережі неприйнятні. Такі мережі дозволяють застосовувати канальну сегментацію – кожен підрозділ або служба має власний канал транзакцій, який може перевірятися незалежно, зберігаючи при цьому загальний консенсус.

Запропонована модель інтеграції блокчейн в КСЗІ базується на трирівневій архітектурі, яка включає:

1. Ідентифікаційний рівень – управління ключами, сертифікатами, криптографічними токенами доступу та реєстрами користувачів.
2. Транзакційний рівень – децентралізований аудит і збереження подій у вигляді блоків із підписами та часовими мітками.
3. Аналітичний рівень – математичне оцінювання довіри, поведінковий аналіз і прогнозування ризиків на основі функції довіри.

Формалізований рівень довіри вузла і у момент часу t визначається як $T_i(t) = \alpha P_i(t) + \beta H_i(t) + \gamma S_i(t)$, де $P_i(t)$ – ймовірність коректної поведінки; $H_i(t)$ – показник історичної надійності; $S_i(t)$ – ступінь узгодженості дій із сусідніми вузлами; α, β, γ – вагові коефіцієнти, що описують вплив кожного параметра $(\alpha + \beta + \gamma = 1)$.

Для моделювання ризику використовується експоненційна функція:

$$R_i(t) = 1 - e\text{^}(-\lambda(T(crit) - T_i(t))),$$

де λ – коефіцієнт чутливості системи, $T(crit)$ – критичне значення довіри, за яким система переходить у режим посиленого контролю. Таким чином, навіть незначне падіння довіри викликає нелінійне зростання ризику, що дає змогу оперативно реагувати на потенційні загрози.

Ймовірність несанкціонованої модифікації даних у блокчейн описується виразом $P(mod) = (1 - p)^n$, де p – імовірність правильного підтвердження транзакції одним вузлом, n – кількість вузлів у консенсусній групі. Для систем із 10 вузлами при p=0,85 імовірність успішної підміни даних становить лише 0,0002, що практично унеможливлює компрометацію журналів аудиту.Моделювання виконано на тестовому середовищі Hyperledger Fabric з використанням алгоритмів RAFT і PBFT. Результати показали, що впровадження блокчейн скорочує час виявлення аномалій на 25-30 %, зменшує кількість помилкових сповіщень на 18% і повністю усуває можливість редагування журналів подій без колективного підтвердження.

Особливу увагу приділено організаційному аспекту інтеграції, який полягає у розподілі функцій контролю між підсистемами [4]. Це дозволяє знизити залежність від людського чинника, автоматизувати управління

політиками безпеки та створити «пояснювану КСЗІ» (Explainable Security), де кожне рішення має формалізоване математичне обґрунтування.

Впровадження блокчейн-технологій у державні інформаційні системи України сприятиме реалізації принципів Zero Trust Architecture [5] – архітектури «нульової довіри», що базується на постійній перевірці кожної дії користувача. Крім того, поєднання блокчейн з алгоритмами штучного інтелекту дозволить створювати самонавчальні системи кіберзахисту, які динамічно адаптуються до змін середовища, зберігаючи відповідність міжнародним стандартам ISO/IEC 27001, 27701 та вимогам GDPR.З практичного погляду, така модель може бути впроваджена у вітчизняних реєстрах, зокрема у системах електронних сервісів «Дія», кадастрових реєстрах, медичних базах, банківських сервісах, де важливо довести незмінність транзакцій і зберегти довіру користувачів. Вона також може стати базою для створення універсальної платформи перевірки подій безпеки, здатної інтегрувати різні державні КСЗІ у спільний довірчий простір.

Підсумовуючи, слід зазначити, що інтеграція блокчейн в архітектуру КСЗІ є не просто технологічним трендом, а стратегічним напрямом розвитку національної інформаційної безпеки. Така синергія математичного моделювання, децентралізованої довіри та автоматизованого аудиту формує нову парадигму – «безпека через довіру», яка має потенціал стати основою майбутніх державних і корпоративних систем кіберзахисту.

Література

1. Балацька В. С., Опірський І. Р. Забезпечення конфіденційності персональних даних і підтримки кібербезпеки за допомогою блокчейну // Кібербезпека: освіта, наука, техніка. – 2023. – № 4(20). – С. 6–19. DOI: https://doi.org/10.28925/2663-4023.2023.20.619

2. Balatska V., Opirskyy I. Blockchain as a tool for transparency and protection of government registries // Ukrainian Scientific Journal of Information Security. – 2024. – Vol. 30(2). – P. 221–230. DOI: https://doi.org/10.18372/2225-5036.30.19211

3. Балацька В., Ткачук Р., Маслова Н. Еволюція КСЗІ та інтеграція блокчейн-технологій у кіберзахисті державних інформаційних систем України // Кібербезпека: освіта, наука, техніка. – 2025. – № 2(30). – С. 316–332. DOI: https://doi.org/10.28925/2663-4023.2025.30.975

4. Opirskyi I., Poberezhnyk V., Balatska V. Method for Ensuring Data Integrity and Authenticity Based on Blockchain Technology Integration / I. Opirskyi, V. Poberezhnyk, V. Balatska // DECaT'2025: Digital Economy Concepts and Technologies, April 4, 2025, Kyiv. CEUR Workshop Proceedings 3800, pp. 70-80. URL: https://ceur-ws.org/Vol-4029/

5. Балацька В. С., Побережник В. О., Стефанків А. В., Шевчук Ю. А. Розробка методу забезпечення достовірності та безпеки персональних даних у блокчейн-системах державних реєстрів. Комп'ютерні системи та мережі. 2025. Т. 7, № 1. С. 1–16. DOI: https://doi.org/10.23939/csn2025.01.001

УДК 004.056.55

АВТОМАТИЗОВАНИЙ АНАЛІЗ БЕЗПЕКИ ПЗ НА ОСНОВІ LLM ТА ВЕКТОРНИХ БАЗ ЗНАНЬ

Роман БИЛБАС, Тетяна ЛАВРИК
Сумський державний університет, Суми, Україна

У роботі розглянуто підхід до автоматизації аналізу безпеки програмного забезпечення з використанням великих мовних моделей (LLM). Запропоновано архітектуру інтелектуальної системи, що поєднує можливості LLM та векторних баз знань для виявлення вразливостей і формування рекомендацій щодо їх усунення.

Ключові слова: *безпека програмного забезпечення, великі мовні моделі, аналіз вразливостей, штучний інтелект.*

The paper presents an approach to automated software security analysis using large language models (LLM). The proposed architecture integrates LLM capabilities and vector databases to detect vulnerabilities and generate recommendations for mitigation.

Keywords: *software security, large language models, vulnerability analysis, artificial intelligence.*

Сучасні підходи до безпеки програмного забезпечення вимагають значних людських і часових ресурсів. Традиційні статичні та динамічні аналізатори, попри свою ефективність у виявленні структурних аномалій, часто не здатні повною мірою обробляти логічні взаємозв'язки та контекстні залежності, які можуть призводити до критичних вразливостей. У цьому контексті використання великих мовних моделей (LLM), таких як GPT чи Llama, відкриває нові можливості для автоматизації аналізу вихідного коду, формування припущень щодо потенційних загроз та оцінювання рівня безпекових ризиків. Завдяки здатності моделювати семантику програмного коду LLM можуть виконувати функції інтелектуальних асистентів з аналізу безпеки, доповнюючи або розширюючи можливості класичних методів.

Запропонована методологічна основа ґрунтується на інтеграції великих мовних моделей із векторною базою знань, що містить формалізовані приклади типових вразливостей, сигнатури атак, фрагменти безпечних реалізацій та результати верифікованих аудитів. Така інтеграція забезпечує не лише доступ до структурованих даних, але й можливість контекстної інтерпретації цих даних у процесі аналізу. Подібний підхід корелює з сучасними світовими тенденціями у розвитку інструментів автоматизованого аналізу безпеки, зокрема рішень на кшталт CodeQL,

Semgrep, Snyk, а також новітніх LLM-орієнтованих платформ, що поєднують семантичний пошук із аналітичною інтерпретацією даних. Використання LLM забезпечує глибинний семантичний аналіз програмного коду, виявлення складних логічних помилок, оцінку впливу потенційно небезпечних фрагментів на інші компоненти системи та формування контекстуалізованих пояснень. Векторна база знань, у свою чергу, підвищує стабільність і відтворюваність результатів, забезпечуючи порівняння з великою кількістю прецедентів, що дозволяє зменшити частку хибнопозитивних висновків.

Перевагами такого підходу є масштабованість, можливість аналізу великих обсягів коду без суттєвого збільшення ресурсних витрат, зменшення потреби в участі експертів на початкових етапах перевірки, а також здатність моделі адаптуватися до нових типів атак шляхом періодичного оновлення векторної бази знань. Важливим аспектом є також підвищення швидкості аналізу, що має значення в умовах безперервної інтеграції та доставки програмного забезпечення (CI/CD). Утім, метод має і певні обмеження: залежність від якості тренувальних даних, можливість генерації неповних або некоректних рекомендацій, потреба в ручній валідації складних випадків, а також технічні труднощі, пов'язані з інтеграцією технології у виробничі середовища. Питання інтерпретованості результатів також залишається актуальним, оскільки LLM можуть пропонувати висновки, які потребують додаткової експертної оцінки.

Алгоритм аналізу передбачає три основні етапи:

1. Попередня обробка коду, що включає нормалізацію, розбиття на фрагменти та векторизацію. На цьому етапі забезпечується уніфікація структури вхідних даних і підготовка до семантичної інтерпретації. Розбиття на логічно завершені блоки дає змогу зменшити шум, виділити ключові операції, підвищити точність подальшої обробки та ефективність порівняння фрагментів коду з наявними у векторній базі знань прикладами.

2. Пошук у векторній базі знань на основі семантичних векторних подань. Цей етап дозволяє моделі знаходити фрагменти коду, які за змістом чи структурою подібні до відомих вразливостей або зразків безпечних реалізацій. На відміну від традиційного пошуку за сигнатурами, семантичний пошук враховує контекстні залежності, стиль програмування, порядок виконання операцій і структуру управління. Завдяки цьому виявляються не лише формальні збіги, але й схожі за логікою патерни помилок, що значно підвищує ефективність аналізу.

3. Аналітична інтерпретація результатів, у межах якої формується звіт із висновками щодо рівня безпеки. Модель узагальнює знайдені відповідності, визначає потенційну критичність виявлених вразливостей та оцінює їхній можливий вплив на функціонування системи. На цьому етапі

також генеруються описові пояснення, рекомендації щодо усунення або пом'якшення ризиків, а в окремих випадках - альтернативні варіанти реалізації фрагментів коду, що покращують загальний рівень захищеності.

На основі теоретичного моделювання та аналізу літературних джерел передбачається, що запропонований підхід здатний суттєво підвищити точність виявлення вразливостей порівняно з класичними статичними аналізаторами, особливо у випадках складних логічних помилок або обробки винятків.

Перспективи подальших досліджень охоплюють практичну реалізацію та експериментальну верифікацію технології у реальних програмних продуктах, розширення бази знань реальними кейсами атак, застосування навчання з підкріпленням для адаптації моделі до специфіки окремих програмних продуктів, а також розробку інструментів візуального представлення ризиків у вигляді інтерактивних графічних елементів. У результаті, ці дослідження сприяють фундаментальному переходу від реактивного (усунення наслідків) до проактивного (превентивного) управління кіберризиками. Такий перехід означає не просто зменшення кількості інцидентів, а й значне підвищення загальної стійкості та надійності критично важливого програмного забезпечення на національному та глобальному рівнях.

Додатковим напрямом розвитку запропонованого підходу є формування комплексних систем оцінювання довіри до автоматизованих результатів аналізу, що включають метрики якості генерацій LLM, рівень збіжності результатів між різними моделями та відповідність знайдених патернів відомим категоріям загроз (наприклад, OWASP або CWE). У межах цього підходу перспективним є використання ансамблевих методів, коли кілька незалежних LLM або гібридних моделей паралельно аналізують один і той самий фрагмент коду, а остаточний висновок формується на основі агрегованих результатів. Такий підхід не лише зменшує вплив випадкових помилок, але й забезпечує більш високу стійкість до помилкових інтерпретацій, що є критичним при роботі з системами підвищеного рівня ризику.

Значний потенціал криється в інтеграції LLM з інструментами формальної верифікації та символьного виконання. У цьому контексті, LLM можуть виступати в ролі "семантичного мосту", трансформуючи складні формальні траси у зрозумілі пояснення природною мовою. У перспективі такі інтегровані системи можуть стати основою для створення повністю автономних платформ аналізу безпеки ПЗ, здатних не лише виявляти вразливості, але й прогнозувати їх появу на ранніх стадіях розробки, моделювати потенційні ланцюги атак і оцінювати стійкість архітектурних рішень до новітніх кіберзагроз.

УДК 004.6

АРХІТЕКТУРНІ ПІДХОДИ ДО МАШТАБУВАННЯ БАЗ ДАННИХ

Ростислав БІЛЬСЬКИЙ, Юлія НАЗАР
Львівський державний університет безпеки життєдіяльності

Робота досліджує стратегії масштабування баз даних як ефективний метод забезпечення продуктивності та стабільності інформаційних систем в умовах високих навантажень. Розглядаються ключові принципи вертикального та горизонтального масштабування, їх переваги та недоліки. Аналізуються перспективні методи розподілу даних, такі як шардінг, реплікація та кешування, що підвищують рівень доступності та відмовостійкості.

Ключові слова: *масштабування баз даних, вертикальне масштабування, горизонтальне масштабування, шардінг, реплікація, балансування навантаження, кешування, висока доступність.*

The paper examines database scaling strategies as an effective method of ensuring the performance and stability of information systems under high loads. The key principles of vertical and horizontal scaling, their advantages and disadvantages are considered. Promising methods of data distribution, such as sharding, replication, and caching, which increase the level of availability and fault tolerance, are analyzed.

Keywords: *database scaling, vertical scaling, horizontal scaling, sharding, replication, load balancing, caching, high availability.*

Сучасний цифровий світ генерує постійно зростаючу кількість даних, що створює серйозні виклики для архітектури зберігання та обробки інформації. Традиційні підходи до побудови баз даних, розраховані на фіксоване навантаження, вже не завжди забезпечують належний рівень швидкодії через зростання кількості користувачів та обсягів транзакцій. У зв'язку з цим, масштабування баз даних стає критично важливою складовою стратегії проектування високонавантажених систем. Система масштабування дозволяє адаптувати ресурси бази даних до зростаючих вимог, що дозволяє значно підвищити надійність сервісу. Поєднання оптимізації запитів з архітектурними змінами, такими як кластеризація чи розподіл даних, значно покращує досвід користувачів.

Масштабування є ключовим компонентом забезпечення безперервності бізнес-процесів, гарантуючи обробку пікових навантажень без деградації продуктивності. Це дієвий спосіб вирішення проблем із затримками (latency) та пропускною здатністю (throughput) [1].

Актуальність масштабування пояснюється наступними ключовими причинами:

1. **Зростання обсягів даних.** Дані подвоюються кожні два роки, і без масштабування БД стає "вузьким місцем" системи.

2. Вимоги до швидкодії. Затримки виконання SQL-запитів через перевантаження призводять до втрати клієнтів.

3. Відмовостійкість. Масштабовані системи часто передбачають надлишковість, що зберігає працездатність при збоях окремих вузлів [2].

Першим кроком при зростанні навантаження зазвичай є **вертикальне масштабування (Scale-up)** збільшення потужності окремого вузла додаванням ресурсів (CPU, RAM, SSD). Головна перевага – простота реалізації без зміни коду чи схеми БД. Система залишається централізованою, що спрощує управління транзакціями. Однак метод має обмеження, зокрема до яких можна віднести фізичну межу (потужність одного сервера неможливо нарощувати нескінченно), вартість (ціна хорошого обладнання зростає нелінійно, що робить масштабування економічно невигідним) **а також – єдина точка відмови (**збій єдиного сервера зупиняє всю систему).

Коли можливості вертикального масштабування вичерпані, застосовують стратегії **горизонтального масштабування (Scale-out)**. Вони передбачають розподіл навантаження між декількома серверами, що дозволяє обійти фізичні обмеження одного "заліза". Найпоширенішими методами для побудови таких розподілених систем є:

- **реплікація (Replication) –** створення копій БД. У схемі Master-Slave запис йде на головний сервер, а читання розподіляється між копіями, розвантажуючи систему;
- **шардинг (Sharding) –** розподіл даних таблиці між серверами за ключем (наприклад, ID користувача). Кожен сервер (шард) зберігає частину даних, дозволяючи паралельну обробку запитів. Ефективно для систем з інтенсивним записом;
- **кешування (Caching) –** зберігання результатів частих запитів у швидкій пам'яті (наприклад, Redis), що зменшує навантаження на основну БД [3].

Варто зазначити, що перехід до розподілених систем , які є основою горизонтального масштабування, створює нові виклики. Зокрема, критично важливим для стабільної роботи баз даних є забезпечення **консистентності** (стану, при якому дані на всіх вузлах системи є однаковими та актуальними в будь-який момент часу). Традиційно реляційні бази даних гарантують консистентність через дотримання жорстких принципів **ACID**, але у високонавантажених розподілених архітектурах досягнення повної ізольованості та узгодженості ускладнюється. Самі ж ACID — це набір властивостей, що гарантують коректність транзакцій, зокрема:

- атомарність (atomicity) – транзакція виконується повністю або не виконується зовсім;
- узгодженість (consistency) – база переходить з одного коректного стану в інший, не порушуючи правил;

- ізольованість (isolation) – паралельні транзакції не впливають одна на одну;
- надійність (durability) – результати транзакції зберігаються навіть після збоїв.

Для визначення оптимальної стратегії масштабування вирішальне значення має профіль навантаження (співвідношення операцій читання/запису — Read/Write ratio) та бізнес-вимоги. Сучасні тренди розвитку архітектури баз даних включають гібридні підходи, які полягають у поєднанні вертикального масштабування з горизонтальним розподілом. Крім того, з'явилися СУБД класу NewSQL, що успішно поєднують ACID-транзакції SQL із масштабованістю NoSQL. Третій важливий напрямок — це хмарне автомасштабування, представлене сервісами, як-от Amazon Aurora чи Google Cloud Spanner, які здатні динамічно додавати ресурси відповідно до зростаючого навантаження. [4].

Отож, стратегії масштабування баз даних стали одним із найважливіших інструментів у сучасному арсеналі інженерів програмного забезпечення. Вони надійно забезпечують стабільність інформаційних систем, поєднуючи різні підходи до розподілу навантаження, що забезпечує значно вищий рівень доступності порівняно з традиційними монолітними архітектурами. Впровадження правильної стратегії масштабування дозволяє ефективно протистояти піковим навантаженням, затримкам у роботі та ризикам втрати даних.

Література

1. Database scaling Stratefies. [Електронний ресурс]. – Режим доступу: https://www.educative.io/blog/scalable-systems-101.
2. Методи масштабування реляційних баз даних: переваги, недоліки та кейси використання. [Електронний ресурс]. – Режим доступу: https://dou.ua/forums/topic/45890.
3. Database Scaling. [Електронний ресурс]. – Режим доступу: https://www.mongodb.com/resources/basics/scaling.
4. Sharding with Amazon Relational Database Service. [Електронний ресурс]. – Режим доступу: https://aws.amazon.com/blogs/database/sharding-with-amazon-relational-database-service/.

УДК 371.3

ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ ВИКОРИСТАННЯ ФРЕЙМВОРКІВ ПРИ СТВОРЕННІ КЛІЄНТСЬКОЇ ЧАСТИНИ САЙТУ

Ілля БОЙКО, Алла ЖЕЛЄЗНЯК
Львівський національний університет ветеринарної медицини та біотехнологій імені С.З. Ґжицького

Розглянуто сучасні підходи до створення клієнтської частини сайту з використанням фреймворків. Проаналізовано основні переваги використання Nuxt 3 на основі Vue3 у сфері веброзробки. Проведено порівняльній аналіз ефективності розробки клієнтської частини сайту з використанням фреймворку Vue.js на основі визначених критеріїв та сформовані відповідні висновки.
***Ключові слова**: сайт, клієнтська частина, веб-розробка, фреймворк, Vue.js.*

Modern approaches to creating the client side of a website using frameworks are considered. The main advantages of using Nuxt 3 based on Vue3 in web development are analyzed. A comparative analysis of the effectiveness of developing the client part of the website using the Vue.js framework based on specific criteria is conducted, and relevant conclusions are drawn.
***Keywords**: website, client-side, web development, framework, Vue.js.*

Розвиток та практичне застосування веб-технологій на сьогодні складно уявити без застосування актуальних підходів управління процесом розробки програмного забезпечення, використання фреймворків та інших технологічних рішень, які можуть позитивно вплинути на терміни виконання проекту та його якість. У сфері веб-розробки одним із актуальних питань є ефективність розробки клієнтської частини сайту як визначальної складової, яка відповідає за взаємодію користувача із системою, візуальне представлення даних на сайті, забезпечує реагування на взаємодію користувача з елементами інтерфейсу, а також передачу запитів до сервера.

Практичний досвід показує, що на рівні клієнта сьогодні можна реалізувати валідацію введення даних, маршрутизацію, керування станом застосунку, кешування запитів і локальну обробку інформації. Застосування такого розподілу навантаження між клієнтом і сервером дасть змогу команді розробників збільшувати швидкодію сайту, зменшувати кількість мережевих запитів, впливати на загальний користувацький досвід.

Розвиток веб-технологій та поява повноцінних JavaScript-фреймворків дали змогу розробникам поєднувати зручність бібліотек із архітектурною впорядкованістю проектів. Проведене дослідження показало, що до основних принципів, які впливають на стандарти написання проєктів, пов’язаних із розробкою веб-застосунків, є: компонентність, реактивність, керування станом, шаблонізація та двохсторонній зв'язок даних.

На сьогодні використання фреймворків є стандартом клієнтської розробки, адже такий підхід дає змогу легше створювати інтерактивні сторінки, їх масштабувати та збільшувати продуктивність. Застосування компонентного підходу в ході використання фреймворків для створення клієнтської частини сайту спрощує підтримку і масштабування проекту шляхом поділу інтерфейсу на незалежні модулі. Це дозволяє команді розробників працювати паралельно над пов'язаним функціоналом, перевикористовувати готові елементи та реалізовувати ізольовану логіку в кожному компонентів.

В ході проведеного дослідження було оцінку ефективності фреймворків у порівнянні з традиційною розробкою без їх застосування. Практична реалізація поставленого завдання показала ефективність застосування фреймворку Nuxt 3 [1] на основі Vue3 [2], який поєднує можливості класичної SPA-архітектури з серверним рендерингом (SSR). Це дало змогу забезпечити швидке завантаження сторінок проекту, покращену індексацію пошуковими системами та зручну маршрутизацію.

Загалом до ключових особливостей Nuxt 3 можна віднести: універсальний рендеринг, можливість генерувати статичні HTML-файли під час збірки (SSR), використання сучасних інструментів для збирання коду, забезпечення підтримки серверних функцій та підвищена продуктивність.

З метою проведення об'єктивного аналізу ефективності використання с під час розробки клієнтської частини веб-застосунку було визначено наступні критерії: швидкість розробки, продуктивність інтерфейсу, масштабованість та зручність підтримки коду (табл.1).

Таблиця 1 – Порівняльна оцінка реалізації проектів з фреймворком Vue.js.

Критерій	Без фреймворку	З використанням Vue.js
Швидкість створення компонентів	Висока кількість ручного коду, повторювані DOM-операції	Перевикористання одних і тих самих компонентів в різних частинах коду, іноді кількість коду менша в рази
Підтримка та оновлення	Зміни в інтерфейсі зазвичай потребують оновлень в кількох файлах	Єдина структура компонентів, часто оновлення потребують лише локальних змін, якщо не зачіпається більш глобальна логіка
Реакції на дії користувача	Обробники подій реалізовуються вручну	Події вбудовані в синтаксис шаблонів
Масштабованість	Обмежена, збільшення об'єму коду підвищує ризик виникнення помилок	Ефективна реактивність та віртуальний DOM забезпечують стабільну швидкодію
Продуктивність	Сповільнення при великому обсязі даних, зокрема через практичну відсутність перевикористовуваних частин коду	Краща стабільніть та зростання продуктивності роботи

Були проаналізовані проекти, які підтримувалися без використання фреймворків на чистому JavaScript та проекти, розроблені з використанням Vue.js.

У результаті практичного порівняння на основі визначених критеріїв Vue.js продемонстрував суттєве зниження обсягу коду та часу розробки, а також кращу стабільність та інтуїтивність при розширенні функціоналу клієнтської частини сайту.

Для тестування продуктивності був використаний вбудований в Chtome DevTools інструмент Lighthouse. Результати тестування були наступні:

1. Середній показний Performance ≥ 90 для основних сторінок;
2. Швидкість першого відображення контенту (First Contentful Paint) – до 1.2 с;
3. Стабільна робота при динамічному оновленні списків подій без помітних затримок;
4. Відсутність витоків пам’яті під час багаторазового перемикання сторінок.

Внутрішні тести підтвердили, що використання реактивних об’єктів Vue (ref, reactive, computed) дозволяє ефективно оновлювати дані без повного перерендеру сторінки.

Отже, проведене дослідження показало ефективність використання фреймворку Vue.js для створення клієнтської частини сайту в порівнянні із традиційними підходами, що може позитивно вплинути як на роботу команди розробників проекту, так і реалізацію та підтримку сайту.

Література

1. 1. Nuxt: The Progressive Web Framework [Електронний ресурс] – Режим доступу: https://nuxt.com/

2. Vue.js – The Progressive JavaScript Framework [Електронний ресурс] – Режим доступу: https://vuejs.org/

УДК 621.396.96:006.354:539.171

ІНТЕЛЕКТУАЛЬНИЙ ПОРТАТИВНИЙ ДОЗИМЕТР З ФУНКЦІЄЮ РЕАЛЬНОГО ЧАСУ ТА ДИСТАНЦІЙНОЇ ПЕРЕДАЧІ ДАНИХ

Ігор БОРИСОВ[1], Ростислав ТКАЧУК[1,2], Ольга БАБАДЖАНОВА[2]
[1]Національний університет «Львівська політехніка», м. Львів, Україна
[2]Львівський державний університету безпеки життєдіяльності, м. Львів, Україна

Анотація. *У роботі представлено портативний мікроконтролерний дозиметр іонізуючого випромінювання з мобільною передачею даних для оперативного радіаційного моніторингу. Пристрій на базі СБМ-20, ATmega328P та SIM800L забезпечує вимірювання, обробку, геоприв'язку та передавання результатів у режимі реального часу. Описано архітектуру сенсорної, керуючої та комунікаційної підсистем, а також рішення щодо енергозбереження й стабілізації живлення. Розроблений прототип є автономним, енергоефективним і точним, що робить його придатним для екологічного моніторингу та цивільного захисту.*

Ключові слова: *дозиметр, іонізуюче випромінювання, СБМ-20, ATmega328P; SIM800L, радіаційний моніторинг, мобільна передача даних, мікроконтролерна система, вимірювальний комплекс.*

Abstract*. The paper presents a portable microcontroller-based ionizing radiation dosimeter with mobile data transmission for operational radiation monitoring. The device based on SBM-20, ATmega328P and SIM800L provides measurement, processing, georeferencing and transmission of results in real time. The architecture of the sensor, control and communication subsystems, as well as solutions for energy saving and power stabilization, is described. The developed prototype is autonomous, energy-efficient and accurate, which makes it suitable for environmental monitoring and civil protection.*

Keywords: *dosimeter, ionizing radiation, SBM-20, ATmega328P; SIM800L, radiation monitoring, mobile data transmission, microcontroller system, measuring complex.*

Проблематика забезпечення радіаційної безпеки, особливо в умовах зростання промислових ризиків та екологічних загроз, зумовлює потребу у впровадженні сучасних, доступних і оперативних засобів контролю. Традиційні дозиметричні прилади, попри високу точність, характеризуються значною вартістю, громіздкістю та необхідністю ручного зчитування показників, що обмежує їх ефективність у польових умовах та під час масового моніторингу. Крім того, відсутність можливості оперативної передачі даних у централізовані системи аналізу створює додаткові бар'єри для своєчасного прийняття управлінських рішень [1, 2].

У відповідь на ці виклики запропоновано інноваційну мікроконтролерну систему дозиметра іонізуючого випромінювання з функцією мобільної передачі даних, яка інтегрує процеси вимірювання, обробки та комунікації. Такий підхід дає змогу трансформувати процедури радіаційного моніторингу у складову мережевої інфраструктури контролю довкілля в режимі реального часу [3, 4].

Основним завданням є створення прототипу пристрою, здатного забезпечувати високоточне вимірювання рівня іонізуючого випромінювання в реальному часі, роботу від автономного джерела живлення з мінімальним енергоспоживанням, а також стабільну бездротову передачу результатів на сервер або мобільний застосунок.

У результаті дослідження було сформовано технічну концепцію портативного дозиметра з функцією мобільної передачі даних. Як первинний сенсор обрано газорозрядну трубку SBM-20, що відзначається достатньою чутливістю, точністю вимірювань та низьким енергоспоживанням [5, 6].

Проєктування апаратно-програмного комплексу моніторингу радіаційного фону ґрунтується на поетапному формуванні функціональної та принципової схем дозиметра іонізуючого випромінення, що забезпечують узгоджену роботу сенсорного, вимірювального та комунікаційного модулів. Основою сенсорної підсистеми є газорозрядний лічильник СБМ-20, вибраний завдяки високій чутливості, стабільності параметрів і широкому діапазону енергій реєстрованого β- та γ-випромінення. Для його живлення реалізовано високовольтний перетворювач зі схемою множення напруги на діодно-конденсаторному каскаді, підсилений системою зворотного контролю для стабілізації вихідної напруги у межах 380–420 В. Такий підхід дозволяє уникнути застосування зовнішніх високовольтних сенсорів і суттєво підвищує надійність роботи. Окремо передбачено логіку захисту від перенапруги та короткого замикання, а також фільтраційні LC-ланцюги для зменшення високочастотних завад.

Цифрове ядро комплексу побудовано на мікроконтролері ATmega328P, який виконує детекцію імпульсів з лічильника, обчислення миттєвих та усереднених показників потужності дози, керування режимами роботи та обробку сигналів периферійних модулів. Принципова схема передбачає окремі гілки живлення для аналогової та цифрової частин із застосуванням розв'язувальних конденсаторів, стабілітронів та RC-фільтрів, що мінімізує вплив імпульсних завад від перетворювача на точність вимірів. Для індикації використано OLED-дисплей із інтерфейсом I2C, що зменшує кількість шинах з'єднань і забезпечує хорошу читаність у різних умовах освітленості. Тактильна та звукова індикація реалізована через MOSFET-ключі, що дає змогу керувати навантаженням із низькими втратами та забезпечує тривалу роботу від акумулятора.

Живлення комплексу здійснюється від Li-ion акумулятора, а схема заряджання на мікросхемі TP4056 забезпечує контроль струму та напруги зарядження, захист від перерозряду й перегріву. Впроваджено додатковий вузол моніторингу напруги батареї з АЦП-контролем у режимі реального часу для своєчасного попередження користувача про критичні рівні заряду. Принципова схема дозволяє інтегрувати додаткові елементи енергозбереження — зокрема, керування живленням периферії, переведення мікроконтролера у сплячі режими та відключення високовольтного перетворювача за відсутності потреби у вимірюванні.

Комунікаційна підсистема представлена модулями GPS NEO-6M та GSM SIM800L, підключеними через окремі UART-інтерфейси, що запобігає конфліктам при передачі даних і забезпечує стабільну роботу в умовах нестабільного зв'язку. GPS модуль забезпечує геоприв'язку кожного вимірювання, що підвищує інформативність моніторингу та дозволяє формувати просторові карти радіаційного фону. GSM-модуль забезпечує передачу даних на сервер моніторингу, надсилання SMS-сповіщень про перевищення допустимих значень дози та можливість дистанційного керування режимами роботи пристрою. У схемі передбачено окремий DC-DC перетворювач для стабілізації живлення SIM800L, оскільки модуль має пікові струми до 2 А під час передачі.

Узгоджена робота сенсорного, керуючого та комунікаційного модулів забезпечує створення автономного, енергоефективного та масштабованого апаратно-програмного комплексу, здатного виконувати безперервний контроль радіаційного фону, оперативно повідомляти про критичні відхилення та передавати дані для подальшої аналітики у центральні системи моніторингу. Така архітектура відповідає вимогам сучасних екологічних, промислових та кризових систем безпеки, забезпечуючи точність, надійність та можливість гнучкого розширення функціоналу.

Запропонований мобільний дозиметр, можезабезпечувати точне вимірювання радіаційного фону та надійну передачу даних через GSM. Компоненти SBM-20, ATmega328P та SIM800L здатні забезпечити ефективну й стабільну роботу. Запропонована система є сучасним технічним рішенням із високим рівнем надійності, точності та практичної значущості для задач контролю радіаційного фону.

Література

1. Кнобельс, П. І. (2020). Методи вимірювання радіаційного фону: теорія та практика. Київ: Наукова думка.

2. Sikora L., Lysa N., Tkachuk R., Fedevych O. Informational and Procedural Description of an Energy-active Control Object Behavior Under Active Threats Conditions. CEUR Workshop Proceedings, 2023, 3373, pp. 507–517.

3. Резник, В. М. (2017). Безпроводова передача даних для систем моніторингу: теорія, методи, реалізація. Львів: ЛНУ.

4. IOT Alliance (2020). NB-IoT: A Low Power, Wide Area Network for IoT. Retrieved from: https://iotalliance.org/nb-iot/

5. Lee, J. H., & Park, H. J. (2017). Wireless data transmission technologies for remote environmental monitoring systems. Journal of Applied Remote Sensing, 11(3), 112-128.

6. Петрович А., Ткачук Р, Івануса А., Ткач М. IT-моделі управління проектами безпеки на інфраструктурних об'єктах. Challenges and Opportunities in Modem Scientific Research : зб. наукових праць 1-ї Міжнародної науково-практичної конференції. (Івано-Франківськ, 19-21 лютого 2025 р.) С. 103–105. DOI: https://doi.org/10.70286/isu-19.02.2025

UDC 004.8

APPLICATION OF MACHINE LEARNING FOR STUDYING EVACUATION PARAMETERS FROM PRESCHOOL EDUCATIONAL INSTITUTIONS WITH INCLUSIVE GROUPS

Volodymyr BROSHKO, Oleksandr KHLEVNOI
Lviv State University of Life Safety

Ensuring safe and timely evacuation from preschool educational institutions (PEIs) has become particularly important in the context of increasing technogenic, natural, and military threats. Evacuation planning is especially complex in PEIs with inclusive groups, where children with musculoskeletal disorders, visual or hearing impairments, autism spectrum disorders, intellectual disabilities, and other special educational needs are present. Such children require individualized support, adult assistance, and adapted movement conditions, which significantly affect evacuation parameters.

Traditional approaches to evacuation analysis are mainly based on regulatory calculations and simplified scenarios that do not fully account for the diversity of children's behavioral patterns, the human factor, and the specific characteristics of inclusive environments. In this regard, the application of machine learning methods represents a promising direction for comprehensive analysis and prediction of evacuation parameters under real operating conditions of PEIs.

The purpose of this study is to develop approaches for applying machine learning methods to analyze and assess evacuation parameters from preschool educational institutions with inclusive groups.

To achieve this purpose, the following objectives are defined: – to analyze the specific features of evacuating preschool children with inclusive educational needs; – to identify key evacuation parameters that can be addressed using machine learning; – to substantiate the feasibility of applying machine learning algorithms for modeling evacuation processes; – to outline potential data sources and data processing methods; – to determine prospects for applying the obtained results in the design and operation of PEIs.

Evacuation of preschool children is characterized by limited independent mobility skills, increased stress levels, and the need for continuous supervision by educators. In inclusive groups, these factors are compounded by additional constraints, including reduced movement speed, the use of assistive devices (wheelchairs, walkers), the need for individual support, and heightened sensitivity to noise and crowding.

These factors lead to uneven evacuation flows, the formation of local congestion zones, increased evacuation time, and higher risks to children's life and health.

Evacuation Parameters as Objects of Machine Learning. The main evacuation parameters that can be studied using machine learning include total and partial evacuation time, movement speed of different categories of children, pedestrian flow density, evacuation route capacity, the influence of architectural and planning solutions, the number and spatial distribution of support staff.

Machine learning makes it possible to identify hidden relationships between these parameters that are difficult or impossible to determine using analytical methods.

Within the framework of the study, it is proposed to use regression algorithms to predict evacuation time, clustering methods to identify typical behavioral scenarios, and neural networks to model complex nonlinear relationships between evacuation parameters. Input data may include observation results, video analysis of evacuation drills, sensor data, and outputs from computer-based evacuation simulations.

Special attention should be paid to the use of computer vision techniques for automated determination of movement speed, trajectories, and crowd accumulation zones during evacuation.

The results of applying machine learning can be used to optimize evacuation plans, justify the required number of support staff, improve architectural solutions, and enhance the safety of children with special educational needs. The developed models may also serve as a basis for creating intelligent decision-support systems in the field of civil protection and fire safety for PEIs.

Conclusions. The application of machine learning methods opens new opportunities for studying evacuation parameters from preschool educational institutions with inclusive groups. The integration of information technologies into evacuation analysis contributes to improved safety levels, adaptation of the environment to the needs of each child, and the development of scientifically grounded solutions in the design and operation of PEIs.

References

1. Khlevnoy, O. V., Kharyshyn, D. V., & Nazarovets, O. B. (2020). Problems of calculating the time of evacuation in case of fires in preschool and secondary education institutions with inclusive groups. Fire Safety, 29, 136–141. https://doi.org/10.32447/20786662.37.2020.11

2. Khlevnoi, Oleksandr & Burak, Nazarii & Borzov, Yurii & Raita, Diana. (2022). Neural Network Analysis of Evacuation Flows According to Video Surveillance Cameras. 10.1007/978-3-031-16203-9_35.

004.94:614.876:351.862

РОЗРОБКА СЕРЕДОВИЩА ДЛЯ ВИЗНАЧЕННЯ ВІДПОВІДНОСТІ ЗАХИСНИХ СПОРУД СТУПЕНЮ ЗАХИСТУ ВІД РАДІАЦІЇ

Назарій БУРАК, Євген КОБКО,
Андрій ГАВРИЛЮК, Вікторія ПРИДАТКО
Львівський державний університет безпеки життєдіяльності,
Національна академії внутрішніх справ

Abstract. *The development of a software and information environment for determining the compliance of protective structures with the level of protection against ionizing radiation is considered. The environment provides automated processing of structural parameters, taking into account their design characteristics and regulatory requirements. The application of the proposed approach increases the efficiency and objectivity of assessment and facilitates informed decision-making in the field of civil protection and radiation safety.*

Keyword. *protective structures, radiation protection, ionizing radiation, software environment, automated assessment, civil protection*

Анотація. *Розглянуто розробку програмно-інформаційного середовища для визначення відповідності захисних споруд ступеню захисту від іонізуючого випромінювання. Середовище забезпечує автоматизовану обробку параметрів споруд з урахуванням їх конструктивних характеристик і нормативних вимог. Застосування запропонованого підходу підвищує оперативність та об'єктивність оцінювання і сприяє прийняттю обґрунтованих рішень у сфері цивільного захисту та радіаційної безпеки.*

Ключові слова. *захисні споруди, радіаційний захист, іонізуюче випромінювання, програмне середовище, автоматизована оцінка, цивільний захист.*

У сучасних умовах, де загроза радіаційних аварій залишається актуальною, питання цивільного захисту набуває особливого значення. Аварії на атомних електростанціях, ядерні випробування та використання радіоактивних матеріалів у промисловості змушують розробляти ефективні засоби захисту населення. Одним із ключових аспектів є протирадіаційні укриття, здатні зменшити вплив іонізуючого випромінювання.

Для оцінки ефективності укриттів використовуються спеціальні методики, що враховують характеристики матеріалів, товщину стін та геометричні параметри. Однак традиційний підхід до розрахунків часто вимагає значних зусиль і часу, а також підвищує ризик помилок. Використання нормативних документів, таких як ДБН В.2.2-5:2023, потребує складних математичних обчислень, що уповільнює процес і може вплинути на безпеку. (рис.1)

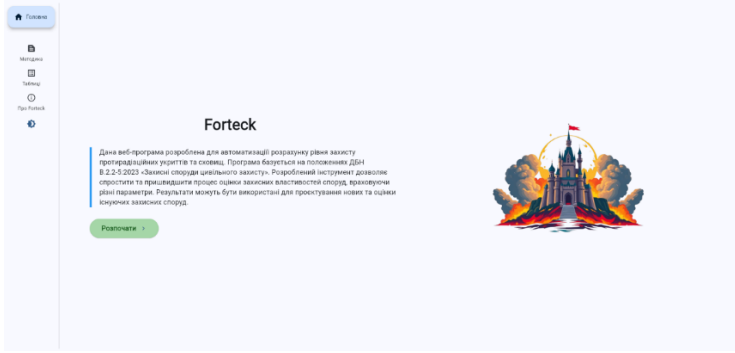

Рисунок 1 – Головна сторінка Forteck

Таким чином виникає потреба в автоматизованому інструменті, який дозволить швидко та точно визначати рівень захисту укриттів. Веб-застосунок може значно спростити процес аналізу, виконуючи обчислення на основі введених параметрів. У надзвичайних ситуаціях, коли часу обмаль, такий підхід дозволяє оперативно приймати рішення, уникнувши помилок, пов'язаних із людським фактором (рис. 2).

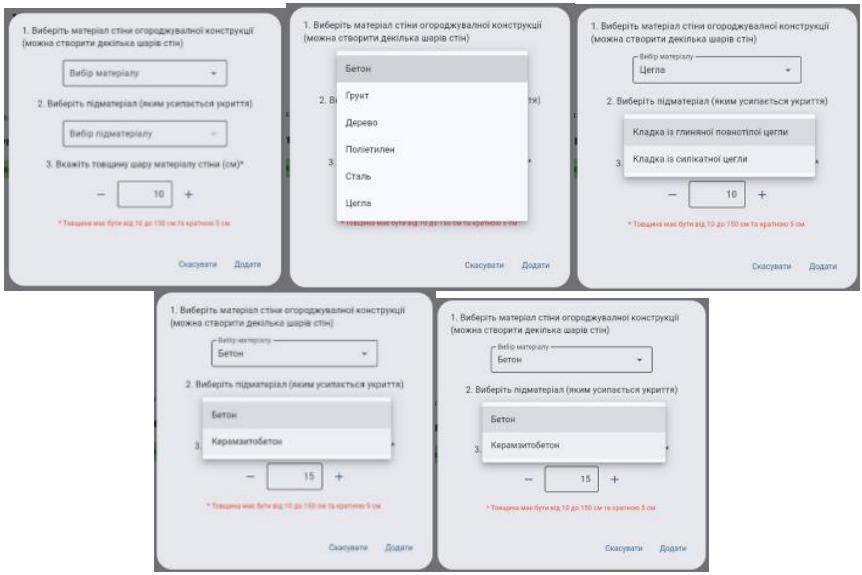

Рисунок 2 – Введення даних типу матеріалів та товщини

Розробка веб-застосунку має низку переваг: доступність для користувачів, централізоване оновлення алгоритмів та можливість інтеграції з іншими базами даних. Автоматизований підхід мінімізує людський фактор, забезпечує об’єктивні результати та економить час, що дозволяє оперативно реагувати на зміни ситуації.

Запропоноване програмне забезпечення може використовуватися працівниками ДСНС України, місцевих адміністрацій та власниками об'єктів критичної інфраструктури для швидкої оцінки рівня захисту укриттів, виявлення слабких місць та прийняття рішень щодо їх модернізації. Це підвищить оперативність і ефективність заходів із захисту населення в умовах радіаційної небезпеки.

Література

1. Martyn, Y., Smotr, O., Burak, N., Prydatko, O., Malets, I. (2020). Software for Shelter’s Fire Safety and Comfort Levels Evaluation. In: Babichev, S., Peleshko, D., Vynokurova, O. (eds) Data Stream Mining & Processing. DSMP 2020. Communications in Computer and Information Science, vol 1158. Springer, Cham. https://doi.org/10.1007/978-3-030-61656-4_31

2. Придатко, О. В., Бурак, Н. Є., Дзень, В. Є., & Кунинець, М. С. (2020). Адаптивна інформаційно-довідкова система "UniBell" як складова частина проєкту "Smart-університет". Scientific Bulletin of UNFU, 30(5), 105-113. https://doi.org/10.36930/40300518

3. ДБН В.2.2-5:2023. Захисні споруди цивільного захисту. Чинний від 01.11.2023. Київ : Міністерство розвитку громад, територій та інфраструктури України, 2023. [Електронний ресурс]. Режим доступу: https://e-construction.gov.ua/laws_detail/BN01:9096-0455-6544-5353?doc_type=2

4. Яковчук Р. Я., Придатко В. В. Оптимізація розташування захисних споруд для забезпечення безпеки населення в умовах війни: аналіз основних вимог // Матеріали Всеукраїнської студентської наукової конференції «84-LYSICon». Львів : Львівський національний медичний університет імені Данила Галицького, 2024. С. 44.

УДК 378:32.019.5

ПІДГОТОВКА СТУДЕНТІВ ЗВО ДО ПРОТИДІЇ ІНФОРМАЦІЙНІЙ АГРЕСІЇ ТА ДЕЗІНФОРМАЦІЇ В СУЧАСНИХ УМОВАХ

Юрій ВІНТЮК
Львівський державний університет безпеки життєдіяльності

Анотація. *Висвітлено особливості налагодження підготовки студентів ЗВО до протидії інформаційній агресії та дезінформації. Описано триетапну позанавчальну програму, що охоплює мотиваційний блок, теоретичні основи (логіка, критичне мислення) та практичні навички (перевірка достовірності інформації). Обґрунтовано необхідність інтеграції цієї роботи у навчальні плани для формування громадянської позиції та досягнення перемоги в інформаційній війні. Зроблено висновок з проведеної роботи.*

Ключові слова: *вища освіта, інформаційна війна, дезінформація, протидія інформаційним впливам, студентське середовище, критичне мислення.*

Abstract. *The features of the preparation of students of higher education institutions to counteract information aggression and disinformation are highlighted. A three-stage extracurricular program is described, which includes a motivational block, theoretical foundations (logic, critical thinking) and practical skills (verification of the reliability of information). The need to integrate this work into curricula for the formation of a civic position and achieving victory in the information war is substantiated. A conclusion is drawn from the work carried out.*

Key words: *higher education, information war, disinformation, counteraction to information influences, student environment, critical thinking.*

Ефективна протидія інформаційній агресії та дезінформації в даний час є важливою умовою не лише припинення війни в Україні, а й підвищення безпеки і збереження єдності європейської та світової спільноти загалом. З огляду на це важливо задіяти відповідні можливості для протидії ворожим інформаційним впливам, для чого потрібно мати не лише належні теоретичні та практичні напрацювання в цьому напрямку, контингент фахівців, які б займалися їхнім застосуванням і поширенням, але й відповідні державні та міжнародні програми для їхньої розробки, впровадження та підтримки. Це зумовлює доцільність розгляду питань, що виникають при організації протидії інформаційній агресії та дезінформації.

Мета дослідження: висвітлити особливості налагодження діяльності з протидії інформаційній агресії та дезінформації в сучасних умовах у студентському середовищі.

Дана тема, що набула особливої важливості протягом останніх років, не раз перебувала в центрі уваги науковців, вітчизняних зокрема [1 - 9]. Проте розпочинати все одно доводиться з проведення власних розвідок і застосування відповідних методів роботи зі студентами. Значно ускладнює роботу в цьому напрямку те, що в навчальних програмах підготовки фахівців немає навчального предмету, в межах якого можна було б проводити цю роботу. Тому

розпочати її довелося спочатку з бажаючими, які виявили цікавіть до даної теми – у вільний від основних навчальних занять час – на рівні гуртка відповідного спрямування, в межах діяльності Студентського наукового товариства. Діяльність у цьому напрямку було проведено в три етапи, кожен з яких був відповідним забезпеченням для наступного.

1 ЕТАП. ***Інформаційно-мотиваційний блок.***

Розпочати роботу в цьому напрямку доводиться з формування належної мотивації до занять нею. Для цього доречно надати студентам інформацію про сучасну ситуацію в Україні, проаналізувати її вплив на всі сфери нашого життя, вказати зумовлюючі чинники, прояви та подальші наслідки. Особливості формування мотивації вивчають лише ті здобувачі вищої освіти, що навчаються за спеціальністю «Психологія», з якими доцільно розпочинати роботу, проте навіть із ними початок роботи у цьому напрямку наражається на чималі труднощі. Тому доводиться приступити до послідовного розгляду наступних питань:

- Історія способів і методів ведення інформаційної війни;
- Психологічні способи впливу на супротивника;
- Результати та наслідки інформаційних впливів у конфліктах;
- Інформаційна агресія та дезінформація в сучасному світі.

Лише після того, як здійснено введення в тему, актуалізовано призначення та намічено біжучі завдання, у студентів з'являється інтерес до подальшої роботи в даному напрямку, який, проте, вимагає постійної уваги та подальшого розвитку. Продемонструвати як наявність дезінформації, так і її вплив на цільову аудиторію часто виявляється дуже складно, для цього потрібно мати не лише необхідні як теоретичну, так і практичну підготовку, але й досвід такої діяльності. Тому після задіяння необхідної мотивації необхідно розпочати теоретичну підготовку з опанування способів і методів протидії інформаційній агресії та дезінформації.

2 ЕТАП. ***Теоретична підготовка:***

- Вивчення логіки, аргументації та доказів;
- Розвиток критичного мислення;
- Здійснення психологічного аналізу;
- Особливості сучасної психологічної війни.

Після проведення початкової теоретичної підготовки в даному напрямку слід приступити до освоєння практичних навичок застосування одержаних знань. Інформація, що подається в державних ЗМІ України, проходить належну перевірку на достовірність, тому для пошуку проявів інформаційної агресії да дезінформації в основному використовується інформація з Інтернету на соціальних мереж.

3 ЕТАП. ***Практична підготовка:***

- Способи перевірки достовірності інформації;
- Виявлення ознак дезінформації;
- Розпізнавання намірів ворога;
- Опанування способів протидії.

Студенти, що пройшли навіть початкову підготовку за запропонованою програмою – протягом одного семестру – визнають її корисність не

лише для їхнього особистісного розвитку, передусім формування відповідної громадянської позиції, але а фахового становлення загалом. Все це підтверджує доцільність і перспективність її продовження в майбутньому, зокрема, серед студентів інших спеціальностей. Передбачено також отримати підтримку цього напрямку навчально-виховної роботи у керівництва закладу, створення та впровадження на підставі проведеної роботи відповідного навчального курсу для здобувачів вищої освіти. Все це сприятиме підвищенню протидії агресії ворога і наближенню перемоги.

Висновки. Сучасна війна проти нашої країни розпочалася не з повномасштабного збройного вторгнення у лютому 2022 року, як і не від початку збройної агресії у квітні 2014 року, оскільки все це стало можливим внаслідок здійснення тривалої інформаційної війни, яка триває вже не одне десятиліття, і стало результатом нашої поразки у ній, через відсутність ефективних засобів протидії цій агресії, взагалі відсутність організованого опору їй. Відповідно, нинішня війна припиниться не раніше, ніж буде здобуто перемогу спочатку в інформаційній війні, тобто одержано спочатку психологічну, передусім ідеологічну перемогу над ворогом. А це, у свою чергу, вимагає розробки, широкого розповсюдження і ефективного застосування системи засобів протидії інформаційній агресії та дезінформації.

Література

1. Горун О. Ю. Протидія ворожій медіа-пропаганді в умовах правового режиму військового стану в Україні. *Інформація і право*. 2023. № 1 (44). С. 116–128.

2. Кушнір І. П., Адамчук С. В. Протидія дезінформації: організаційно-правовий аспект. *Аналітично-порівняльне правознавство*. 2025. Випуск 1. С. 470-475.

3. Медіаграмотність як ключ до боротьби з російською пропагандою: виклики та рішення для України. URL: https://media.1plus1.ua/news/mediagramotnist-iak-kliuc-do-borotbi-z-rosiiskoiu-propagandoiu-vikliki

4. Гула Р. В., Дзьобань О. П., Передерій О. Г., Павліченко О. О., Філь Г. О. Інформаційна війна: соціально-онтологічний та мілітарний аспекти : монографія. К.: Каравелла, 2023. 288 с.

5. Почепцов Г. Сучасні інформаційні війни. К.: Вид-во КМА, 2018. 489 с.

6. Рудник Л. І. Поширення недостовірної інформації як засіб ведення гібридних війн. *Інформація і право*. 2024. № 4(51), с. 46–54.

7. Рудь О. В. Медіаграмотність як інструмент протидії інформаційній агресії РФ в умовах війни. *Педагогічний пошук*. 2023. № 4 (120). С. 39-44.

8. Христенко Є. В. Маніпулювання свідомістю в умовах гібридної війни: психологічний аспект. URL: http://repositsc.nuczu.edu.ua/bitstream/123456789/5929/1/Khrystenko_monogr.pdf

9. Як протидіяти дезінформації в Інтернеті. URL: https://kolomyichiska-gromada.gov.ua/news/1734345532/

УДК 004.056

ІНФОРМАЦІЙНІ ЗАГРОЗИ У СУЧАСНОМУ СУСПІЛЬСТВІ ТА ЗАХИСТ ВІД НИХ

Юрій ВІНТЮК
Львівський державний університет безпеки життєдіяльності, м. Львів

Анотація. Розглянуто інформаційні загрози як невід'ємний наслідок *залежності сучасного суспільства від цифрових систем. Визначено їхню класифікацію за аспектами безпеки (конфіденційність, цілісність, доступність) та чинниками (кіберзагрози, дезінформація, соціальна інженерія). Обґрунтовано необхідність комплексного захисту, що охоплює технічні засоби, правові механізми та підвищення інформаційної культури громадян для забезпечення стійкості суспільства.*

Ключові слова: *інформаційні загрози, кібербезпека, інформаційна безпека, дезінформація, соціальна інженерія, комплексний захист, критичне мислення.*

Abstract. *Information threats are considered as an inherent consequence of modern society's dependence on digital systems. Their classification is determined by security aspects (confidentiality, integrity, availability) and factors (cyber threats, disinformation, social engineering). The need for comprehensive protection, which includes technical means, legal mechanisms and improving the information culture of citizens to ensure the sustainability of society, is substantiated.*

Key words*: information threats, cybersecurity, information security, disinformation, social engineering, comprehensive protection, critical thinking.*

Застосування інформаційних технологій у різних сферах життєдіяльності суспільства не лише підвищує продуктивність діяльності, але й повсякчас створює непередбачувані ускладнення. Розвиток інформаційних технологій трансформував суспільство, зробивши його залежним від них; проте ця залежність від цифрових систем і даних породила нові, складні й багатогранні інформаційні загрози. Причому вони стосуються не лише технічної сфери, а й соціальної, економічної та національної безпеки. Ефективний захист від них є пріоритетним завданням для кожної держави, організації та окремої особи. Дана обставина зумовлює актуальність розгляду інформаційних загроз у сучасному суспільстві та захисту від них.

Мета дослідження: розглянути специфіку інформаційних загроз у сучасному суспільстві та можливості захисту від них.

Дана тема неодноразово перебувала в полі уваги науковців, вітчизняних зокрема [1-7]; враховуючи наявні напрацювання, передусім доцільно розглянути найпоширеніші їх види.

1. Класифікація видів інформаційних загроз.

Інформаційні загрози можна класифікувати за різними критеріями, але найчастіше їх поділяють за аспектом безпеки, на який вони спрямовані:

1.1. Аспекти безпеки:

- Конфеденційність: неправомірний доступ до інформації, її витік (наприклад: шпигунські програми, фішинг, зламування баз даних, інсайдерська діяльність).

- Цілісність: несанкціонована зміна або знищення інформації (наприклад: хакерські атаки з метою спотворення даних, віруси-шифрувальники, помилки персоналу).
- Доступність: блокування або унеможливлення санкціонованого доступу до інформації чи систем (наприклад: DDoS-атаки, відмова обладнання, перебої в електропостачанні, мережеві "хробаки").

Наступний критерій класифікації розрізняє їх за зумовлюючими чинниками.

1.2. Технологічні (кіберзагрози)

Це найвідоміші загрози, пов'язані з програмним забезпеченням і мережами:

- Шкідливе ПЗ: віруси, троянські програми, шпигунське ПЗ, програми-вимагачі, які блокують системи або шифрують дані з метою одержання викупу.
- Кібератаки: спрямовані на критичну інфраструктуру, державні установи чи великі корпорації з метою порушення їхньої роботи або крадіжки інформації.

1.3. Соціально-психологічні та політичні

Ці загрози спрямовані на свідомість і стабільність суспільства:

- *Дезінформація та фейкові новини:* поширення неправдивої інформації для маніпулю-вання громадською думкою, створення паніки чи підриву довіри до державних інститутів.
- Інформаційно-психологічні операції: комплексний вплив на суспільну свідомість із метою зміни політичних настроїв, розпалювання ворожнечі та дестабілізації.
- Соціальна інженерія: використання людського фактору (довірливості, неуважності) для отримання доступу до конфіденційних даних (це фішинг-листи, телефонне шахрайство).

2. Захист від інформаційних загроз: комплексний підхід

Як показує наявний досвід протидії інформаційним загрозам, ефективний захист вимагає впровадження заходів на всіх рівнях: технічному, організаційно-правовому й освітньому.

2.1. Технічні та програмні засоби

Це база для протидії більшості кіберзагроз:

- Багаторівневий захист: використання антивірусного ПЗ, міжмережевих екранів, систем виявлення вторгнень.
- Резервне копіювання: регулярне створення копій критично важливих даних для швидкого відновлення після атак чи збоїв.
- Криптографічний захист: шифрування даних, що передаються (наприклад: за допомогою VPN, SSL/TLS), і даних, що зберігаються, для забезпечення конфіденційності.
- Оновлення ПЗ: регулярне встановлення оновлень операційних систем і програм для закриття "дірок" у безпеці.

2.2. Організаційні та правові механізми

Але ні одна технологія не працюватиме без чітких правил і відповідальності:

- Політики безпеки: розробка та неухильне дотримання внутрішніх правил роботи з інформацією, використання паролів і доступу до ресурсів.
- Контроль доступу: впровадження принципу мінімальних привілеїв і двофакторної (або багатофакторної) автентифікації.
- Законодавче регулювання: прийняття та вдосконалення законів у сфері кібербезпеки, захисту персональних даних (наприклад: GDPR в ЄС) і боротьби з кіберзлочинністю.

2.3. Людський фактор та освіта

Людина залишається найслабшою ланкою в системі захисту, тому доцільно задіяти:

- Навчання персоналу – регулярні тренінги з основ інформаційної гігієни, розпізнавання фішингу та правил роботи з конфіденційною інформацією.
- Критичне мислення – розвиток у суспільстві навичок критичного аналізу інформації, перевірки джерел та фактів для протидії дезінформації.
- Культура безпеки – формування відповідального ставлення до власної та корпоративної інформаційної безпеки.

Висновки. Інформаційні загрози в сучасному суспільстві є динамічними, глобальними та комплексними. Вони вимагають не лише постійного вдосконалення технічних засобів захисту, але й формування високої інформаційної культури та критичного мислення у громадян. Захист від цих загроз – це безперервний процес, що включає єдність технологій, законодавства й освітянської роботи. Тільки комплексний підхід, де кожен учасник інформаційного простору усвідомлює свою роль і відповідальність, може забезпечити стійкість і безпеку сучасного суспільства.

Література

1. Виздрик В., Мельник О. Інформаційна безпека в Україні. Grail of Science. 2023. № 24. С. 196-202.

2. Гаврильців М. Т. Інформаційна безпека держави в системі національної безпеки України. *Юридичний науковий електронний журнал*. 2020. № 2. С. 200-203.

3. Залєвська І. І., Удренас Г. І. Інформаційна безпека в Україні в умовах російської військової агресії. *Південно український правничий часопис*. 2022. № 1. С. 20-26.

4. Ільницька У. Інформаційна безпека України: сучасні виклики, загрози та механізми протидії негативним інформаційно-психологічним впливам. *Політичні науки*. 2019. № 1. Вип. 2. С. 27-32.

5. Панченко О. Інформаційна безпека держави як елемент соціокультури. *Аспекти публічного управління*. 2020. № 1. С. 58-67.

6. Уханова Н.С. Правова культура молоді в Україні. *Інформація і право*. 2019. № 2. С. 156-166.

7. Шевчук О.М. Сучасні виклики і загрози в сфері інформаційної безпеки держави. *Актуальні проблеми вітчизняної юриспруденції*. 2024. № 6. С. 160-166.

УДК 004.932.2

MATERIAL SURFACE DEFECTS DETECTION USING DISTRIBUTED AND INVARIANT IMAGE INTENSITY FEATURES

Юрій ВІПШОВСЬКИЙ
Національний університет «Львівська політехніка», Львів

У роботі проведено аналіз алгоритму виявлення поверхневих дефектів металів на основі кумулятивних гістограм інтенсивностей. Метод не потребує навчальних даних і базується на статистичному аналізі зображень. Досягнуто точності понад 83%, що підтверджує придатність методу для практичного використання. Ключові слова: гістограма; аналіз зображень; комп'ютерний зір; штучний інтелект.

The paper presents an improved analysis of a cumulative histogram–based algorithm for detecting surface defects in metallic materials. The method does not require training data and relies on statistical intensity analysis. Achived accuracy over 83%, confirming its suitability for practical use. Keywords: histogram; image analysis; computer vision; artificial intelligence.

Introduction. Defect detection in materials increases product quality and reliability while reducing cost. Automated systems effectively perform this task by minimizing human error. However, existing solutions are often complex and require large amounts of training data. Main idea of proposed approach is based on statistical image analysis that does not require extensive training data and simplifies the system compared to popular neural network-based methods [1]. Proposed algorithm can be applied on production lines for detecting metal surface defects.

Problem statement and goal formulation. The primary objective of this work is to analyze the accuracy of the proposed algorithm for detecting surface defects in materials based on the construction of cumulative histogram visualizations [2]. The research focuses on evaluating how effectively this algorithm identifies defects across various material textures and illumination conditions.

To achieve this, the work involves systematic testing of the algorithm using benchmark datasets containing diverse types of metallic surface defects. The study examines the optimal parameter ranges for practical use in industrial environments.

The analysis further explores the algorithm’s scalability and adaptability to real-time quality inspection systems, where large volumes of high-resolution images must be processed continuously without loss of information. Ultimately, the results are intended to validate the algorithm’s capability to serve as a lightweight, data-independent alternative to complex neural network models in automated defect detection.

Algorithm and software description. The prototype software operates as follows: the user uploads a grayscale image (or converts it to grayscale within the program) to be checked for defects, sets the minimum (MinInt) and maximum intensity (MaxInt), and the allowable deviation (P), and receives a result indicating whether defects are present.

To solve the defect detection problem, algorithm analyzing pixel intensities across rows and columns, followed by the construction of cumulative histograms and their visualizations (formula 1) [2].

$$hist[i][k] = \frac{\sum_{j=0}^{H} 1, if\ (intensity(column, j) = k)}{count(hist[i])} \quad (1)$$

For each row and column, the defect detection algorithm builds N cumulative histograms (formula 2), each representing pixels of a specific intensity.

$$N = (MaxInt - MinInt) \quad (2)$$

As a result, information is obtained about the presence of pixels of each intensity in each row or column (depending on the selected variant of algorithm). Then, a column visualization of the cumulative histogram is created, showing which intensities are present in each column. These visualizations columns are combined into an image used by the algorithm to determine whether defects are present, after identifying the most frequent intensity in the image. If the visualization contains pixels with intensities deviating from the most frequent one by more than the allowed threshold (P), the algorithm reports that defects were detected.

To evaluate the algorithm, two datasets – NEU-DET and GC10-DET – containing images of various defects were used. The algorithm's performance was compared with methods proposed in studies [3,4]. The datasets used in this study lacked defect-free samples, so additional images were created. From the GC10-DET dataset, cropped regions without visible defects were saved in a separate clear folder. From these datasets were formed three sub datasets:

- 300 small images (200×200) images from NEU-DET, manually corrected to remove defects.
- 100 large images (>1000×1000) cropped defect-free images from GC10-DET.
- 100 mixed-resolution images combining both datasets.

These sub datasets were used to evaluate the algorithm's defect detection accuracy across different image scales. To ensure measurement accuracy, 3 experiments were conducted with each detection threshold on each dataset, and the values obtained as a result of the experiments were averaged.

For different allowable deviation (P) results are different, because if P is too small than all images determines as defected even when it was just small

difference in metal texture, but if P is too big all images becomes undefected even if they have a magore defect. Best results for each are combined to table 1.

Table 1

Dataset	TP	TN	FP	FN	Precision	Recall	F1	Accuracy
300 small images	249	45	5	1	98.03%	99.6%	98.81%	98%
100 large images	69	17	13	1	84.15%	98.57%	90.78%	86%
100 mixed images	49	34	16	1	75.38%	98%	84.11%	83%

As we can see from this table results for small images are very good, that is because on small image the lighting is uniform and we can focus even on small differences between main intensity and intensities of pixels. However, when picture is big and it is taken from big material surface it is harder to determine main intensity as on different parts of material we have a different lighting. This is the main reason why accuracy become smaller.

Results.

- Created undefected images and sub datasets with different images
- Analyzed defect detection accuracy. Get up to 98% accuracy for small images, up to 86% for big images and up to 83% for images with different sizes

Conclusions. The study confirmed that the proposed cumulative histogram–based algorithm effectively detects surface defects without using training data, achieving up to 98% accuracy on small images and around 83–86% on larger ones. Its simplicity, speed, and adaptability make it suitable for real-time industrial quality control applications.

References

1. Сторожик Д. Технології опрацювання зображень на основі комплексування даних (Огляд) [Електронний ресурс] / Д. Сторожик, А. Протасов // Технічна діагностика та неруйнівний контроль. – 2022. – Т. 2022, № 4. – С. 17–26.

2. R. Melnyk and Y. Vipshovskyi // The Detection of the Surface Defects in Materials by Distributed and Invariant Features of Image Intensity // 2024 IEEE 19th International Conference on Computer Science and Information Technologies (CSIT) - Lviv, Ukraine – 2024. - pp. 1-5.

3. Zhang C. [et al.] Multilayer feature extraction of AGCN on surface defect detection of steel plates // Computational intelligence and neuroscience. – 2022. – Vol. 2022. – P. 1–13

4. Lv X. [et al.] Deep Metallic Surface Defect Detection: The New Benchmark and Detection Network // Sensors 2020. – Vol. 20, no. 6. – P. 1562.

УДК 004.9

МОДЕЛІ ТА ПІДХОДИ ДО АВТОМАТИЗАЦІЇ УПРАВЛІНСЬКИХ РІШЕНЬ В ІТ-ПРОЄКТАХ

Войніков Н.А
Національний університет «Одеська політехніка», Одеса

У тезі розглянуто основні моделі та підходи до автоматизації управлінських рішень в ІТ-проєктах. Проаналізовано аналітичні, оптимізаційні, симуляційні та машинні моделі, визначено їх роль у підвищенні ефективності менеджменту та забезпеченні обґрунтованого прийняття рішень. Ключові слова: автоматизація рішень, ІТ-проєкти, моделі управління, оптимізація, машинне навчання, симуляція, СППР.

The thesis considers the main models and approaches to automating management decisions in IT projects. Analytical, optimization, simulation and machine models are analyzed, their role in increasing management efficiency and ensuring informed decision-making is determined. Keywords: decision automation, IT projects, management models, optimization, machine learning, simulation, DSS.

Ефективне управління ІТ-проєктами потребує швидкого та обґрунтованого прийняття рішень у ситуаціях невизначеності, високої змінності вимог, обмежених ресурсів та жорстких часових рамок. Класичні методи менеджменту часто не враховують величезні обсяги даних і складних взаємозв'язків між параметрами проєкту, що зумовлює потребу впровадження автоматизованих систем підтримки прийняття рішень (СППР). Такі системи базуються на математичних моделях, алгоритмах та аналітичних підходах, покликаних підвищити точність прогнозів, швидкість оцінювання ситуацій та об'єктивність управлінських дій.

Одним з ключових підходів до автоматизації управлінських рішень є використання аналітичних моделей, що включають теорію рішень, імовірнісні методи, моделі ризик-менеджменту та методи багатокритеріальної оптимізації. Наприклад, метод аналізу ієрархій (AHP) дозволяє структурувати складні управлінські проблеми та визначати вагомість критеріїв при виборі альтернатив. У свою чергу методи нечіткої логіки застосовуються для моделювання суб'єктивних факторів, що важко піддаються формальній оцінці, таких як експертні судження або якість комунікацій у команді [1].

Другим важливим напрямом є застосування математичних моделей оптимізації, які дозволяють знаходити найефективніші рішення щодо розподілу ресурсів, планування завантаження команди, побудови графіків та визначення критичних шляхів. Алгоритми лінійного та цілочисельного програмування здатні автоматизувати процеси планування спринтів, формування roadmap або оцінювання ризику перевантаження ресурсів. Такі

моделі широко використовуються у системах корпоративного планування, де точність і швидкість обчислень мають вирішальне значення [2].

Окреме місце серед інструментів автоматизації займають моделі машинного навчання, які дозволяють аналізувати історичні дані та формувати рекомендації на основі попередніх патернів. Регресійні моделі забезпечують прогнозування строків виконання задач і тривалості спринтів, класифікаційні алгоритми визначають ризикові задачі, а моделі кластеризації допомагають формувати збалансовані команди за компетенціями. Використання ML-моделей сприяє переходу до адаптивних систем управління, у яких рішення базуються на даних, а не тільки на досвіді менеджера [3].

Важливо також зазначити широке застосування симуляційних моделей, таких як моделювання Монте-Карло, системна динаміка та моделювання дискретних подій. Вони дозволяють проаналізувати розвиток проєкту під впливом різних сценаріїв, оцінити стійкість планів, протестувати альтернативні стратегії та визначити ймовірні точки відхилень. Симуляційні моделі особливо ефективні у комплексних проєктах, де взаємодіє багато змінних і де важко передбачити наслідки управлінських рішень традиційними методами.

Сучасні СППР для ІТ-проєктів часто комбінують різні підходи, утворюючи гібридні моделі. Наприклад, системи прогнозування продуктивності команди можуть поєднувати статистичні моделі з алгоритмами машинного навчання, а модулі оптимізації — інтегруватися з симуляціями для уточнення результатів. Такий підхід забезпечує більш високу точність, гнучкість та здатність адаптуватися до унікальних умов проєкту.

Отже, використання моделей і підходів до автоматизації управлінських рішень у ІТ-проєктах сприяє значному підвищенню ефективності управління, знижує ризики та забезпечує кращу прогнозованість результатів. Інтеграція аналітичних, оптимізаційних, симуляційних та машинних моделей у системи підтримки прийняття рішень формує основу для розвитку інтелектуального проєктного менеджменту, у якому людські рішення доповнюються об’єктивними даними та алгоритмічними обчисленнями.

Література

1. Сидоренко В. М., Козлова О. П. Моделювання управлінських рішень : навч. посіб. Київ : КНЕУ, 2021. 284 с.

2. Kerzner H. Project Management: A Systems Approach to Planning, Scheduling, and Controlling. 12th ed. Hoboken : John Wiley & Sons, 2017. 816 p.

3. Larson E. W., Gray C. F. Project Management: The Managerial Process. 7th ed. New York : McGraw-Hill Education, 2021. 680 p.

УДК 004.42

РОЗРОБКА МОБІЛЬНОГО ДОДАТКУ НА ПЛАТФОРМІ ANDROID ДЛЯ КООРДИНАЦІЇ ЕВАКУАЦІЙНИХ ЗАХОДІВ ТА ВОЛОНТЕРСЬКОЇ ДОПОМОГИ НА ТЕРРИТОРІЇ БОЙОВИХ ДІЙ

Юрій ВОЙТОВИЧ, Юлія НАЗАР
Львівський державний університет безпеки життєдіяльності

Описано підхід до створення мобільного додатку для підтримки цивільних і волонтерів у районах бойових дій. Використання Java та стандартних засобів Android забезпечує роботу на малопотужних пристроях, в офлайн-режимі та зі збереженням безпеки даних завдяки вбудованому модулю шифрування.
Ключові слова: *мобільний додаток, евакуація, волонтерська допомога, шифратор, енергоефективність, безпека даних.*

The paper describes an approach to developing a mobile application supporting civilians and volunteers in combat zones. Using Java and native Android tools enables operation on low-performance devices, offline functionality, and secure data handling through integrated encryption.
Keywords: *mobile application, evacuation, volunteer assistance, encryptor, energy efficiency, data security.*

У період активних бойових дій одним із ключових ресурсів є оперативна та достовірна інформація: про безпечні маршрути, пункти призначення та потреби цивільного населення (де безпечно?, куди їхати?, кому потрібні ліки?). Стандартні месенджери (наприклад, Telegram чи Viber) не забезпечують належного структурування повідомлень, швидко перевантажуються інформацією та ускладнюють пошук критично важливих даних. Тому виникає потреба у спеціалізованому мобільному додатку, який забезпечуватиме впорядковану обробку заявок та маршрутів.

Основною вимогою до такого додатку є його «легкість», тобто здатність працювати на малопотужних або застарілих пристроях, мінімізувати споживання енергоресурсів та забезпечувати функціонування навіть при відсутності стабільного інтернет-з’єднання. Саме тому для розробки обрано мову Java та стандартні засоби Android, що дозволило відмовитися від ресурсоємних сторонніх бібліотек. Сучасні додатки часто створюються як конструктор з багатьох готових деталей (бібліотек). Це пришвидшує розробку, але робить програму "важкою", що підвищує вимоги до апаратних ресурсів і погіршує продуктивність на слабких пристроях.

У зоні ведення бойових дій користувачі можуть тривалий час не мати доступу до джерел живлення для підзарядки мобільних пристроїв. У

зв’язку з цим розробка здійснюється із застосуванням стандартних механізмів Android, орієнтованих на мінімальне споживання енергії, зокрема:

- програма не виконує зайвих дій у фоновому режимі;
- без зайвих налаштувань, додаток реагує миттєво навіть на слабких телефонах;
- чим менше сторонніх деталей, тим менше шансів, що щось зламається.

Зв'язок на фронті або на тимчасово окупованих територіях може бути нестабільним і з’являтися лише епізодично. Тому робота застосунку побудована за принципом "спочатку запиши — потім відправ". Уся інформація (зокрема списки на евакуацію чи потреби в медикаментах) фіксується у внутрішній базі даних пристрою, що дозволяє користувачеві формувати заявки навіть у повній відсутності зв’язку. Як тільки з’являється хоча б мінімальний доступ до мережі, додаток автоматично та невеликими порціями передає накопичені дані на сервер і завантажує нові інструкції.

Використання повноцінних онлайн-карт вимагає високошвидкісного інтернету, що у таких умовах, як правило, недоступно. Тому реалізовано спрощений підхід: картографічні матеріали завантажуються заздалегідь у вигляді статичних зображень або схем. Визначення геолокації також здійснюється енергоощадно — замість постійного звернення до супутників відстеження координат виконується рідко або лише за ініціативою користувача, наприклад для підтвердження точки збору.

Інформація щодо місцеперебування цивільних осіб або волонтерів має високий рівень критичності, оскільки у разі її перехоплення противником може становити безпосередню загрозу життю та безпеці людей. Тому передача таких даних у відкритому вигляді є неприпустимою. У мобільному додатку реалізовано спеціалізований модуль — Шифратор. Він перетворює дані на зашифрований формат ще до їх збереження у пам’яті пристрою. Аналогічний підхід застосовується і під час передавання інформації через мережу — дані надсилаються виключно у зашифрованому вигляді. Ключі для розшифрування доступні лише уповноваженим координаторам на сервері та безпосередньо користувачу, що унеможливлює відновлення інформації навіть у випадку втрати або викрадення пристрою сторонніми особами.

Функціонування додатку передбачає можливість його використання у стресових та екстремальних умовах, коли користувач може перебувати під обстрілами, у транспорті на пошкоджених дорогах або зазнавати фізичних обмежень (наприклад, тремтіння рук чи робота в рукавицях). Тому інтерфейс має бути максимально спрощеним і зручним для швидкої взаємодії: великі елементи керування, що легко натискаються навіть у несприятливих умовах; контрастне колірне оформлення (наприклад, чорний текст на світлому фоні або навпаки) для забезпечення читабельності при

поганому освітленні; мінімум текстових пояснень. Замість розгорнутих описів використовуються короткі та однозначні статуси на кшталт "Потрібна евакуація", "Є місця", "Виїхав", що дозволяє пришвидшити інтерпретацію інформації та прийняття рішень.

Як висновок, створення мобільного застосунку, орієнтованого на використання в умовах бойових дій, насамперед передбачає пріоритет функціональності та надійності над візуальною привабливістю. Застосування стандартних засобів Java і платформних механізмів Android дозволяє розробити стійке програмне рішення, здатне забезпечувати роботу навіть у ситуаціях, коли сучасні ресурсоємні додатки втрачають працездатність. Це сприяє підтримці безперервної комунікації між волонтерами та постраждалими, що є критично важливим для оперативного реагування й порятунку людей у надзвичайних ситуаціях.

Література

1. Android Developers Documentation: Guides and API Reference [Електронний ресурс]. – Режим доступу: https://developer.android.com.

2. Android Developers. App Perfomance Guide [Електронний ресурс]. – Режим доступу: https://developer.android.com/topic/performance/overview.

3. Joshua Bloch Effective Java. Addison-Wesley Professional, 2018.

4. Kordunova Y., Prydatko O., Smotr O., Golovatyi R. Expert Decision Support System Modeling in Lifecycle Management of Specialized Software. Lecture Notes on Data Engineering and Communications Technologies, Springer, Switzerland. Vol. 149, 2022, pp. 367-383, https://doi.org/10.1007/978-3-031-16203-9_22

УДК 004.43

COMPARATIVE ANALYSIS OF AUTOMATED WEB DATA EXTRACTION TOOLS IN THE PYTHON ENVIRONMENT

Andrii HAVRYLIUK
Lviv State University of Life Safety

Анотація. *Робота аналізує інструменти автоматизованого збору даних (web scraping) у середовищі Python, оцінюючи їхню ефективність при роботі зі статичним та динамічним контентом. Розглянуто архітектурні відмінності між підходами на основі HTTP-запитів та повної емуляції браузера на прикладі бібліотек Beautiful Soup, Scrapy та Selenium. Запропоновано рекомендації для вибору оптимального стеку технологій залежно від обсягу даних та складності веб-інтерфейсу цільового ресурсу.*

Ключові слова: *мова програмування Python, веб-скрапінг, парсинг даних, Beautiful Soup, Scrapy, Selenium, автоматизація збору даних.*

Abstract. *This paper analyzes automated web data extraction tools (web scraping) within the Python environment, evaluating their effectiveness in handling static and dynamic content. The study examines architectural differences between HTTP-request-based approaches and full browser emulation, focusing on libraries such as Beautiful Soup, Scrapy, and Selenium. Recommendations are provided for selecting the optimal technology stack based on data volume and the complexity of the target web interface.*

Keywords: *Python programming language, web scraping, data parsing, Beautiful Soup, Scrapy, Selenium, data collection automation.*

Today, data is very important for everything: business, machine learning, and science. The internet is developing very quickly, so it is impossible to collect data manually. This requires automated methods. This is called ‘web scraping.’ Python is the most popular language for this because it is easy to use and has a lot of good tools.

However, modern websites are changing. They used to be simple HTML pages. Now they are complex applications that use a lot of JavaScript. This makes web scraping more difficult. Developers have to choose between two methods. The first method uses simple HTTP requests. It is fast but cannot ‘see’ everything on the pages. The second method uses browser automation. It acts like a real user, but it is slow and uses a lot of computing power. The purpose of this article is to compare three popular Python tools: Beautiful Soup, Scrapy, and Selenium. We will see which one is best suited for different tasks.

To understand which tool is best, we will consider three things:

1. Performance: how fast the tool works and how much memory it needs.
2. Dynamic content: can the tool read data that appears after the page loads (using JavaScript)?
3. Ease of Use: Is it easy to learn? Can it handle big projects?

Beautiful Soup (with Requests) is a library for simple projects. It helps read code from a web page and find specific data. When we use it together with the requests library, it works very quickly and easily. It is great for simple static websites. But it has a big problem: it cannot execute JavaScript. If a website uses JavaScript to display data, Beautiful Soup cannot see it. Therefore, it is only suitable for simple pages.

Scrapy is different. It is not just a library, but a full-fledged framework. It is designed to load many pages simultaneously. Scrapy is very fast for large tasks because it performs many operations simultaneously. It has tools for saving data and controlling download speed. On its own, it cannot execute JavaScript. But you can add plugins (such as Scrapy-Splash) to fix this. The downside is that Scrapy is more difficult to learn. It may be too complex for small scripts.

Selenium is actually a tool for testing websites. But people use it for scraping because it controls a real web browser (e.g., Chrome). Selenium can do almost anything. It opens a real browser, so it sees exactly what the user sees. It easily deals with JavaScript, cookies and login forms. However, it is very slow. It uses a lot of CPU and RAM resources. It is suitable for complex websites, but not if you need to download thousands of pages really quick.

We should also talk about new tools. Selenium is outdated. Many developers now prefer Microsoft's Playwright. It is pretty faster and more stable than Selenium. It interacts directly with the browser engine, so it works better with modern web features.

In addition, there is a real problem: websites try to block bots. Scraping is not just downloading HTML. Many sites check if you are a robot. Simple tools like Beautiful Soup are really easy to block. Even Selenium can be detected. Developers have to be smart to hide their bots. They use special plugins to look like real people. This makes scraping much more complicated than just writing code.

In summary, there is no perfect tool for everything. It all depends on the website and the amount of data you need to gather.

Beautiful Soup is perfect for newbies or simple static gigs where you want to get in and out fast. Scrapy is your pick for pro-level, high-volume setups that need to be solid and fast. Selenium (or newer options like Playwright) is a must for those wild, JavaScript-heavy apps, even if it slows things down. Getting these pros and cons lets devs whip up smarter, easier-to-maintain scraping systems.

References

1. Richardson L. (2023). Beautiful Soup Documentation. Crummy: The software that powers this site. URL: https://www.crummy.com/software/BeautifulSoup/bs4/doc/

2. Scrapy Developers. Scrapy 2.11 Documentation. Scrapy.org. URL: https://docs.scrapy.org/en/latest/

3. Selenium Project. (2024). The Selenium Browser Automation Project. Selenium.dev. URL: https://www.selenium.dev/documentation/

4. Real Python. A Practical Introduction to Web Scraping in Python. Real Python Tutorials. URL: https://realpython.com/python-web-scraping-practical-introduction/

5. Akhter Z. (2021). Web Scraping with Python - A Comprehensive Guide. freeCodeCamp.org. URL: https://www.freecodecamp.org/news/web-scraping-python-tutorial-how-to-scrape-data-from-a-website/

6. GeeksforGeeks. (2024). Python Web Scraping Tutorial. GeeksforGeeks. URL: https://www.geeksforgeeks.org/python-web-scraping-tutorial/

УДК 004.92

ПРОБЛЕМАТИКА СЕГМЕНТАЦІЇ ВЕЛИКОГАБАРИТНИХ МОДЕЛЕЙ ДЛЯ ДРУКУ НА 3D-ПРИНТЕРАХ З МАЛОЮ ОБЛАСТЮ ПОБУДОВИ

Андрій ГАВРИЛЮК, Назарій БУРАК
Львівський державний університет безпеки життєдіяльності

Анотація. *Розглянуто методи поділу масштабних архітектурних макетів для друку на обладнанні з обмеженою робочою зоною. Проаналізовано вплив геометрії ліній розрізу на міцність та естетику готового виробу. Визначено основні труднощі при позиціонуванні та склеюванні фрагментів моделей, а також запропоновано шляхи оптимізації процесу підготовки до друку.*

Ключові слова: *3D-друк, сегментація, макетування, FDM-технологія, великогабаритні моделі, постобробка.*

Abstract. *Methods for dividing large-scale architectural models for printing on equipment with a limited working area are considered. The influence of the geometry of the cut lines on the strength and aesthetics of the finished product is analysed. The main difficulties in positioning and gluing model fragments are identified, and ways to optimise the pre-printing process are proposed.*

Keywords: *3D printing, segmentation, layout, FDM technology, large-scale models, post-processing.*

Стрімка інтеграція адитивних технологій у процес архітектурного проєктування докорінно змінила підхід до створення презентаційних матеріалів. FDM(Fused Deposition Modeling)-друк став своєрідним стандартом для макетування завдяки своїй економічності та відносній швидкості. Проте, попри значне поширення цієї технології, більшість доступних для студентів та лабораторій 3D-принтерів мають суттєве технічне обмеження — малу область побудови, яка майже завжди не перевищує стандартні 200–300 мм. Це створює серйозний бар'єр при спробі відтворити великогабаритні об'єкти, такі як, наприклад, цілісний макет головного корпусу Львівського державного університету безпеки життєдіяльності (рис. 1), зі збереженням високого рівня деталізації.

Просте масштабування моделі «під розмір принтера» часто є неприпустимим, адже це нівелює точність відтворення дрібних елементів фасаду, віконних отворів та вхідних груп. Єдиним шляхом вирішення цієї технічної суперечності залишається програмна сегментація — поділ великого цифрового об'єкта на менші частини. Однак цей процес не можна зводити до механічного розрізання площинами. Хаотичний або автоматичний поділ часто призводить до критичних дефектів: помітних стиків, порушення геометрії під час склеювання та зниження загальної міцності конструкції. В результаті виникає нагальна потреба в розробці продуманої стратегії сегментації, яка враховує не лише габарити робочої камери, але й особливості подальшого монтажу.

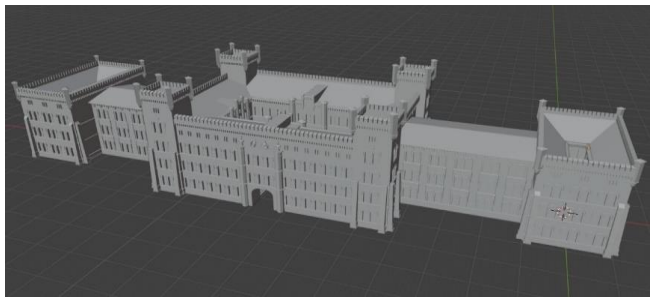

Рисунок 1 – 3D-модель головного корпусу ЛДУ БЖД м. Львів

У процесі дослідження особливостей макетування було виявлено, що довільне розрізання довгих фасадів є помилковою стратегією. Натомість більш раціональним визначено метод сегментації «по блоках» або секціях. Суть підходу полягає у поділі моделі на логічні архітектурні блоки, межі яких проходять виключно по внутрішніх кутах будівлі (місцях примикання перпендикулярних стін), як зображено на рисунку 2. Внаслідок такого позиціонування лінія стику природним чином ховається в тіні кута. Це дозволяє майже повністю відмовитися від запаювання та затирання швів, оскільки візуально з'єднання сприймається як конструктивна особливість будівлі, а не дефект друку. Склеювання площин у такому випадку забезпечує достатню жорсткість без складних замкових з’єднань.

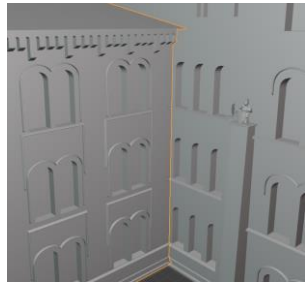

Рисунок 2 – Лінією зображено грані сегментації габаритної моделі

Окремим аспектом роботи стала проблема деталізації віконних отворів у дрібних масштабах (1:200). Під час тестових друків суцільних стін було помічено, що дрібні перемички часто ламаються при видаленні підтримок або виходять нечіткими через вібрації принтера. В результаті аналізу було запропоновано концепцію «гібридного» збирання. Основні

стіни друкуються з пустими отворами, тоді як віконні рами виготовляються окремо в горизонтальному положенні на платформі (рис. 3).

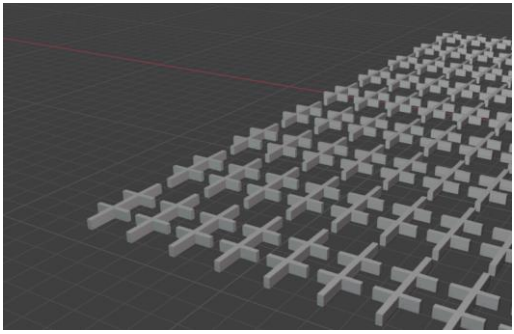

Рисунок 3 – 3D-модель віконних рам для горизонтального друку

Такий метод продемонстрував суттєві переваги при виготовленні складних об'єктів, подібних до моделі університету. Горизонтальний друк рам забезпечує ідеальну адгезію першого шару та високу міцність тонких елементів. Крім того, це дозволяє уникнути використання підтримок у віконних отворах, що значно пришвидшує постобробку стін. Вклеювання готових рам у пази створює додатковий об’єм та реалістичність, якої неможливо досягти при монолітному друку. Хоча час на ручне збирання дещо зростає, загальна якість та презентабельність макета суттєво покращуються.

У підсумку встановлено, що сегментація по внутрішніх кутах архітектурних форм є найбільш оптимальним методом поділу великогабаритних моделей. Такий підхід нівелює проблему маскування швів та спрощує позиціонування деталей. Водночас виокремлення дрібних елементів для окремого друку є критично важливим для малого масштабу, дозволяючи досягти професійної якості виробу навіть на обладнанні бюджетного класу.

Література

1. Адитивне виробництво: технологія, матеріали та переваги 3D-друку. URL:https://makerly.eu/uk/adytyvne-vyrobnycztvo-tehnologiya-materialy-ta-perevagy-3d-druku/ (дата звернення: 18.11.2025).

2. Що таке 3D моделювання для друку: як створювати моделі. URL: https://easy3dprint.com.ua/uk/shcho-take-3d-modelyuvannya-dlya-druku/ (дата звернення: 19.11.2025).

3. Адитивні технології виробництва (3D-друк): лекційні матеріали. URL: https://learn.ztu.edu.ua/ pluginfile.php/158653/ (дата звернення: 19.11.2025).

УДК 004.4:004.7:355

АРХІТЕКТУРА СИСТЕМИ КООРДИНАЦІЇ ВІЙСЬКОВИХ ЗАПИТІВ І ВОЛОНТЕРСЬКОЇ ДОПОМОГИ НА БАЗІ SPRING BOOT

Владислав ГАРМАТА, Ольга СМОТР
Львівський державний університет безпеки життєдіяльності, м. Львів

У сучасних умовах бойових дій ефективна координація між військовими та волонтерами є критично важливою для оперативного забезпечення підрозділів необхідними ресурсами. Запропоновано архітектуру централізованої системи, що реалізує три ключові ролі: військовий користувач, модератор та волонтер. Система побудована на основі Spring Boot із використанням MVC-підходу, де Model відповідає за роботу з реляційною базою даних, View реалізовано на Thymeleaf для динамічного рендерингу HTML, а Controller забезпечує обробку запитів та бізнес-логіку. Особливу увагу приділено безпеці: багаторівнева автентифікація, токенна авторизація, логування критичних дій, перевірка достовірності даних та розмежування доступу за ролями. Додатково передбачено модуль чату для комунікації та механізми запобігання шахрайським заявкам. Запропоноване рішення підвищує прозорість, швидкість обробки запитів та безпечність взаємодії між військовими та волонтерами.

***Ключові слова**: Spring Boot, MVC, координація запитів, військові потреби, безпека даних, волонтерська допомога.*

In modern combat conditions, effective coordination between military personnel and volunteers is crucial for timely delivery of essential resources. This paper proposes the architecture of a centralized system implementing three key roles: military user, moderator, and volunteer. The system is built using Spring Boot and follows the MVC pattern, where the Model manages relational database entities, the View is implemented with Thymeleaf for dynamic HTML rendering, and the Controller handles requests and business logic. Special attention is given to security: multi-level authentication, token-based authorization, logging of critical actions, data verification, and role-based access control. Additionally, the system includes a chat module for communication and mechanisms to prevent fraudulent requests. The proposed solution enhances transparency, accelerates request processing, and ensures secure interaction between military personnel and volunteers.

***Keywords:** Spring Boot, MVC, request coordination, military needs, data security, volunteer support.*

У сучасних умовах ведення бойових дій ефективна координація між військовими та волонтерами є критично важливою. Запити на дрони, тепловізори, медичні засоби, спорядження та інше обладнання повинні бути оброблені швидко, прозоро та з дотриманням правил безпеки. Без централізованої системи такі процеси часто супроводжуються втратами інформації, дублюванням заявок або неможливістю перевірити їх достовірність [1]. Вважаємо, за доцільне розробити систему з наступним функціоналом та архітектурою.

Розроблена система включатиме три ключові ролі:

1. Військовий користувач – створює запити на необхідні ресурси, вказуючи опис, важливість та підрозділ.

2. Перевіряючий (модератор) – верифікує запити, перевіряє їх правдивість, виключає можливі шахрайські звернення та дублікати.

3. Волонтер – переглядає підтверджені запити, бере їх у роботу, оновлює статуси та формує звіти про виконання.

З метою забезпечення високої продуктивність, масштабованості та швидкої розробки доцільно побудувати систему з використанням Spring Boot [2, 3]. Для створення інтерфейсу пропонуємо Thymeleaf, який дозволяє рендерити динамічні HTML-сторінки без потреби у складному фронтенд-коді [4]. Дані зберігатимуться у реляційній базі даних [5], що дає змогу забезпечити цілісність, швидкий доступ та безпечну обробку інформації.

Архітектура MVC дозволяє розділити логіку системи на три компоненти.

- Model міститиме сутності «Запит», «Користувач», «Роль», «Статус», «Звіт» та відповідає за взаємодію з базою даних.
- View, реалізований на Thymeleaf, забезпечуватиме динамічне відображення даних та зручні інтерфейси для кожної ролі.
- Controller прийматиме запити користувачів, перевірятиме їхні права доступу, викликатиме бізнес-логіку та повертатиме необхідні представлення.

Особливу увагу необхідно приділити безпеці системи, беручи до уваги те, що робота з військовими потребами містить чутливі дані [6]. У платформі необхідно зреалізувати:

- багаторівневу автентифікацію користувачів;
- токенну авторизацію;
- логування всіх критичних дій;
- перевірку достовірності даних через роль перевіряючого;
- розділення функціоналу відповідно до ролей;
- обмеження доступу до конфіденційних запитів;
- механізм запобігання шахрайським заявкам.

Також доцільно вбудувати в систему модуль чату, що забезпечуватиме комунікацію між волонтерами та військовими щодо деталей запиту, його статусу та підтвердження виконання. Модуль звітності повинен формувати інформацію про закриті запити, динаміку роботи волонтерів та потреби підрозділів.

Запропонована платформа значно оптимізує процес координації військових потреб, підвищує прозорість взаємодії та забезпечує безпечне, централізоване управління всіма заявками. Система легко масштабується та може бути розширена додатковими модулями аналітики або інтеграцією з іншими сервісами.

Література

1. Кордунова Ю. С., Смотр О. О., Кокотко І. Я., Малець Р. Б. Аналіз традиційного та гнучкого підходів до створення програмного забезпечення в динамічних умовах // *Управління розвитком складних систем*. – Київ, 2021. – № 47. – С. 71–77. – DOI: https://doi.org/10.32347/2412-9933.2021.47.71-77.

2. DeFranceschi R., Salomon M. *Spring Security in Action*. – Manning Publications, 2020.

3. Spring Boot – офіційна документація [Електронний ресурс]. – Режим доступу: https://spring.io/projects/spring-boot (дата звернення: 19.11.2025).

4. Thymeleaf Documentation. *Thymeleaf: Modern Server-Side Java Template Engine for Web and Standalone Environments*. [Електронний ресурс]. – Режим доступу: https://www.thymeleaf.org

5. Silberschatz A., Korth H., Sudarshan S. *Database System Concepts*. – McGraw-Hill, 2020.

6. Majithiya D. *Building Secure and Scalable Applications with Spring Boot*. – ShivLab Blog, 2024. [Електронний ресурс]. – Режим доступу: https://www.researchgate.net/publication/392892637_BUILDING_SCALABLE_SECURE_MICROSERVICES_WITH_SPRING_BOOT/citations

УДК 004.65

ВИКОРИСТАННЯ СТРУКТУРОВАНИХ ДАНИХ В СФЕРІ РОБОТИЗАЦІЇ ДОСЛІДЖЕНЬ ТА ВИРОБНИЦТВА

Гащук Л. П., Придатко О. В.
Львівський державний університет безпеки життєдіяльності

Сучасний світ невпинно рухається в напрямку зменшення присутності людини в найрізноманітніших галузях виробництва, наукових досліджень, в сфері сервісу та розваг. Все це націлено для полегшення повсякденного життя людини та збільшення комфорту життя. Велику роль в цьому відіграють системи автоматизованого виробництва та збірки. Але для їхньої ефективної та точної роботи, необхідно навчити їх правильно це робити. Навчанням звісно займається людина, а для того щоб навчити, вона використовує дані добуті протягом багатьох досліджень. .

***Ключові слова**: бази даних, структуризація даних, роботизовані системи, масове виробництво, людський фактор.*

The modern world is steadily moving towards a reduction in human presence in a wide variety of industries, including production, scientific research, service, and entertainment. All this is aimed at making people's daily lives easier and increasing the quality of life. Automated production and assembly systems play a major role in this. But for their effective and accurate work, it is necessary to teach them how to do it correctly. Learning is, of course, done by humans, and in order to teach, they use data obtained during many studies.

***Key words:** databases, data structuring, robotic systems, mass production, human factor.*

Символом індустріалізації 18-19 століть була широка і стрімка автоматизація виробництва за рахунок використання верстатів різного типу а також розвитку концепції двигунів різного типу які могли виконувати корисну роботу без допомоги людини. Верстати використовувались для дублювання людської роботи яка вимагала постійної повторюваності та точності її виконання. Ці механізми виконували завдання зі сталою швидкістю та створювали вироби з мінімальними відхиленнями один від одного на рівні масового виробництва. Розвиток автоматизації та інженерії став поворотним моментом для історії людства та напрямку розвитку технологій на десятки років вперед. Зараз, на прикладі автомобільного машинобудування, існують цілі заводи на яких збірка автомобіля проходить виключно з допомогою автоматичних верстатів та роботів, з мінімальним втручанням людини для коригування програми виробництва. Роботи здатні проводити операції з надвеликою точністю для створення як великих, так і дуже дрібних деталей, забезпечуючи найбільшу відповідність цих деталей до потрібних та наперед заданих параметрів.

Якщо заглянути в глибину, ні верстати 18ст., ні сучасні роботизовані системи не змогли б функціонувати, чи в принципі бути створеними, без знань і бачення людини яка виконувала цю роботу самостійно. В основі цих знань стоїть величезна кількість даних зібраних протягом довгого часу, іноді за рахунок випадкових спостережень, а іноді за рахунок цілеспрямованих досліджень. Поняття “Дані”, є дуже широким. До них можна віднести як і все, що людина сприймає органами чуття так і речі які вона вимірює і описує таким чином, щоб вони були зрозумілими для запису та передачі іншим, а також для використання в майбутньому. Всі дані зазви-

чай отримуються в сирому вигляді, тобто такими, які не зразу можна використати або які є малоефективними. Тут ми підходимо до того, що для використання даних нам потрібно їх структуризувати.

В першу чергу, під структуризацією ми маємо на увазі зведення "сирих" даних, отриманих низкою різних способів, до такої (наприклад математичної), яку можна легше пояснити і працювати з нею. Мається на увазі або створення вибірки, або трансформація множини хаотичних даних в корисні дані.

При масовому виробництві, зі всією можливою точністю і виробництво однакових (серійних) виробів, завжди буде присутня певна похибка в параметрах. Тому найчастіше при описі виробу використовуються типові параметри, а всі відхилення рахуються при потребі окремо. Само собою, що типові значення не з'являються ні звідки, або вираховуються з величезних масивів даних отриманих при дослідженні.

Яке це значення має для автоматизації різних систем? При розробці механізмів та роботизованих верстатів, потрібно написати відповідну програму, за якою буде працювати машина. Першою частиною є навчити машину рухатись та виконувати певні дії. Коли цей етап пройдено, можна перейти до навчання дій націлених на виконання конкретних завдань з метою виготовлення продукту або іншого об'єкту. На обох рівнях для навчання використовуються різні дані які вводяться в програму машини для розуміння виконуваних дій. Для коректного розуміння та виконання дій та завдань, ці дані повинні бути структурованими та нести специфічне значення.

Отож дані, а саме структуровані дані, є невід'ємною частиною створення роботизованих систем здатних виконувати складні завдання з мінімальним втручанням людини. Але для цього потрібна постійна робота з даними, а саме добування нових даних, створення баз даних, їх аналіз та структуризація для можливості їх ефективного використання.

Література

1. Groover, Mikell (2014). *Fundamentals of Modern Manufacturing: Materials, Processes, and Systems*.

2. Survey of Text Mining I: Clustering, Classification, and Retrieval / Ed. by M. W. Berry. — 2004. — Springer, 2003. — 261 с.

3. Silberschatz, Abraham; Sudarshan, S. (2011). *Database system concepts* (вид. 6). New York: McGraw-Hill.

4. Structure, Models and Meaning: Is «unstructured» data merely unmodeled?, Intelligent Enterprise, March 1, 2005.

5. ГОРОХОВАТСЬКИЙ, В. О.; ТВОРОШЕНКО, І. С. Методи інтелектуального аналізу та оброблення даних: навч. посібник. 2021.

6. Кучук Н. Г. Метод зменшення часу доступу до слабкоструктурованих даних / Н. Г. Кучук, В. Ю. Мерлак, В. В. Скородєлов // Сучасні інформаційні системи = Advanced Information Systems. – 2020. – Т. 4, № 1. – С. 97-102.

7. Основи автоматики та автоматизації: навч. посіб. / Є. П. Пістун, І. Д. Стасюк; Нац. ун-т «Львів. політехніка». — Львів, 2014. — 333 с. — Бібліогр.: с. 303—304.

УДК 532.5.6

АЛГОРИТМИ ІДЕНТИФІКАЦІЇ НЕПЕРЕВНИХ АКУСТИЧНИХ СИГНАЛІВ МАТЕМАТИЧНИМИ МЕТОДАМИ ДИСКРЕТИЗАЦІЇ

Тарас ГЕМБАРА
Львівський державний університет безпеки життєдіяльності

Abstract. *An approach to processing reflected acoustic signals in buildings is developed for object recognition and human search under technological and environmental noise. The input acoustic signals are treated as continuous functions of time with amplitude–frequency characteristics and are discretized using integral transforms. Mathematical models based on the Fourier transform, short-time Fourier transform and wavelet transform are considered.*

Key words: *acoustic signal, Fourier transform, wavelet transform, speaker recognition.*

Анотація. *Розроблено підхід до обробки відбитих акустичних сигналів у будівлях для задач ідентифікації об'єктів та пошуку людини в умовах технологічних і природних завад. Вхідні акустичні сигнали розглядаються як неперервні функції часу з амплітудно-частотними характеристиками та дискретизуються за допомогою інтегральних перетворень. Розглянуто математичні моделі на основі перетворення Фур'є, короткочасного Фур'є-перетворення та вейвлет-перетворення.*

Ключові слова: *акустичний сигнал, перетворення Фур'є, вейвлет перетворення, ідентифікація спікера.*

Проблема надійного виявлення та ідентифікації акустичних сигналів, що генеруються людиною (мовлення, крик, удари по конструкціях), є актуальною для пошуку постраждалих у зруйнованих будівлях, а також для інформаційної безпеки та технічної діагностики. У реальних умовах такі сигнали накладаються на фоновий шум обладнання, транспортні шумові поля, вітрові та інші природні завади, що ускладнює їх виділення та аналіз. Актуальною задачею є реєстрація, ідентифікація та верифікація акустичних сигналів, що має також на меті встановлення (уточнення) місцезнаходження джерел їх емісії [1]. В роботі [2] використано прилад GM1356, що дало змогу реєструвати рівні звукового тиску в широкому частотному діапазоні з подальшою передачею даних до персонального комп'ютера через інтерфейс USB. Це відкриває можливості для застосування математичних методів цифрової обробки сигналів, зокрема інтегральних перетворень, для аналізу амплітудно-частотних характеристик та розроблення алгоритмів автоматичної ідентифікації.

Ґрунтовний аналіз сучасних теоретичних та експериментальних досліджень з ідентифікації акустичних джерел в просторі представлено в праці [3]. В ній розглянута складна проблема у тривимірній (3D) області, де проведено вимірювання за допомогою сферичного масиву мікрофонів, що передбачає оцінку кутового положення джерел, відстані відносно масиву та кількісної оцінки амплітуд джерел. Запропоновано 3D-модель ло-

калізації джерела з використанням сферичної мікрофонної решітки зі сферичним поширенням хвилі, а для локалізації в 3D-просторі використовується розріджене байєсівське навчання.

Об'єктом дослідження є неперервні акустичні сигнали, що реєструються всередині будівель, зокрема у зруйнованих конструкціях, де можливе знаходження людини. Вхідні дані розглядаються як функції часу x(t) з амплітудно-частотними характеристиками, що можуть включати як мовні сигнали, так і ударні імпульси. Для аналізу проблеми використано математичну модель [1] дискретизації неперервних акустичних сигналів із використанням перетворення Фур'є та вейвлет-перетворення, що враховує особливості нестаціонарних мовних і ударних акустичних сигналів [2]. Для розрахунків створене спеціальне програмне забезпечення в середовищі Scilab. Сформульовано дворівневу схему ідентифікації акустичних сигналів: визначення приналежності джерела сигналу людині та верифікація конкретної особи на основі набору спектральних і часово-частотних ознак. На першому рівні ідентифікації необхідно встановити, чи є джерелом сигналу людина. Для цього аналізуються такі ознаки: частотний діапазон (основна енергія зосереджена до 4–5 кГц); наявність основної частоти f та її гармонік для голосових сигналів; формантна структура (резонанси F1, F2, F3 для голосу); частота переходів через нуль (ZCR), яка для голосу, як правило, нижча, ніж для білого шуму; часові патерни енергії, що відповідають серіям ударів або фразам мовлення. На практиці сигнал розбивається на послідовність вікон, для кожного з яких обчислюють енергетичні та спектральні характеристики. Якщо протягом достатньо тривалого інтервалу спостерігаються ознаки, характерні для людського голосу або серій ударів, робиться висновок про наявність людського джерела акустичних сигналів. Другий рівень ідентифікації пов'язаний із розпізнаванням людини. Для цього найчастіше використано мел-кепстральні коефіцієнти (MFCC - Mel-Frequency Cepstral Coefficient), коефіцієнти лінійного передбачення (LPC), формантні частоти та інші ознаки голосу. Для еталонного запису певної особи обчислюється послідовність MFCC-векторів, після чого визначається середній вектор ознак. Аналогічно обробляється новий запис. Порівняння проводиться за відстанню між середніми векторами, що можливо здійснити і за більш складними статистичними моделями (наприклад, моделями гаусових сумішей). Якщо відстань не перевищує наперед заданого порогового значення, сигнал вважають таким, що належить тій самій людині. У процесі ідентифікації акустичних сигналів, особливо мовлення, важливо враховувати особливості сприйняття звуку людиною. Для апробації запропонованого підходу було проведено реєстрацію акустичних сигналів у приміщенні із застосуванням реєстратора GM1356. Прилад працював у діапазоні 31,5 Гц – 8,5 кГц, рівні звукового тиску вимірювалися в дБ із використанням зважувальних фільтрів A та C. Через USB-інтерфейс дані передавалися до ПК, де програма SoundLab формувала файли дискретизації, а програма Soundcard Oscilloscope забезпечувала

візуалізацію сигналів у режимі реального часу.

З урахуванням апаратних можливостей приладу GM1356 та програмного забезпечення SoundLab і Soundcard Oscilloscope алгоритм обробки сигналів можна подати у вигляді таких кроків:

1) реєстрація рівнів звукового тиску в дБ у заданому частотному діапазоні;

2) передача даних на ПК через USB та формування файлів дискретизації;

3) перетворення рівнів у дБ до лінійних амплітуд за потреби та нормування сигналу;

4) спектральний аналіз (FFT, STFT) та побудова спектрограм;

5) вейвлет-аналіз для виявлення ударних та інших короткочасних компонент;

6) обчислення ознак для ідентифікації (форманти, ZCR, MFCC тощо);

7) прийняття рішень за дворівневою схемою: людина (не людина), конкретна особа (інша особа).

Порівняння класичних Фур'є-спектрограм із вейвлет-спектрограмами засвідчило, що для нестаціонарних мовних сигналів вейвлет-перетворення забезпечує більш інформативне подання часово-частотної структури. Для сигналів ударної емісії вейвлет-аналіз дозволяє точніше локалізувати моменти виникнення імпульсів і оцінити їх спектральний вміст. Записувалися як фонові шуми, так і сигнали, породжені людиною: мовлення, крик, удари по конструкціях. На основі отриманих даних було побудовано спектри та спектрограми, а також вейвлет-спектрограми. Якісний аналіз показав, що мовні сигнали характеризуються наявністю виразної гармонічної структури спектра та формантних резонансів, тоді як ударні сигнали мають короткі у часі широкосмугові компоненти

Література

1. Гембара Т. Математичні методи та програмне забезпечення візуалізації фазово-частотних. характеристик акустичних сигналів // Зб. тез IV-ої Міжнародної науково-практичної конференції "Інформаційна безпека та інформаційні технології" ІБІТ 2022 "Cybersecurity and information technology", Львів, 30.11. 2022. – С.228-230.

2. Гембара Т. Ідентифікація неперервних акустичних сигналів математичними методами дискретизації інтегральними перетвореннями // Зб. тез V-ої Міжнародної науково-практичної конференції "Інформаційна безпека та інформаційні технології" ІБІТ 2024 "Cybersecurity and information technology", Львів, 27.11. 2024. – С.448-453.

3. Ping G., Fernandez-Grande E., Gerstoft P., Chu Z. Three-dimensional source localization using sparse Bayesian learning on a spherical microphone array // J. Acoust. Soc. Am. – 2020. – 147. – P. 3895–3904.

УДК 621.39:004.8:004.6

АНАЛІЗ СУЧАСНИХ ПІДХОДІВ ДО УПРАВЛІННЯ РЕСУРСАМИ В ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ НА ОСНОВІ ШІ

Віктор ГНАТЮК[1,2], Іван ГОРБАЧОВ[1], Олександр ЛИТВИНЮК[1]
[1]Державний університет «Київський авіаційний інститут», Київ
[2]Державний науково-дослідний інститут технологій кібербезпеки та захисту інформації, Київ

Анотація. *У роботі здійснено аналіз сучасних підходів до управління ресурсами в телекомунікаційних системах на основі ШІ та систематизуються дослідження щодо використання контрольованого, неконтрольованого, підкріплюваного та федеративного навчання для оптимізації радіо-, обчислювальних та енергетичних ресурсів у мережах наступного покоління.*

Ключові слова*: телекомунікаційні системи, управління ресурсами, ШІ, машинне навчання, QoS, 5G.*

Abstract. *The paper analyzes modern approaches to resource management in telecommunication systems based on AI and systematizes research on the use of supervised, unsupervised, reinforced, and federated learning to optimize radio, computing, and energy resources in next-generation networks.*

Keywords: *telecommunication systems, resource management, AI, machine learning, QoS, 5G.*

У сучасних телекомунікаційних системах управління ресурсами (Resource Management) є ключовим завданням, що визначає ефективність функціонування мереж п’ятого та шостого поколінь. За останні роки дослідники активно впроваджують методи штучного інтелекту (ШІ), зокрема машинного навчання (ML) та глибокого підкріплювального навчання (Deep Reinforcement Learning, DRL), для підвищення рівня автоматизації, адаптивності та енергоефективності мереж [1–5]. Згідно з узагальнюючим оглядом [1], методи машинного навчання відіграють фундаментальну роль у вирішенні задач оптимізації телекомунікаційних систем. Автори класифікують сучасні ML-підходи за типами задач — прогнозування трафіку, управління пропускною здатністю, динамічне планування ресурсів та адаптивне управління QoS. Огляд також підкреслює важливість інтеграції ML у системи з багаторівневою архітектурою (cloud–edge–device) для мінімізації затримок і підвищення ефективності. В огляді [2] проведено систематизацію підходів ШІ до управління ресурсами у гетерогенних мережах 6G. Зокрема, розглядаються питання сумісності інтелектуальних рішень із технологіями Network Slicing, Massive MIMO, RIS та edge computing. Автори вказують на переваги використання моделей глибинного навчання для розподілу обчислювальних і спектральних ресурсів, а також звертають увагу на проблеми енергоефективності та потребу у стандартизованих інтерфейсах обміну даними. Дослідження [3], опубліковане в журналі IEEE Communications Surveys & Tutorials, охоплює широкий спектр ML-застосувань для управління ресурсами у бездротових системах. Огляд виділяє тенденцію переходу від централізованого до децентралізованого управління ресурсами

на основі ШІ, де ключову роль відіграють агенти, здатні до самонавчання в умовах змінного навантаження. Окрему увагу у літературі приділено застосуванню підкріплювального навчання для управління радіоресурсами в архітектурах [4] демонструють, що алгоритми RL здатні ефективно адаптувати політики розподілу радіоресурсів у реальному часі з урахуванням QoS-параметрів користувачів. Раніше подібні підходи узагальнив [5], які показали, що DRL перевершує традиційні евристичні методи у складних динамічних сценаріях мобільних мереж. Робота [6] розширює підхід управління ресурсами на середовище SAGIN (Space–Air–Ground Integrated Networks), поєднуючи комунікаційні й обчислювальні ресурси. Автори наголошують на необхідності створення уніфікованих моделей оптимізації, які враховують взаємодію між сегментами мережі. Дослідження [7] демонструє практичну реалізацію оптимізації розподілу ресурсів у 5G slicing-мережах, де використано вагові експоненційні та логарифмічні функції для покращення QoS. Це підтверджує ефективність математично-інтелектуальних моделей у задачах управління із багатьма критеріями. Для підвищення масштабованості AI-рішень у розподілених середовищах запропоновано підхід Federated Deep Reinforcement Learning (FDRL) [8], який дозволяє навчати моделі на різних вузлах без централізованого збору даних. Це знижує навантаження на канал і забезпечує конфіденційність користувачів. Питання енергоефективності та «зелених» комунікацій детально розглянуте в роботі [9], де підкреслено, що інтеграція ШІ в управління ресурсами є ключовим напрямом розвитку екологічно стійких 6G-мереж. Запропоновано підхід, який мінімізує споживання енергії базових станцій при збереженні QoS. Дослідження [10, 11] демонструє можливість інтеграції AI у систему управління Network Slicing через створення модульної архітектури, що динамічно виділяє ресурси для кожного сервісного вирізу мережі. Це забезпечує високий рівень адаптивності та автоматизації управління. Основні напрями застосування методів AI у телекомунікаційних системах, типи алгоритмів AI/ML зазначені у табл. 1.

Таблиця 1 – Основні напрями застосування методів AI у телекомунікаційних системах

Напрям застосування	**Тип алгоритму AI/ML**	**Очікуваний ефект**	**Приклади робіт**
Розподіл радіоресурсів	Reinforcement Learning (RL)	Оптимізація пропускної здатності, зниження затримок	[3], [4], [5]
Управління енергоспоживанням	Supervised Learning	Зменшення втрат енергії, баланс навантаження	[2], [9]
Розподіл обчислювальних ресурсів	Deep RL, Federated Learning	Підвищення ефективності MEC-сервісів	[6], [8]
Network Slicing	Cognitive AI, Heuristic ML	Адаптивне виділення зрізів мережі	[7], [10], [11]

Підсумовуючи аналіз, можна зробити висновок, що застосування методів ШІ в управлінні ресурсами телекомунікаційних систем формує нову парадигму інтелектуального управління, у якій основну роль відіграють глибоке навчання, розподілене навчання та енергоефективна оптимізація в контексті 6G.

Література

1. Elias Dritsas, Maria Trigka, *Machine Learning in Information and Communications Technology: A Survey*, Information 2025, 16(1), P. 8. https://doi.org/10.3390/info16010008

2. Hayder Faeq Alhashimi, Mhd Nour Hindia, Kaharudin Dimyati, Effariza Binti Hanafi, Feras Zen Alden, Faizan Qamar, Quang Ngoc Nguyen, *Survey on AI-Enabled Resource Management for 6G Heterogeneous Networks: Recent Research, Challenges, and Future Trends* // Computers, Materials and Continua,Volume 83, Issue 3, 19 May 2025, Pages 3585-3622. https://doi.org/10.32604/cmc.2025.062867

3. D. G. S. Pivoto, F. A. P. de Figueiredo, C. Cavdar, G. R. d. L. Tejerina and L. L. Mendes, "A Comprehensive Survey of Machine Learning Applied to Resource Allocation in Wireless Communications," in IEEE Communications Surveys & Tutorials, DOI: 10.1109/COMST.2025.3552370

4. Caio P. Galdino, Rodrigo Souza Couto, Dianne Scherly Varela de Medeiros, *Reinforcement Learning for Radio Resource Management in O-RAN*. Conference: 2024 IEEE 13th International Conference on Cloud Networking (CloudNet). DOI: 10.1109/CloudNet62863.2024.10815702

5. Alwarafy A., Abdallah M., Ciftler B. S., Al-Fuqaha A., Hamdi M. *Deep Reinforcement Learning for Radio Resource Allocation and Management in Next Generation Heterogeneous Wireless Networks: A Survey* // arXiv preprint arXiv:2106.00574. – 2021.

6. Qian Chen, Zheng Guo, Weixiao Meng, Shuai Han, Cheng Li, Tony Q. S. Quek. *A Survey on Resource Management in Joint Communication and Computing-Embedded SAGIN*. https://doi.org/10.48550/arXiv.2403.17400

7. Nong, X., Liang, X. Scheduling allocation in 5G slicing networks utilizing weighted exponential and logarithmic functions to improve QoS. Sci Rep 15, 32204 (2025). https://doi.org/10.1038/s41598-025-17385-4

8. L. Zang, X. Zhang and B. Guo, "Federated Deep Reinforcement Learning for Online Task Offloading and Resource Allocation in WPC-MEC Networks," in *IEEE Access*, vol. 10, pp. 9856-9867, 2022, DOI: 10.1109/ACCESS.2022.3144415.

9. N. Alhussien and T. Aaron Gulliver, "Toward AI-Enabled Green 6G Networks: A Resource Management Perspective," in *IEEE Access*, vol. 12, pp. 132972-132995, 2024, DOI: 10.1109/ACCESS.2024.3460656.

10. D. Bega, M. Gramaglia, A. Garcia-Saavedra, M. Fiore, A. Banchs and X. Costa-Perez, "Network Slicing Meets Artificial Intelligence: An AI-Based Framework for Slice Management," in *IEEE Communications Magazine*, vol. 58, no. 6, pp. 32-38, June 2020, DOI: 10.1109/MCOM.001.1900653.

11. Gnatyuk, V., & Gorbachov, I. (2025). Dynamic Slice Network Management Method in 5G For QOS Enhancement In VOIP. *Herald of Khmelnytskyi National University. Technical Sciences*, *353*(3.2), 104-109. https://doi.org/10.31891/2307-5732-2025-353-12

УДК 004.056, 004.75

РОЛЬ ЦИФРОВИХ ДВІЙНИКІВ У ЗАБЕЗПЕЧЕННІ ІНФОРМАЦІЙНОЇ НАДІЙНОСТІ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ

Віктор ГНАТЮК[1,2], Левон ПЕТРОСЯН[1]
[1]Державний університет «Київський авіаційний інститут», Київ
[2]Державний науково-дослідний інститут технологій кібербезпеки та захисту інформації, Київ

Анотація. *У тезах розглянуто роль технології цифрових двійників у підвищенні інформаційної надійності телекомунікаційних систем. Проаналізовано концепцію Network Digital Twin (цифрового двійника мережі), міжнародні стандарти ISO 23247, підходи IoT та AI. Визначено напрями застосування цифрових двійників для моніторингу, виявлення аномалій і прогнозування відмов.*

Ключові слова: *цифровий двійник, телекомунікаційна система, інформаційна надійність, Internet of Things, машинне навчання, прогнозування відмов.*

Abstract. *The paper substantiates the use of digital twin technology to improve the information reliability of telecommunication systems. The Network Digital Twin concept is analyzed, including ISO 23247 standards, IoT and AI approaches. Application areas are identified: network state monitoring, anomaly detection and failure prediction.*

Keywords: *digital twin, telecommunication system, information reliability, Internet of Things, machine learning, failure prediction.*

Актуальність теми. Сучасні телекомунікаційні мережі є критичною інфраструктурою, тому зростають вимоги до їх безперервності та захищеності. Гетерогенність, динамічні топології, великі обсяги трафіку та кіберзагрози ускладнюють забезпечення надійності традиційними засобами. У цих умовах технологія цифрових двійників, один із ключових інструментів Індустрії 4.0 та IoT, розглядається як ефективний підхід до підвищення інформаційної надійності телекомунікаційних систем [1–3].

Постановка проблеми. Ускладнені мережі важко контролювати вручну: аномалії та відмови часто фіксуються запізно, а реактивні системи діагностики не забезпечують проактивного виявлення. Це спричиняє простої, втрату даних і зниження стійкості до кібератак. Потрібні підходи, що забезпечують безперервний моніторинг, раннє виявлення відхилень і прогнозування відмов на основі цифрових моделей мережі.

Мета роботи. Метою є теоретичне обґрунтування використання концепції цифрового двійника мережі (NDT) для підвищення інформаційної надійності телекомунікаційних систем, з аналізом стандартів Digital Twin, принципів IoT та ML/AI, а також визначенням напрямів застосування NDT для моніторингу, виявлення аномалій і прогнозного обслуговування.

Концептуальна база дослідження. Цифровий двійник – це динамічна віртуальна модель фізичного об’єкта, що синхронізується з реальним прото-

типом завдяки потоковим даним від сенсорів і мережевого обладнання [1–4]. Стандарти ISO 23247 визначають архітектуру, вимоги до обміну даними та життєвого циклу цифрового двійника, що створює основу для NDT [1, 2]. Консорціуми IIC та Digital Twin Consortium розробляють рекомендації і кейси впровадження цифрових двійників для промислових та телекомунікаційних систем [3, 4]. Інтеграція IoT забезпечує актуальне відображення параметрів мережі, а штучний інтелект і машинне навчання дозволяють формувати прогнозні моделі та оптимізувати конфігурації мережі [5–8].

Використання NDT забезпечує безперервний моніторинг стану мережі: цифровий двійник, що синхронно оновлюється, слугує узгодженою моделлю топології, навантаження та показників якості. Порівняння очікуваної поведінки моделі з фактичними вимірюваннями дозволяє рано виявляти аномалії трафіку, погіршення радіопараметрів чи ознаки кібератак [6, 9]. Поєднання NDT із ML підвищує точність виявлення відхилень у мережах нового покоління [6, 9]. Другим напрямом є прогнозна аналітика: цифровий двійник дає змогу оцінювати ризики перевантаження вузлів, відмов обладнання та зниження якості сервісу. Моделі прогнозного обслуговування та підкріплювального навчання дозволяють заздалегідь вибирати способи перерозподілу трафіку або планових ремонтів [7, 8]. Реальні проєкти впровадження цифрових двійників демонструють зменшення кількості аварійних відключень завдяки ранньому виявленню слабких компонентів [5, 10].

Третя функція NDT – можливість безпечного моделювання сценаріїв «what-if» для оптимізації мережі. Конфігурації, протоколи чи параметри розташування базових станцій можуть тестуватися на цифровому двійнику без ризику для реальної мережі, що дозволяє заздалегідь обирати оптимальні рішення [9, 11, 12].

Висновки. Технологія цифрових двійників телекомунікаційних мереж забезпечує перехід від традиційного реактивного контролю до повноцінного проактивного управління надійністю. Поєднання актуальної цифрової моделі мережі з аналітичними інструментами дає змогу своєчасно виявляти приховані відхилення у роботі вузлів, прогнозувати розвиток критичних ситуацій та оцінювати наслідки різних технічних рішень без втручання у реальну інфраструктуру. Завдяки цьому знижується ймовірність аварійних відмов, скорочується час простоїв і підвищується стабільність надання послуг у складних та динамічних умовах.

Подальший розвиток технології передбачає створення більш точних моделей поведінки мережі, удосконалення методів прогнозування на основі ML/AI та впровадження єдиних стандартів обміну даними між фізичною та цифровою мережею. Окремим завданням є забезпечення кіберстійкості самої платформи цифрового двійника, оскільки вона стає критичним елементом системи управління. Сукупність цих напрямів формує підґрунтя для впровадження високорівневих інструментів підтримки рішень, здатних забезпечити довгострокову надійність і захищеність телекомунікаційних систем.

Література

1. ISO 23247-1:2021. Automation systems and integration – Digital Twin framework for manufacturing – Part 1: Overview and general principles. Женева : International Organization for Standardization, 2021. 12 с.

2. Shao G., Frechette S. P., Srinivasan V. An Analysis of the New ISO 23247 Series of Standards on Digital Twin Framework for Manufacturing. Proc. MSEC 2023. Gaithersburg : National Institute of Standards and Technology (NIST), 2023. DOI: 10.6028/NIST.AMS.400-2. Режим доступу: https://nvlpubs.nist.gov/nistpubs/ams/NIST.AMS.400-2.pdf.

3. Industrial Internet Consortium (IIC). Journal of Innovation. November 2019 (Digital Twin Edition). Boston : Industrial Internet Consortium, 2019. Режим доступу: https://www.iiconsortium.org/journal-of-innovation.

4. Digital Twin Consortium. Telecommunications Working Group – Leveraging Digital Twins for Virtual-First Planning That Will Connect the Entire Planet. Boston : Digital Twin Consortium, 2024. Режим доступу: https://www.digitaltwinconsortium.org.

5. Шкурак Л. Digital Twins — цифрові двійники: як технологія змінює світ уже сьогодні. AIN.UA, 20.05.2025. Режим доступу: https://ain.ua/2025/05/20/shho-take-cifrovi-dviiniki-i-iak-cia-texnologiia-zminiuje-svit

6. Moharam M. H., Hany O., Hany A., Mahmoud A., Mohamed M., Saeed S. Anomaly detection using machine learning and adopted digital twin concepts in radio environments. Scientific Reports. 2025. Vol. 15. Article 18352. DOI: 10.1038/s41598-025-02759-5.

7. Zhang Z., Liu Y., Peng Z., Xu D., Chen M., Cui S. Digital Twin-Assisted Data-Driven Optimization for Reliable Edge Caching in Wireless Networks. IEEE Journal on Selected Areas in Communications. 2024. Vol. 42, No. 11. C. 3306–3320. DOI: 10.1109/JSAC.2024.3431575.

8. Reinforcement Learning for Predictive Maintenance in Network Digital Twins. IEEE Access, 2023.

9. IEEE Communications Society. Network Digital Twin for Anomaly Detection in 5G Systems. IEEE Network, 2024.

10. DTEK Case Study: Implementation of Digital Twin for Power Networks. UA.News, 08.10.2024. Режим доступу: https://ua.news/ua/ukraine/dtek-realizuvala-proyekt-tsifrovogo-dvijnika-elektromerezh-na-kiyivshhini.

11. Digital Twin-Based What-if Simulation for Network Planning. Journal of Telecommunications and Information Technology, 2023.

12. Bakirtzis S., Chen J., Qiu K., Zhang J., Wassell I. EM DeepRay: An Expedient, Generalizable, and Realistic Data-Driven Indoor Propagation Model. IEEE Transactions on Antennas and Propagation. 2022. Vol. 70, No. 6. C. 4140–4154. DOI: 10.1109/TAP.2022.3146394.

УДК: 004.8: 378.147:37.018.43

ДОСЛІДЖЕННЯ АРХІТЕКТУРИ ПРОГРЕСИВНОГО ВЕБЗАСТОСУНКУ ОСВІТНЬОГО ХАБУ З ІНТЕГРАЦІЄЮ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ

Максим ГОЛІНКА, Ольга СМОТР
Львівський державний університет безпеки життєдіяльності

Abstract. *The paper examines the features of designing and developing an intelligent educational hub based on Progressive Web Application (PWA) technology. The advantages of PWA for ensuring accessibility and autonomy of the educational process are analyzed. Architectural solutions are proposed for integrating artificial intelligence modules that provide personalization of learning, content adaptation, and intelligent user support.*

Keywords: *PWA, artificial intelligence, personalization, adaptive learning, web technologies*

Анотація*. У роботі розглянуто особливості проєктування та розробки інтелектуального освітнього хабу на базі технології Progressive Web Application (PWA). Проаналізовано переваги PWA для забезпечення доступності та автономності навчального процесу. Запропоновано архітектурні рішення для інтеграції модулів штучного інтелекту, які забезпечують персоналізацію навчання, адаптацію контенту та інтелектуальну підтримку користувачів.*

Ключові слова: *PWA, штучний інтелект, персоналізація, адаптивне навчання, веб-технології.*

Стрімкий розвиток цифрових технологій та перехід до змішаних форм навчання актуалізують потребу у створенні гнучких, доступних та ефективних освітніх платформ. Сучасні системи управління навчанням часто мають вигляд громіздких веб-сайтів, які не завжди зручні для використання на мобільних пристроях, або ж вимагають розробки окремих нативних додатків для різних операційних систем (iOS, Android), що підвищує вартість підтримки продукту. Водночас, статичний характер подачі матеріалу в традиційних системах не враховує індивідуальних особливостей здобувачів освіти, що знижує ефективність навчання.

Вирішенням цих проблем є розробка інтелектуального освітнього хабу у форматі прогресивного веб-застосунку (Progressive Web Application, PWA) з інтегрованими можливостями штучного інтелекту (ШІ) для персоналізації взаємодії. Метою цієї роботи є дослідження особливостей проєктування архітектури та потреб ключових функціональних можливостей такої системи.

Технологія PWA поєднує в собі найкращі риси веб-сайтів та нативних мобільних додатків [1,2]. Для освітнього хабу це надає низку стратегічних переваг:

- *Кросплатформність:* застосунок розробляється як єдиний веб-ресурс, який коректно працює на будь-яких пристроях (смартфони, планшети, десктопи) через браузер, не вимагаючи розміщення в магазинах додатків (App Store, Google Play).
- *Робота в оф-лайн-режимі:* завдяки використанню Service Workers, освітній хаб може кешувати навчальні матеріали (тексти, зображення, тести), дозволяючи студентам продовжувати навчання навіть за відсутності стабільного інтернет-з'єднання, що є критично важливим в умовах нестабільного зв'язку.
- *Швидкодія та залученість:* PWA завантажуються миттєво та підтримують push-сповіщення, що дозволяє оперативно інформувати користувачів про нові завдання, зміни в розкладі чи дедлайни, підвищуючи рівень залученості.

Ми пропонуємо розробити хаб, ключовою інновацією якого буде відхід від статичних навчальних програм до динамічної генерації контенту за допомогою великих мовних моделей (LLM), зокрема Google Gemini, у поєднанні з економічною моделлю мотивації. Архітектура системи передбачає впровадження модуля генеративного навчання.

При архітектурі з модулем генеративного навчання (AI-Driven Learning), на відміну від традиційних LMS із фіксованим набором курсів, система надає користувачеві повну свободу у виборі предметної області. Алгоритм роботи базується на запиті користувача (наприклад, «Кібербезпека» або «Історія козацтва»), який обробляється через API Google Gemini. ШІ миттєво формує персоналізований теоретичний модуль, структурований для легкого сприйняття, та автоматично генерує унікальний набір тестових завдань (квіз) для перевірки засвоєння саме цього матеріалу [3,4]. Це перетворює платформу на «нескінченний генератор» освітнього контенту.

Для забезпечення швидкого старту (onboarding) та покриття фундаментальних дисциплін у систему, як правило, інтегрують статичні, попередньо розроблені курси (зокрема, з української мови та історії України). Це дозволяє поєднати надійність перевірених академічних програм із гнучкістю AI-генерації.

Для підвищення мотивації здобувачів освіти, на нашу думку, доречно впровадити систему «Ризик та Винагорода». Тобто, гейміфікувати процес навчання через внутрішню економіку, використати такі підходи, як механіка оцінювання, магазин ваучерів тощо. Тобто використати так звану економічну модель гейміфікації (Risk & Reward):

- правильні відповіді на тестуваннях приносять бали (віртуальну валюту), тоді як помилки призводять до їх втрати. Це стимулюватиме студента відповідально ставитися до відповідей, а не вгадувати їх;
- накопичені знання конвертуються у реальні блага. Реалізувати модуль «Магазин», де користувач може обміняти зароблені бали на промокоди або знижки від партнерів платформи.

Особистий кабінет користувача виступатиме центром моніторингу прогресу. Він включатиме статистику успішності за генерованими та базовими модулями, історію проходження тестів та стан «віртуального гаманця». Це дозволить користувачеві відстежувати кореляцію між здобутими знаннями та отриманими винагородами.

Застосунок реалізований як прогресивний веб-застосунок (PWA) забезпечує кросплатформенність та доступність. Backend-частина виступає посередником між клієнтським інтерфейсом та Google Gemini API, забезпечуючи валідацію запитів, збереження історії генерацій у базі даних та обробку транзакцій у внутрішній системі балів. Така архітектура дозволить мінімізувати навантаження на клієнтський пристрій, переносячи обчислювальні процеси генерації контенту у хмару.

Висновки. Розробка PWA-хабу з інтеграцією Google Gemini дозволяє створити принципово новий формат самоосвіти. Поєднання необмеженої генерації навчальних матеріалів з ігровою економікою вирішує дві головні проблеми онлайн-навчання: неактуальність контенту (вирішується генерацією «на льоту») та низьку мотивацію (вирішується можливістю монетизації знань через ваучери). Система не просто навчає, а створює інтерактивне середовище, де знання стають активом.

Література

1. Google Developers. Progressive Web Apps [Електронний ресурс]. – Режим доступу: https://developers.google.com/web/progressive-web-apps (дата звернення: 19.11.2025).

Holmes W., Bialik M., Fadel C. *Artificial Intelligence in Education: Promises and Implications for Teaching and Learning*. – Boston : Center for Curriculum Redesign, 2019. – 226 p.

2. Maghsudi S., Lan A., Xu J., van der Schaar M. Personalized Education in the AI Era: What to Expect Next? // *IEEE Signal Processing Magazine*. – 2021. – Vol. 38, no. 3. – P. 37–50.

3. Смотр О., Карабин О., Лоза В. Трансформація діяльності викладача. Нові підходи та технології підготовки освітніх матеріалів // *Штучний інтелект у науці та освіті (AISE 2024). Artificial intelligence in science and education* : зб. матеріалів міжнар. наук. конф. (Київ, 1–2 березня 2024 р.) [Електронний ресурс]. – Київ : УкрІНТЕІ, 2024. – С. 263–266. – DOI: 10.35668/978-966-479-141-7.

4. Спірін О. М., Лупаренко Л. А. Проєктування та розроблення хмаро орієнтованого середовища для адаптивного навчання // *Інформаційні технології і засоби навчання*. – 2022. – Т. 88, № 2. – С. 123–140.

УДК 351:862.4

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ УПРАВЛІННЯ РЕСУРСНИМ ЗАБЕЗПЕЧЕННЯМ РЯТУВАЛЬНИХ ПІДРОЗДІЛІВ ОБ'ЄДНАНИХ ТЕРИТОРІАЛЬНИХ ГРОМАД В УМОВАХ ВІЙНИ

Роман ГОЛОВАТИЙ, Нестор ГОЦІЙ
Львівський державний університет безпеки життєдіяльності

Розглянуто концептуальні засади створення та впровадження інформаційних технологій управління ресурсним забезпеченням рятувальних підрозділів об'єднаних територіальних громад (ОТГ). Акцентовано увагу на особливостях функціонування системи цивільного захисту в умовах війни та необхідності цифровізації ресурсного планування для підвищення стійкості місцевих громад.

Ключові слова: *інформаційні технології, ресурсне забезпечення, цивільний захист, надзвичайна ситуація.*

The abstracts consider the conceptual principles of creating and implementing information technology for managing resource provision of rescue units of united territorial communities (UTCs). The focus is on the peculiarities of the functioning of the civil protection system in war conditions and the need to digitize resource planning to increase the resilience of local communities.

Keywords: *information technology, resource provision, civil protection, emergency.*

Реформа децентралізації та створення ОТГ сприяли розвитку місцевого самоврядування, але водночас висунули нові вимоги щодо організації цивільного захисту. Законом України «Про місцеве самоврядування в Україні» [2] та ст. 19 Кодексу цивільного захисту України (Кодекс ЦЗ) [1] визначено повноваження органів місцевого самоврядування у сфері організації заходів цивільного захисту, захисту населення і територій від природних та техногенних загроз, реагування на надзвичайні ситуації та ліквідації їх наслідків, забезпечення пожежної безпеки, функціонування пожежно-рятувальних підрозділів МПО та добровільної пожежної охорони (ДПО).

До основних повноважень органів місцевого самоврядування базового рівня віднесено забезпечення гасіння пожеж, що передбачає подальший розвиток та підвищення боєздатності вже існуючих та створення нових підрозділів МПО, затверджених Концепцією реформування місцевого самоврядування та територіальної організації влади в Україні, схваленої розпорядженням Кабінету Міністрів України від 01.04.2014 року № 333-р [4]. Удосконалення потребує також система організації та забезпечення цивільного захисту на відповідних територіях. Відповідно до статті 26 Закону України «Про місцеве самоврядування в Україні» [3] до виключної компетенції сільських, селищних, міських рад віднесено питання створення відповідно до законодавства комунальної аварійно-рятувальної служби.

Війна суттєво ускладнила діяльність рятувальних підрозділів ОТГ, зокрема через різке збільшення кількості надзвичайних подій, спричинених бойовими діями, потребу у швидкому поповненні ресурсів (паливо, техніка, захисне спорядження, інструменти), зростання вимог до логістики,

мобільності та координації, руйнування інфраструктури, що потребує оперативного реагування та відновлення та необхідність взаємодії з військовими підрозділами та гуманітарними службами.

Потреба використання сучасних інформаційних технологій в сфері ресурсного забезпечення підрозділів ДСНС зросла в умовах повномасштабної війни, коли громади стикаються з постійними ризиками, обстрілами, руйнуванням критичної інфраструктури та необхідністю швидкої координації сил. Ефективність роботи рятувальних підрозділів значною мірою залежить від якості цифрового управління ресурсами. Інформаційні технології дозволяють оперативно відслідковувати наявні запаси, ухвалювати швидкі управлінські рішення та координувати допомогу між громадами, що особливо важливо в умовах обмежених ресурсів та високої динаміки подій.

Інформаційні технології у сфері цивільного захисту включають:

- інтегровану базу даних ресурсів;
- модулі моніторингу та аналітики;
- електронний облік техніки і спорядження;
- геоінформаційну складову для планування і реагування;
- систему управління інцидентами в реальному часі.

Очікувані переваги інформаційних технологій управління ресурсами

- покращення прозорості та контрольованості процесів ресурсного планування;
- скорочення часу реагування на надзвичайні ситуації;
- оптимізація використання бюджетних коштів;
- підвищення стійкості громад під час воєнних дій;
- можливість прогнозування ресурсних потреб та ризиків;
- якісна координація між ОТГ, ДСНС та військовими структурами.

Запровадження сучасних інформаційних технологій управління ресурсним забезпеченням рятувальних підрозділів ОТГ є критично важливим для забезпечення безпеки населення в умовах війни. Системна цифровізація сприяє ефективній організації реагування, оптимізації матеріально-технічних ресурсів та формуванню стійких громад. Досвід країн ЄС в організації та діяльності ДПО також демонструє, що Україна потребує вдосконалення системи забезпечення пожежної безпеки.

Література

1. Кодекс цивільного захисту України: Закон України від 02 жовтня 2012 р. № 5403-VI / Верховна Рада України. URL: https://zakon.rada.gov.ua

2. Про місцеве самоврядування в Україні: Закон України від 21 травня 1997 р. № 280/97-ВР / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/ show/280/97-%D0%B2%D1%80#Text

3. Постанова КМУ «Про затвердження Порядку створення та функціонування місцевих пожежно-рятувальних підрозділів»№ 315 від 7 квітня 2023 р**.**

4. Про схвалення Концепції реформування місцевого самоврядування та територіальної організації влади в Україні: Розпорядження Кабінету Міністрів України від 01.04.2014 р. № 333-р / Кабінет Міністрів України. URL: https://zakon.rada.gov.ua/laws/ show/333-2014-%D1%80#Text

УДК 004.4

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ УПРАВЛІННЯ ПРОЄКТАМИ (НА ПРИКЛАДІ СТВОРЕННЯ САЙТУ «НГУ ТАВРІЯ ХЕРСОН»)

Анастасія ГОРДІЄНКО
Львівський державний університет безпеки життєдіяльності, м. Львів

Анотація. *У роботі розглянуто застосування інформаційних технологій під час створення сайту футбольного клубу «НГУ Таврія Херсон». Проаналізовано етапи планування, розробки, тестування та підтримки проєкту. Показано, як сучасні вебтехнології і методи управління проєктами допомагають ефективно реалізовувати навчальні ІТ-проєкти. Ключові слова: управління проєктами, веброзробка, ІТ, сайт, футбол.*

Annotation. *The paper examines the use of information technologies in creating the "NGU Tavria Kherson" football club website. Planning, development, testing, and maintenance stages are analyzed. The role of modern web technologies and project management methods in effectively implementing educational IT projects is demonstrated. Keywords: project management, web development, IT, website, football.*

Сучасні інформаційні технології відіграють ключову роль у реалізації та управлінні проєктами різного рівня складності. Навіть створення невеликого вебсайту потребує ретельного планування, визначення функціональних вимог, розподілу завдань, вибору інструментів і контролю за результатом.

Прикладом застосування ІТ у навчальному проєктному менеджменті є розробка сайту футбольного клубу «НГУ Таврія Херсон». Метою проєкту було створення інтерактивного ресурсу для фанів, гравців та тренерів команди, що дозволяє отримувати актуальні новини, переглядати розклад матчів і статистику команди, а також спілкуватися між собою.

Проєкт реалізовувався у кілька етапів: планування, розробка дизайну, створення структури сайту, тестування функціоналу та подальша підтримка. Такий підхід дозволив систематизувати роботу та уникнути помилок у процесі створення ресурсу.

На етапі планування визначались цілі сайту, його аудиторія та структура. Було проведено аналіз потреб користувачів, визначено найважливіші розділи та функції. Також встановлювались пріоритети щодо контенту, дизайну та інтерактивних елементів.

Розробка дизайну включала створення зручного інтерфейсу, адаптивності та логічної навігації. Для цього застосовувалися HTML, CSS, JavaScript та фреймворк Bootstrap, що значно пришвидшило процес створення зовнішнього вигляду.

Тестування сайту дозволило перевірити його роботу на різних пристроях, браузерах та інтернет-швидкостях. Після завершення тестування сайт був запущений у відкритий доступ.

Підтримка ресурсу включає оновлення новин, фото, відео та результатів матчів. Також здійснюється корекція структури та дизайну у відповідь на побажання користувачів.

Робота над проєктом виконувалася за принципами Agile, що дозволило оперативно реагувати на зміни та покращувати функціонал. Застосування канбан-дошок та інших інструментів планування значно підвищило ефективність роботи.

Створення сайту «НГУ Таврія Херсон» дало можливість здобути практичні навички у галузі веброзробки та управління проєктами, а також створити корисний ресурс, який використовується реальною командою.

Література

1. Бойко О. В. Інформаційні технології в управлінні проєктами. – Київ: КНУ, 2020.

2. Воронін В. І. Основи веброзробки: навчальний посібник. – Львів: ЛДУ БЖД, 2023.

3. Офіційна документація Bootstrap. – Режим доступу: https://getbootstrap.com

4. Офіційний сайт футбольного клубу «НГУ Таврія Херсон». – Режим доступу: https://tavria.ks.ua

УДК 004.8

ПЕРСПЕКТИВИ ЗАСТОСУВАННЯ МАШИННОГО НАВЧАННЯ ДЛЯ ВИЯВЛЕННЯ ВТОМИ РОБІТНИКІВ У БУДІВНИЦТВІ З МЕТОЮ ПРОФІЛАКТИКИ ТРАВМАТИЗМУ

Ігор ГУДЗЕЛЯК, Олександр ХЛЕВНОЙ
Львівський державний університет безпеки життєдіяльності

Будівельна галузь є однією з найбільш травмонебезпечних у світі, де щорічно фіксуються мільйони інцидентів, пов'язаних з людським фактором, обладнанням та зовнішніми умовами, і втома робітників відіграє критичну роль у виникненні цих проблем, спричиняючи до 30 відсотків усіх нещасних випадків через знижену концентрацію уваги, уповільнену реакцію та фізичні помилки, такі як падіння з висоти чи неправильне поводження з інструментами. Втома, як фізична, так і когнітивна, накопичується через тривалі зміни, важку фізичну працю, несприятливі погодні умови та психологічний стрес, що особливо актуально для будівництва, де робітники часто працюють у динамічних середовищах з високим ризиком. Традиційні методи виявлення втоми, такі як суб'єктивні опитування чи візуальний контроль, є неефективними через їхню суб'єктивність, нестачу об'єктивності та неможливість реального часу моніторингу, що призводить до реактивного підходу замість профілактичного. Саме тут машинне навчання відкриває нові можливості, дозволяючи аналізувати дані з носимих пристроїв, таких як інерційні вимірювальні модулі чи сенсори пульсу, для автоматизованого виявлення ознак втоми та запобігання травмам. Наш огляд сфокусовано на застосуванні алгоритмів машинного навчання для обробки даних з акселерометрів, гіроскопів та біометричні сенсорів, які дозволяють відстежувати рухи, серцевий ритм та інші фізіологічні показники в реальних умовах будівельних майданчиків.

Огляд літератури показує, що впродовж останніх років, зокрема з 2023 по 2025, спостерігається зростання інтересу до інтеграції машинного навчання з носимими технологіями для моніторингу втоми в високоризикових галузях, включаючи будівництво, де втома пов'язана з перевищенням фізичних навантажень і призводить до зниження продуктивності та виникнення аварій. Одним із популярних напрямків досліджень є можливість виявлення інцидентів, близьких до нещасних випадків, та оцінки фізичної втоми серед будівельників за допомогою носимих сенсорів, придатних для будівельних робіт, де дані з акселерометрів для класифікації рівнів втоми, можуть виявляти зміни у рухах, зокрема уповільнення. Такі дослідження підкреслюють переваги використання IMU-сенсорів, інтегрованих у захисний одяг, для реального часу оцінки, де моделі типу випадкового лісу та нейронних мереж обробляли дані про прискорення та кутові швидкості, дозволяючи прогнозувати ризики падінь чи ударів. Окремої уваги також заслуговують роботи, орієнтовані на водіїв, що аналізують сонливість через текст-to-image аугментацію та комп'ютерний зір. Моделі

на базі YOLOv8 та YOLO11 дають класифікувати стани "пильний" та "сонливий" на основі зображень обличчя, досягаючи середньої точності до 90% після аугментації даних синтетичними зображеннями. Тут слід розглянути можливість обробки візуальних даних, генерованих за допомогою Midjourney, яке дозволить подолати обмеження малих датасетів реальних фото, покращивши узагальнення моделей для різних умов освітлення та поз робітників, і це особливо корисно для профілактики травм, пов'язаних з втратою уваги під час керування технікою чи роботи на висоті.

Загалом сучасні дослідження в сфері застосування машинного навчання для виявлення втоми робітників у будівництві демонструють кілька ключових тенденцій, що відображають перехід від традиційних методів моніторингу до інноваційних технологічних рішень. Передусім, спостерігається активне використання носимих пристроїв, таких як сенсори для вимірювання прискорення, тиску та фізіологічних показників, які дозволяють збирати дані в реальних умовах праці без значних перешкод для робітників. Ці пристрої інтегруються в захисний одяг або взуття, забезпечуючи неінвазивний підхід до оцінки фізичної та когнітивної втоми, що особливо важливо для динамічних середовищ будівельних майданчиків, де фактори на кшталт тривалих змін, важких навантажень та зовнішніх умов сприяють накопиченню втоми. Алгоритми машинного навчання, включаючи класифікатори та нейронні мережі, застосовуються для аналізу цих даних та дозволяють класифікувати рівні втоми від низького до високого з достатньою точністю, що перевищує можливості суб'єктивних опитувань чи біомеханічних моделей, і сприяє ранньому виявленню ризиків, пов'язаних з м'язово-скелетними розладами чи іншими травмами.

Ще однією помітною тенденцією є впровадження мультимодальних підходів, де поєднуються різні типи даних, наприклад, електрокардіографічні, електроміографічні чи електроенцефалографічні сигнали з інерційними вимірами, для підвищення точності прогнозування порогів втоми. Такі гібридні моделі дозволяють враховувати як фізичні, так і когнітивні аспекти, забезпечуючи більш комплексну оцінку в високоризикових галузях, однією з яких є будівництво. Дослідження підкреслюють потенціал реального часу моніторингу за допомогою edge computing, що мінімізує затримки в обробці даних безпосередньо на пристроях, роблячи системи придатними для практичного використання на майданчиках з обмеженим доступом до мережі. Крім того, акцент робиться на персоналізованих системах, які адаптуються до індивідуальних особливостей робітників, таких як рівень фізичної підготовки чи тип виконуваних завдань, наприклад, підйом вантажів чи робота на висоті, що сприяє створенню попереджувальних механізмів, як сигнали про необхідність перерви через смарт-пристрої.

У контексті алгоритмів, популярними є методи, стійкі до великих обсягів даних, такі як метод опорних векторів чи ансамблі дерев рішень, які ефективно справляються з шумом та варіативністю сигналів у реальних умовах, хоча переважна частина робіт все ще базується на лабораторних симуляціях. Зростає інтерес до польових випробувань, де моделі тестуються на

невеликих групах робітників під час реальних завдань, що допомагає виявляти тенденції втоми через аналіз ключових характеристик рухів чи спектральних параметрів. Однак, тенденції також вказують на обмеження, зокрема, залежність від якості даних, чутливість до артефактів від зовнішніх факторів та труднощі з узагальненням моделей через малі вибірки, що спонукає до розвитку більших датасетів та стандартизації підходів. Загалом, ці дослідження підкреслюють перехід до проактивної безпеки, де машинне навчання інтегрується з IoT для створення систем, що не тільки виявляють, але й запобігають травмам, пов'язаним з втомою, хоча повне впровадження вимагає вирішення етичних питань приватності та підвищення пояснюваності моделей для зростання довіри серед стейкхолдерів.

Переходячи до викликів, однією з основних проблем є якість даних, оскільки фізіологічні сигнали, як HRV чи EMG, чутливі до артефактів від руху, погоди чи індивідуальних відмінностей – віку чи рівня фізичної підготовки робітників, що призводить до шумів та неповноти датасетів. У будівництві це посилюється динамічними умовами, де сенсори можуть зміщуватися, а батареї розряджатися під час довгих змін. Етичні аспекти, включаючи приватність біометричних даних, є критичними, оскільки постійний моніторинг може порушувати права робітників, а відсутність пояснюваності моделей (black-box AI) знижує довіру менеджерів та профспілок. Крім того, брак великих мультимодальних датасетів для будівництва, де втома залежить від типу робіт (висотні, важкі вантажі), ускладнює тренування моделей, а trade-off між точністю та обчислювальною потужністю ускладнює впровадження на edge-пристроях без інтернету. У візуальних підходах суттєвими викликами є різні варіації освітлення та оклюзії, що вимагають аугментації, але синтетичні дані можуть не повністю відтворювати реальність. Загалом, дослідження рідко охоплюють довгострокові тести, фокусуючись на коротких сесіях, що не враховує хронічну втому від тижневих графіків.

Щодо перспективних напрямків, майбутні роботи повинні зосередитися на розробці великих спеціалізованих датасетів для втоми в будівництві, включаючи анотовані дані з носимих пристроїв для різних типів робіт, таких як висотні операції чи підйом вантажів, з інтеграцією IoT для реального часу виявлення. Наприклад, персоналізовані моделі на базі серцевого ритму можуть адаптуватися до індивідуальних профілів. Інтеграція з emerging технологіями, як edge computing, дозволить обробляти дані локально, зменшуючи затримки, а використання XAI підвищить довіру. Крім того, гібридні системи з BIM для візуалізації ризиків та AR для тренінгів можуть розширити застосування, а open-source інструменти для ML у будівництві полегшать впровадження.

Можна підсумувати, що застосування машинного навчання для виявлення втоми відкриває шлях до проактивної безпеки, знижуючи травматизм та підвищуючи ефективність у будівництві, але вимагає подолання викликів через стандартизацію, етику та реальні тести для глобального впливу.

УДК 004.942

ІНТЕРАКТИВНЕ МОДЕЛЮВАННЯ АСТЕРОЇДНОГО УДАРУ ДЛЯ ОСВІТНЬО-ДЕМОНСТРАЦІЙНИХ ЦІЛЕЙ

Богдан ДАШКОВСЬКИЙ, Олена СИДОРЕНКО
Національний технічний університет «Харківський політехнічний інститут»

Анотація. *Розроблено інтерактивний застосунок для 3D-моделювання астероїдних зіткнень. Програма дозволяє змінювати фізичні параметри в реальному часі, візуалізувати процес утворення кратера, будувати графіки динаміки та експортувати результати для науково-освітнього використання.*

Ключові слова: *комп'ютерне моделювання, астероїд, ударний кратер, тривимірна візуалізація, застосунок.*

Abstract. *An interactive application for 3D modeling of asteroid impacts has been developed. The program enables real-time adjustment of physical parameters, visualization of the crater formation process, plotting of dynamics graphs, and result export for scientific and educational use.*

Keywords: *computer modeling, asteroid, impact crater, three-dimensional visualization, application.*

Астероїдні зіткнення належать до рідкісних, але надзвичайно масштабних явищ, тому їхнє моделювання та візуалізація привертають увагу не тільки науковців, а й фахівців з планетарної безпеки та освітян. Сучасні комп'ютерні симуляції природних катастроф дозволяють відтворювати такі сценарії у наочній формі. Зокрема, існують веб-інструменти на кшталт Asteroid Launcher, які дають змогу інтерактивно задати параметри астероїда і миттєво отримати оцінку наслідків удару – розмір кратера, зону вибухової хвилі, тепловий ефект – у доступному візуальному форматі [1]. Такі симулятори слугують не лише аналітичними, а й навчальними інструментами, однак їм притаманні обмеження, зокрема відсутність реалістичної тривимірної візуалізації форми [2] кратера та самого небесного тіла.

У межах даної роботи розроблено інтерактивний застосунок, що моделює процес утворення ударного кратера та надає користувачеві засоби для візуалізації наслідків у реальному часі. Застосунок дозволяє змінювати ключові параметри астероїда – розміри, масу, швидкість, кут входження в атмосферу й одразу спостерігати, як ці зміни впливають на розміри та морфологію результуючого кратера. Отримані результати зіткнення подаються у декількох формах: будуються 2D-графіки, що показують динаміку польоту під час падіння, а також умовні профілі кратера у горизонтальній і вертикальній площинах.

Одночасно застосунок вбудовує тривимірну сцену – у вікні програми відображається модель астероїда та область удару, яку користувач може оглядати з різних ракурсів, збільшувати та обертати [3]. Він фактично поєднує науково обґрунтоване моделювання з наочною тривимірною графікою, що відкриває нові можливості для наукових демонстрацій і освітніх проєктів у галузі планетології. Додатково передбачено експорт згенерованої поверхні у формат .obj, завдяки чому результати можна імпортувати в професійні середовища для створення фотореалістичних зображень чи анімацій, а також може слугувати інтерактивним засобом для популяризації знань про астероїдні удари та їхні наслідки.

Література

1. Earth Impact Effects Web-based Computer Program [Електрон. ресурс]. – Режим доступу: https://impact.ese.ic.ac.uk/ImpactEarth/ImpactEffects/effects.pdf – Earth Impact Effects Program: A Web-based computer program for calculating the regional environmental consequences of a meteoroid impact on Earth.

2. *Clemens M. Rumphf* Asteroid impact risk. Doctoral Thesis – 2016. – С. 1–15.

3. Visualization of Asteroid Impacts. URL: https://cgl.ethz.ch/Downloads/Publications/Papers/2018/Ibr18b/Ibr18b.pdf – Visualization and Analysis of Deep Water Asteroid Impacts.

УДК 004.8:004.021:351.86

ОСНОВИ ТА ІНТЕГРАЦІЯ DATA SCIENCE І ШТУЧНОГО ІНТЕЛЕКТУ В СУЧАСНИХ ЦИФРОВИХ ТЕХНОЛОГІЯХ ТА ЇХ ЗНАЧЕННЯ ДЛЯ СИСТЕМИ ЦИВІЛЬНОГО ЗАХИСТУ

Даніїл ДЕРКАЧ, Нікіта ВЕРБІЦЬКИЙ, Ольга СМОТР
Львівський державний університет безпеки життєдіяльності

Анотація. *Розглянуто основи Data Science та штучного інтелекту (ШІ), а також особливості їх інтеграції у сучасні цифрові технології. Показано, яким чином ці технології формують підхід до обробки даних, прогнозування та автоматизації управлінських процесів. Окрему увагу приділено можливостям застосування Data Science і ШІ у сфері цивільного захисту — зокрема у прогнозуванні надзвичайних ситуацій, аналізі відеоданих, підтримці рішень керівника гасіння пожежі та оптимізації реагування рятувальних підрозділів. Підкреслено ключові виклики впровадження інтелектуальних систем, серед яких якість даних, етичні стандарти та потреба у кваліфікованих фахівцях. Зроблено висновок про важливість цих технологій для підвищення ефективності та безпеки у системі цивільного захисту.*

Ключові слова: *Data Science, штучний інтелект, машинне навчання, глибоке навчання, цифрові технології, цивільний захист, рятувальні служби, аналіз даних.*

Annotation*. This thesis explores the fundamentals of Data Science and Artificial Intelligence (AI), as well as the integration of these technologies into modern digital systems. The work highlights how Data Science and AI support the processing of large datasets, predictive analytics, and the automation of decision-making processes. Special attention is given to their application in the field of civil protection, including forecasting emergencies, analyzing drone and video data, supporting firefighting decision-making, and optimizing operational response for rescue units. The thesis also discusses key challenges related to data quality, ethical considerations, and the need for qualified professionals. The conclusion emphasizes the importance of these technologies for improving efficiency, safety, and situational awareness in emergency response systems.*

Keywords: *Data Science, artificial intelligence, machine learning, deep learning, digital technologies, civil protection, rescue services, data analysis.*

У сучасному цифровому середовищі Data Science і штучний інтелект (ШІ) посідають провідне місце серед технологій, що визначають темпи розвитку промисловості, економіки та безпеки. Data Science розглядається як міждисциплінарна галузь, яка поєднує статистичні методи, аналіз даних, алгоритмічне мислення та програмні інструменти з метою отримання нових знань зі структурованих і неструктурованих наборів даних. У свою чергу, ШІ, зокрема машинне навчання та глибоке навчання, дозволяє автоматизувати обробку великих масивів інформації та створювати моделі, здатні передбачати події, виявляти закономірності та приймати рішення у змінних умовах.

Інтеграція Data Science і ШІ базується на послідовному циклі роботи з даними: від їх збирання й очищення до моделювання, тестування та практичного застосування. Сучасні інформаційні системи отримують дані з датчиків, камер, супутникових знімків, документації або користувацьких взаємодій. Після попередньої обробки інформація перетворюється на аналітичні моделі, які здатні прогнозувати тенденції, аналізувати поведінку систем або пропонувати оптимальні рішення в реальному часі. Глибокі нейронні мережі та інші інструменти ШІ дозволяють працювати не лише з числовими даними, а й з текстами, мовою, зображеннями, тепловими картами чи сигналами зі складних сенсорних систем.

Практичне застосування цих технологій охоплює надзвичайно широкий спектр сфер. У медицині використання прогнозних моделей допомагає визначати ризики захворювань та формувати персоналізовані плани лікування. У промисловості алгоритми прогнозного обслуговування попереджають відмови обладнання, зменшуючи операційні витрати. У транспортній галузі аналітика даних забезпечує оптимізацію маршрутів і підвищує безпеку руху. У сфері національної безпеки та охорони громадського порядку ШІ використовується для аналізу потоків відеонагляду, виявлення підозрілих ситуацій і моделювання можливих загроз.

Особливо актуальною є інтеграція Data Science і ШІ для системи цивільного захисту. Рятувальні служби працюють у середовищі, де кожна секунда може впливати на життя людей, а інформація часто надходить у великих обсягах і в умовах невизначеності. Технології аналізу даних дозволяють прогнозувати ймовірність виникнення пожеж, вибухів або техногенних аварій, а також аналізувати метеорологічні та екологічні показники. Системи на основі ШІ можуть автоматично обробляти відео з дронів, тепловізорів і камер спостереження, виявляючи осередки загорянь або потерпілих. У ситуаціях, коли керівнику гасіння пожежі необхідно швидко оцінити ризики, моделі машинного навчання допомагають прогнозувати можливий розвиток ситуації та визначати оптимальні маршрути для підрозділів. Завдяки цьому підвищується ефективність реагування і знижується небезпека для особового складу. Попри значний потенціал, впровадження Data Science та ШІ супроводжується низкою викликів. До найбільш критичних належать питання якості даних, захисту приватності, етичного використання алгоритмів і забезпечення прозорості моделей. Інтелектуальні системи потребують постійного моніторингу, оновлення та перевірки, адже навіть незначні помилки у вихідних даних можуть впливати на точність рішень. Важливо також, щоб фахівці, які працюють із такими системами, розуміли не лише технічні аспекти, а й реальні потреби галузі, особливо коли йдеться про безпеку людей.

Таким чином, поєднання Data Science та штучного інтелекту формує основу сучасної цифрової трансформації. Ці технології створюють умови

для підвищення ефективності, автоматизації процесів і оперативного прийняття рішень у різних сферах. Для системи цивільного захисту їхнє застосування є не лише перспективним, а й необхідним, адже дає змогу швидше реагувати на надзвичайні ситуації, приймати обґрунтовані рішення та зменшувати ризики для населення та рятувальників.

Література

1. Russell S., Norvig P. Artificial Intelligence: A Modern Approach. 4th ed. Hoboken : Pearson, 2021. 1136 p.

2. Головатий Р. Р., Босак Г. С. Інформаційні технології в оперативному реагуванні: аналіз і оптимізація рішень для підрозділів ДСНС України // Цивільний захист в умовах війни: збірник тез І Міжнародної науково-практичної конференції. Львів : ЛДУБЖД, 2025. С. 112–116.

3. Goodfellow I., Bengio Y., Courville A. Deep Learning. MIT Press, 2022. 800 p.

4. Зачко О. Б., Головатий Р. Р., Кобилкін Д. С. Models of Safety Management in Development Projects // 2019 IEEE 14th International Scientific and Technical Conference on Computer Sciences and Information Technologies (CSIT). Lviv, 2019. P. 47–52.

5. LeCun Y., Hinton G., Bengio Y. Deep learning — past, present, and future // Communications of the ACM. 2024. Vol. 67, No. 1. P. 36–45.

УДК 378.1:004.738.5 + 37.091.33

ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ ІНТЕГРОВАНОГО МОНІТОРИНГУ ПРОГРАМНИХ ПРОЕКТІВ В ОСВІТНЬОМУ СЕРЕДОВИЩІ SMART-УНІВЕРСИТЕТУ

Віталій ДЗЕНЬ, Юрій БОРЗОВ
Львівський державний університет безпеки життєдіяльності

Анотація. *У роботі досліджено проблему розриву між академічною розробкою програмного забезпечення та промисловими DevOps-практиками. Запропоновано інформаційну технологію "DevOps-as-a-Service", що надає централізовану платформу моніторингу для студентських проєктів. Розроблено архітектуру системи (рис. 1) та алгоритм її роботи (рис. 2), що автоматизують збір метрик та логів за допомогою клієнтської бібліотеки (sdk). Проведено порівняльний аналіз запропонованого підходу, який довів значне зниження порогу входу та скорочення часу на інтеграцію інструментів спостережуваності (observability) порівняно з традиційними методами. Технологія сприяє формуванню у студентів практичних навичок аналізу продуктивності програмних систем.*

Ключові слова. *Smart-університет, DevOps, моніторинг, observability, мікросервіси, інформаційна технологія, освітнє середовище, Prometheus, Grafana.*

Abstract. *The paper investigates the gap between academic software development and industrial DevOps practices. A "DevOps-as-a-Service" information technology is proposed, providing a centralized monitoring platform for student projects. The system architecture (Fig. 1) and its operational algorithm (Fig. 2) have been developed to automate metric and log collection via a client library (sdk). A comparative analysis of the proposed approach has demonstrated a significant reduction in the entry barrier and the time required to integrate observability tools compared to traditional methods. The technology promotes the development of practical skills among students for analyzing the performance and reliability of software systems.*

Keywords. *Smart university, DevOps, monitoring, observability, microservices, information technology, educational environment, Prometheus, Grafana.*

Сучасна підготовка ІТ-фахівців вимагає не лише вміння писати код, а й розуміння повного життєвого циклу програмного продукту, включаючи його розгортання, моніторинг та підтримку. Однак в освітньому процесі студенти рідко стикаються з промисловими DevOps-практиками через високу складність налаштування спеціалізованих інструментів, таких як Prometheus, Grafana, Loki чи ELK Stack, для кожного окремого навчального проєкту. Це створює значний розрив між академічними знаннями та реальними вимогами ринку праці.

Для вирішення цієї проблеми було розроблено інформаційну технологію, що функціонує за моделлю "DevOps-as-a-Service" у межах освітнього середовища. Вона складається з централізованої серверної платформи та легкої клієнтської бібліотеки (sdk), що інтегрується у студентські проєкти. Концептуальна архітектура системи, що забезпечує збір, агрегацію та візуалізацію даних, представлена на рис. 1.

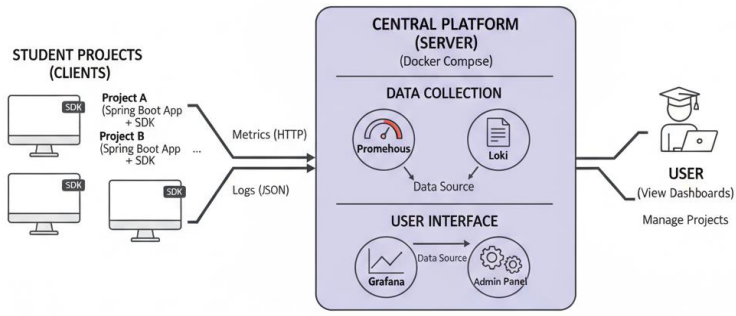

Рисунок 1 – Концептуальна модель архітектури платформи

Алгоритм взаємодії компонентів системи (рис. 2) побудований таким чином, щоб максимально автоматизувати процеси налаштування. Студенту достатньо додати одну залежність (sdk) у свій проєкт, після чого метрики та логи починають автоматично надсилатися на центральну платформу для подальшого аналізу.

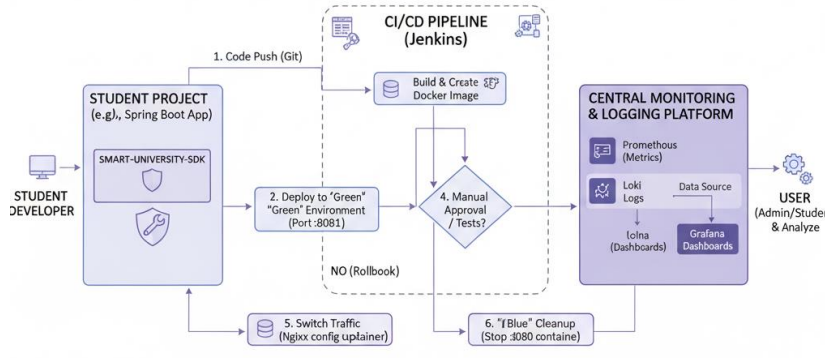

Рисунок 2 – Алгоритм взаємодії компонентів системи

На поточному етапі проведено порівняльний аналіз запропонованого рішення з існуючими підходами за ключовими для освітнього процесу критеріями. Результати аналізу (табл. 1) демонструють, що розроблена технологія значно знижує поріг входу та трудомісткість інтеграції інструментів моніторингу, дозволяючи студентам сфокусуватися на аналізі продуктивності свого коду, а не на адмініструванні інфраструктури.

Таблиця 1 – Порівняльний аналіз підходів до організації моніторингу

Критерій оцінки	**Традиційний підхід (Ручне налаштування)**	**Запропонована платформа**
Поріг входу для студента	Високий	Низький
Час на первинну інтеграцію	Години / Дні	Хвилини
Вимоги до інфраструктури	Високі (окремий стек на проєкт)	Мінімальні (централізований сервер)
Освітня цінність	Зміщена на адміністрування	Фокус на аналізі коду

Перспективним напрямом подальших досліджень є розширення функціональності платформи шляхом інтеграції модуля автоматизованого розгортання (CI/CD) з підтримкою стратегій Blue-Green, що дозволить охопити ще один важливий аспект DevOps-практик.

Висновки. Розроблена інформаційна технологія є ефективним дидактичним інструментом, що долає розрив між теорією та практикою у використанні сучасних підходів до розробки ПЗ. Завдяки низькому порогу входу та централізації інфраструктури, вона дозволяє інтегрувати промислові практики моніторингу безпосередньо в навчальний процес, підвищуючи практичну цінність студентських проєктів та конкурентоспроможність майбутніх випускників.

Література

1. Beyer B., Jones C., Petoff J., Murphy N. R. Site Reliability Engineering: How Google Runs Production Systems. O'Reilly Media, 2016. 552 p.

2. Downey A. B. Think Bayes: Bayesian Statistics in Python. O'Reilly Media, 2021. 250 p.

3. Prometheus: Up & Running: Infrastructure and Application Performance Monitoring / B. Brazil. O'Reilly Media, 2018. 266 p.

4. Спасітєлєва, Світлана Олексіївна та Чичкань, І. та Шевченко, Світлана Миколаївна та Жданова, Юлія Дмитрівна (2023) Розробка безпечних контейнерних застосунків з мікросервісною архітектурою Кібербезпека: освіта, наука, техніка, 1 (21). с. 193-210.

5. Абакумов, Р. В. (2025). Інноваційні підходи до зменшення технічного боргу в середовищі мікросервісної архітектури. Академічні візії, (48). вилучено із https://www.academy-vision.org/index.php/av/article/view/2241

УДК 004.89:004.4

АРХІТЕКТУРА МУЛЬТИАГЕНТНОЇ СИСТЕМИ ОРКЕСТРАЦІЇ ЗАПИТІВ НА БАЗІ ПЛАТФОРМИ N8N

Богдан ДМИТРУК, Олександр ХЛЕВНОЙ
Львівський державний університет безпеки життєдіяльності

Анотація. *У роботі досліджено підходи до побудови автоматизованих систем обслуговування користувачів із використанням генеративного штучного інтелекту. Розроблено архітектуру мультиагентної системи на базі Low-code платформи n8n, де центральний вузол (AI Supervisor) виконує маршрутизацію запитів між спеціалізованими агентами: юридичним консультантом (RAG) та генератором документів. Продемонстровано ефективність інтеграції векторних баз даних Pinecone та сервісів Google Workspace для автоматизації рутинних бізнес-процесів.*

Ключові слова: *n8n, AI Supervisor, мультиагентні системи, RAG, Pinecone, автоматизація, LLM, Google Gemini.*

Abstract. *The paper investigates approaches to building automated user service systems using generative artificial intelligence. A multi-agent system architecture based on the n8n Low-code platform was developed, where a central node (AI Supervisor) routes requests between specialized agents: a legal consultant (RAG) and a document generator. The effectiveness of integrating Pinecone vector databases and Google Workspace services for automating routine business processes is demonstrated.*

Keywords: *n8n, AI Supervisor, multi-agent systems, RAG, Pinecone, automation, LLM, Google Gemini.*

Стрімкий розвиток великих мовних моделей (LLM) дозволяє перейти від простих чат-ботів до складних мультиагентних систем, здатних виконувати різнопланові завдання в межах одного інтерфейсу. Проте інтеграція різних інструментів (пошук у базі знань, генерація файлів, доступ до API) часто вимагає складної розробки. Метою роботи є розробка та практична реалізація архітектури інтелектуального асистента на базі платформи n8n, який використовує патерн "Supervisor" для керування спеціалізованими агентами. Для реалізації системи обрано візуальне середовище n8n, що дозволяє поєднувати AI-ланцюжки (LangChain) із зовнішніми вебхуками. Топологія системи включає: вхідний канал (чат-інтерфейс), центральний роутер (AI Supervisor) та виконавчі інструменти.

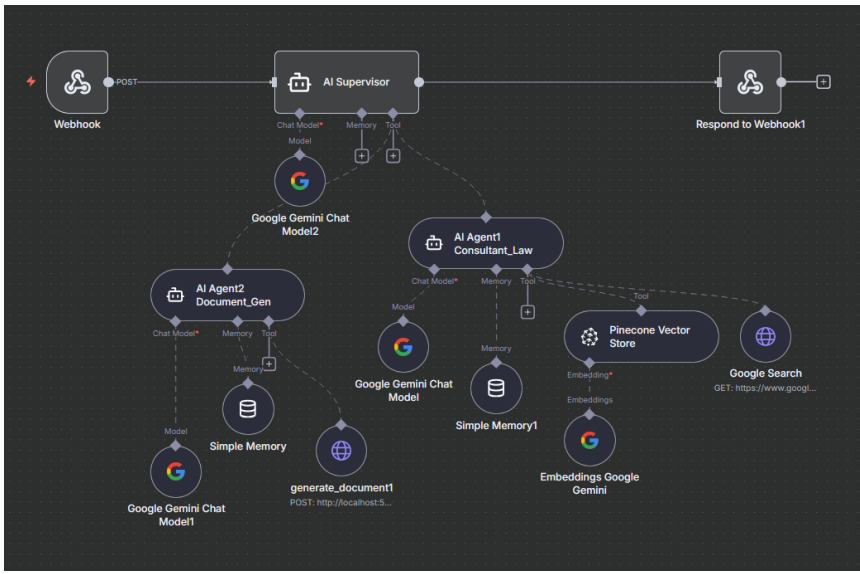

Рисунок 1 – Загальна схема мультиагентної системи в середовищі n8n (AI Supervisor та підлеглі агенти)

В ході дослідження реалізовано логіку роботи трьох ключових компонентів:

1. **AI Supervisor (Майстер-Роутер).** Виступає в ролі оркестратора. Він аналізує вхідний текст користувача, визначає інтенцію (намір) та передає виконання одному з підключених агентів-інструментів, не генеруючи відповідь самостійно.

2. **Агент юридичної консультації (RAG).** Використовує технологію Retrieval-Augmented Generation. Для забезпечення точності відповідей з питань законодавства підключено векторну базу даних Pinecone. Попередньо оброблені тексти законів перетворюються на вектори (Embeddings) за допомогою моделі Google Gemini та завантажуються у сховище.

3. **Агент генерації документів.** Працює в режимі заповнення слотів (Slot Filling). Агент збирає необхідні дані від користувача (ПІБ, деталі заяви) і передає їх на зовнішній Workflow. Цей процес автоматично створює документ у Google Docs за шаблоном, зберігає його на Google Drive та повертає посилання користувачу.

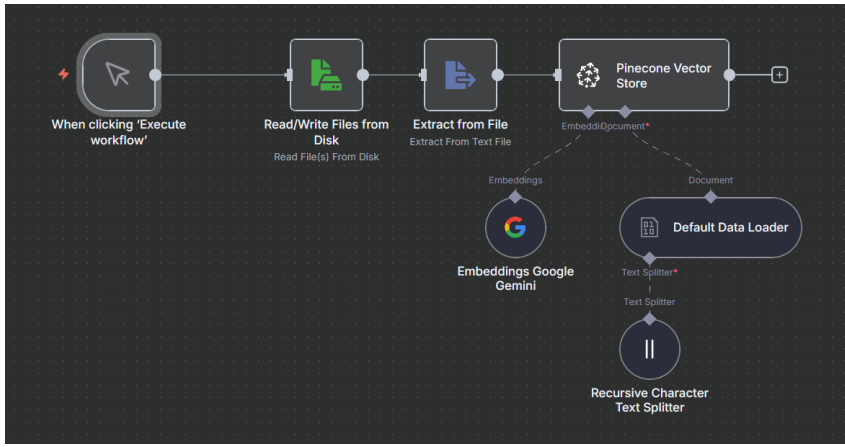

Рисунок 2 – Процес векторизації даних та завантаження в Pinecone Vector Store.

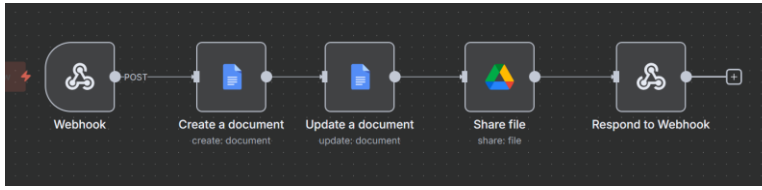

Рисунок 3 – Автоматизований ланцюжок створення та поширення документа через Google Drive API.

Висновки. Запропонована архітектура дозволяє створити гнучку систему підтримки, яка легко масштабується шляхом додавання нових агентів-інструментів без зміни основної логіки Супервайзера. Використання n8n значно знижує поріг входження в розробку складних AI-додатків, забезпечуючи при цьому високу функціональність завдяки інтеграції з хмарними сервісами.

Література

1. **n8n.** How to build AI Agents with n8n | Crash Course. YouTube. 2024. URL: https://www.youtube.com/watch?v=s0X8C01tUkw

2. **Pinecone.io.** Introduction to Vector Databases for AI. *Pinecone Learning Center*. URL: https://www.pinecone.io/learn/vector-database/

3. **n8n Documentation.** Google Docs Node & Integrations. URL: https://docs.n8n.io/integrations/builtin/app-nodes/n8n-nodes-base.googledocs/

4. **Google Cloud.** Gemini API: Quickstart. *Google* AI *for Developers*. URL: https://ai.google.dev/gemini-api/docs/quickstart

ВИКОРИСТАННЯ ТЕХНОЛОГІЙ 3D-МОДЕЛЮВАННЯ У ПІДГОТОВЦІ ФАХІВЦІВ ПОЖЕЖНО-РЯТУВАЛЬНИХ СПЕЦІАЛЬНОСТЕЙ У КОНТЕКСТІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА СУЧАСНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Віра ДОВБНЯК
Львівський державний університет безпеки життєдіяльності

Цифровізація в сфері безпекових технологій спричинила появу нового покоління навчальних рішень, зокрема симуляційних комплексів на основі 3D-моделювання та VR/AR-технологій. Пожежно-рятувальні підрозділи працюють в умовах високого ризику, тому якість підготовки особового складу має ключове значення. Сучасні 3D-середовища дозволяють моделювати складні пожежні сценарії, поведінку диму та вогню, динаміку обвалів, роботу систем вентиляції та інші процеси, які складно відтворити у реальних умовах.

Однак такі навчальні системи одночасно є об’єктами кібер ризиків, оскільки містять критичні набори даних: цифрові моделі будівель, інформацію про системи безпеки, навчальні сценарії та телеметрію дій здобувачів освіти. Забезпечення їхньої інформаційної безпеки є необхідною умовою ефективного функціонування сучасних навчальних комплексів.

Застосування 3D-моделювання у навчальному процесі надає можливість відтворювати реалістичні та небезпечні сценарії, які складно змоделювати у фізичному просторі. До таких належать:

– пожежі у висотних будівлях;
– загоряння легкозаймистих матеріалів;
– аварійні ситуації з вибухонебезпечними речовинами;
– обвали конструкцій і складні операції пошуку та порятунку.

Це підвищує ефективність навчальних програм, але водночас створює нові виклики у сфері інформаційної безпеки. Цифрові дані, що використовуються у VR-тренажерах, можуть бути цінними для зловмисників. Їхній витік або модифікація становить загрозу для реальних об’єктів, тактичних методик і самих працівників служб порятунку.

Мета – дослідити можливості технологій 3D-моделювання у професійній підготовці пожежних фахівців та визначити підходи до забезпечення інформаційної безпеки таких систем.

Завдання дослідження:

1. Проаналізувати сучасні 3D- та VR-технології, що застосовуються у фаховій підготовці.

2. Визначити інформаційні ризики, властиві цифровим навчальним платформам.

3. Розробити рекомендації щодо захисту даних 3D-тренажерів.

4. Оцінити перспективи розвитку технологій у сфері безпечних симуляцій.

Для досягнення мети застосовано такі методи:

– аналіз програмних платформ та архітектури 3D-симуляцій;
– оцінка ризиків (risk assessment);
– побудова моделі загроз;
– аналіз мережевих протоколів і механізмів автентифікації;
– елементи тестування на проникнення;
– статистичний аналіз телеметрії користувачів VR-систем.

3D-моделювання дозволяє:

1. Реалістично відтворювати фізичні процеси пожежі. Сучасні рушії враховують температуру, швидкість горіння, вологість, електричні фактори, хімічні реакції.

2. Моделювати складні та небезпечні ситуації. Симуляції аварій на АЗС, вибухів у промислових комплексах, пожеж у лікарнях чи торгових центрах.

3. Створювати цифрові двійники будівель та інфраструктури на основі BIM-даних, лазерного сканування, креслень та планів.

4. Забезпечувати безпечне відпрацювання тактичних дій. Рятувальники можуть тренуватися у віртуальних сценаріях без ризику для життя.

5. Аналізувати поведінку курсантів. Телеметрія дозволяє фіксувати час реакції, якість рішень, координацію дій у групах.

Основні загрози

– несанкціонований доступ до 3D-моделей будівель;
– модифікація навчальних сценаріїв шляхом підміни файлів;
– перехоплення телеметрії (рухів, рішень, координат);
– атаки на програмні рушії та мережеву інфраструктуру;
– витік даних через хмарні сервіси;
– DDoS-атаки на VR-платформи.

Критично важливі дані, що потребують захисту:

– цифрові копії об’єктів;
– алгоритми пожежогасіння;
– конфігурація систем безпеки;
– записи тренувальних сесій;
– журнали інструкторів.

У ході роботи встановлено:

– 3D-моделювання значно підвищує якість навчання;

– VR-технології сприяють розвитку командної взаємодії та стійкості до стресових ситуацій;

– найбільш критичними ризиками є підміна сценаріїв, витік моделей та атаки на сервери симуляцій;

– запропоновані заходи кіберзахисту забезпечують надійну роботу тренажерних комплексів.

Технології 3D-моделювання та VR/AR є перспективним напрямом у підготовці фахівців пожежно-рятувальних спеціальностей. Вони надають можливість формувати компетентності, які неможливо отримати у традиційних умовах. Проте цифрові навчальні системи стають об'єктами кіберзагроз, тому їх захист є ключовою умовою ефективності.

Подальші дослідження слід спрямувати на: створення стандартів кіберзахисту VR-тренажерів, застосування штучного інтелекту для аналізу дій курсантів, розвиток систем автоматичного виявлення аномалій у симуляціях.

Література

1. Burbeck S. *Virtual Reality in Emergency Response Training: Technologies and Applications*. — Springer, 2021.
Flin R., Arbuthnot K. *Incident Command: Tales from the Hot Seat*. — CRC Press, 2020.
2. Lee K., Sohn J. "Cybersecurity Challenges in VR/AR Training Systems" // *Journal of Information Security*, 2022.
3. BIM Forum. *Level of Development Specification*. – 2020.
4. NFPA 1700: *Guide for Structural Fire Fighting*. National Fire Protection Association, 2021.
5. ISO/IEC 27001:2022 — Information Security Management Systems.
6. Sherman W. *Understanding Virtual Reality*. — Morgan Kaufmann, 2019.
7. Гнатюк С. Інформаційна безпека: сучасні загрози та технології захисту. — Київ: 2022.

УДК 004.8:004.932.4

ПОРІВНЯННЯ МОЖЛИВОСТЕЙ СУЧАСНИХ AI-МОДЕЛЕЙ У ЗАДАЧІ FACE SWAPPING

Ванесса ЄЗЕРСЬКА, Роман ГОЛОВАТИЙ
Львівський державний університет безпеки життєдіяльності

Анотація. *У роботі проведено розширений аналіз якості виконання задачі Face Swapping трьома сучасними моделями штучного інтелекту: Gemini, Ideogram та Grok. Основну увагу зосереджено на таких параметрах, як візуальна чіткість, природність синтезованих рис обличчя, збереження міміки та відповідність оригінальному джерелу. Детально описано механізм формування результату — від виявлення обличчя і вирівнювання ключових точок до генерації та підсумкового змішування зображення. На основі низки експериментів встановлено, що Gemini демонструє найвищу стабільність і точність заміни облич, забезпечуючи гармонійне поєднання нового обличчя із загальною сценою.*

Ключові слова: *Face Swapping, генеративні моделі, комп'ютерний зір, виявлення обличчя, Gemini, Ideogram, Grok.*

Abstract. *This paper examines the effectiveness of three contemporary AI systems—Google Gemini, Ideogram, and Grok—when performing face swapping tasks. The study focuses on evaluating the visual quality, realism, and semantic accuracy of generated faces by analyzing the alignment of facial landmarks, blending techniques, and stylistic consistency between the source and target images. Special attention is paid to the perceptual integrity of facial features as well as the models' ability to maintain the natural expressiveness and structural uniqueness of the original identity. The findings show that Gemini and Ideogram outperform Grok by providing more coherent results with fewer distortions and better adherence to the context of the scene.*

Keywords: *face swapping, generative models, image synthesis, Gemini, Ideogram, Grok, computer vision.*

Face Swapping як технологія комп'ютерного зору за останні роки досягла значного розвитку, і сучасні генеративні моделі здатні відтворювати обличчя з високою точністю. Алгоритм зазвичай включає три ключові етапи:

- виявлення обличчя (Face Detection);
- вирівнювання на основі ключових точок (Face Alignment);
- накладання та змішування (Synthesis and Blending).

Саме точність виконання цих етапів визначає якість підсумкового результату. Три моделі, обрані для порівняння — Gemini, Ideogram та Grok — по-різному реалізують ці процеси, що і стало об'єктом нашого аналізу.

Gemini продемонстрував найвищий рівень відповідності оригінальному зображенню. У більшості випадків нове обличчя виглядало практично невідрізним від того, яке мало бути вставлене. Чіткість деталей, збереження характерних рис, природна інтеграція з фоном та освітленням — усе це підкреслює високий ступінь когнітивної узгодженості.

На прикладі мистецьких зображень Gemini не лише зберіг стиль оригіналу, але й коректно відтворив міміку й напрямок погляду, що є складним завданням для штучного інтелекту. Тестові результати показали до 99,9% схожості між оригіналом і згенерованим обличчям.

Ideogram також показав високу точність у відтворенні рис обличчя. Модель зберегла форму очей, носа та рота, а також виконувала коректне поєднання з ракурсом оригінального зображення.

Разом із тим у деяких випадках спостерігалися:

- легкі зміни кольорової температури шкіри;
- невелике падіння деталізації;
- штучні переходи між областями змішування.

Попри це, Ideogram забезпечував реалістичну передачу стилістики персонажів, що особливо помітно у випадках з мультяшними образами, де важливо зберегти художні риси.

У порівнянні з двома попередніми моделями Grok найчастіше демонстрував нижчу точність. Хоча загальні риси обличчя передавалися правильно, найпомітніші недоліки включали:

- спотворені або "скляні" очі,
- надто гладку або неприродну шкіру,
- відсутність коректної міміки,
- недостатній збіг пропорцій.

Оцінювання та узагальнення результатів. Порівняння демонструє, що точність Face Swapping прямо залежить від здатності моделі правильно розпізнати контури обличчя та його ключові точки. Обидві моделі — Gemini та Ideogram — здатні забезпечити плавні переходи, реалістичне освітлення та точне збереження виразу обличчя. Grok же часто має труднощі з природністю генерації, що призводить до менш якісних результатів. Під час аналізу було виявлено, що Gemini найкраще справляється із збереженням структурної унікальності обличчя, тоді як Ideogram інколи втрачає частину мікродеталей. Проте обидві моделі перевершують Grok у більшості критеріїв.

Висновки. Отже, результати проведеного дослідження свідчать, що Gemini та Ideogram є найбільш ефективними інструментами для задач Face Swapping. Вони демонструють високу якість синтезу, точність вирівню-

вання та природність підсумкового зображення. Grok, незважаючи на здатність виконувати базові операції, поки що поступається конкурентам у точності накладання та збереженні міміки.

Таким чином, для практичного використання в проектах, де важлива реалістичність і точна передача обличчя, доцільно обирати Gemini або Ideogram.

Література

1. Google AI. Gemini: Multimodal Large Model Capabilities and Applications. Google Research Publications, 2024. URL: https://ai.googleblog.com (дата звернення: 10.11.2025).

2. Ideogram Inc. Ideogram Model Overview and Image Generation Framework. Офіційна документація, 2023. URL: https://ideogram.ai/docs (дата звернення: 10.11.2025).

3. Зачко О.Б., Головатий Р.Р. Мультиагентна модель управління безпекою при плануванні проектів створення об'єктів з масовим перебуванням людей // Вісник НТУ «ХПІ». Серія: Стратегічне управління, управління портфелями, програмами та проектами. – Х.: НТУ «ХПІ», 2017. – № 2 (1224) – С. 46-51.

4. xAI. Grok Technical Report. xAI Official Documentation, 2024. URL: https://x.ai/docs (дата звернення: 10.11.2025).

УДК 004.8:658.5

ОБГРУНТУВАННЯ КОНЦЕПЦІЇ ІНТЕЛЕКТУАЛЬНОЇ СИСТЕМИ ДЛЯ ОБСЛУГОВУВАННЯ ТА РЕМОНТУ СІЛЬСЬКОГОСПОДАРСЬКОЇ ТЕХНІКИ

Роман-Ростислав ЖУКОВСЬКИЙ
Львівський національний університет ветеринарної медицини та біотехнологій імені С.З. Ґжицького

Розглянуто необхідність впровадження інтелектуальної інформаційної системи для доступу до інструкцій з обслуговування та ремонту сільськогосподарської техніки. Визначено її значення для підвищення точності та оперативності сервісного інжинірингу в аграрному секторі.

Ключові слова: *інтелектуальна система, сервісний інжиніринг, обслуговування, ремонт, агротехніка.*

The need to implement an intelligent information system for access to instructions for maintenance and repair of agricultural machinery is considered. Its importance for increasing the accuracy and efficiency of service engineering in the agricultural sector has been determined.

Keywords: *intelligent system, service engineering, maintenance, repair, agricultural machinery.*

Стрімкий розвиток цифрових технологій у сільському господарстві зумовлює потребу у впровадженні спеціалізованих інформаційних систем для підтримки сервісних процесів. Зокрема, ефективне технічне обслуговування і ремонт складної сільськогосподарської техніки вимагає швидкого доступу до великого обсягу технічної документації, що включає інструкції з експлуатації, регламенти з технічного обслуговування, схеми вузлів, рекомендації з усунення несправностей та сервісні бюлетені.

Існуючі довідники, каталоги та інформаційні системи для обслуговування техніки часто мають фрагментарний характер, не забезпечують швидкого пошуку інструкцій, а також не інтегруються з реальними сервісними процесами. У критичних ситуаціях поломка техніки може вплинути на швидкість і якість відновлення, а отже прямопропорційно на економічні результати підприємства. В цілому розвиток сервісного інжинірингу на основі інформаційних технологій має передбачати підвищення ефективності та зменшення часу на реалізацію проектів з обслуговування та ремонту сільськогосподарської техніки.

Аналіз наукових досліджень із зазначеної тематики показав, що існує позитивний вплив інтелектуальних технологій, зокрема штучного інтелекту на вирішення задач, пов’язаних із технічним обслуговуванням, ремонтом та заміною запчастин [1, 2]. Дослідження підтверджують, що сільськогосподарські підприємства не завжди розуміють перспективи використання інтелектуальних систем для вирішення прикладних задач в напрямку автоматизації бізнес-процесів. З іншої сторони сільськогосподарські виро-

бники мають накопичений практичний досвід реальних кейсів ремонту обладнання як на основі класичних інструкцій, так і шляхом практичної взаємозаміни дефіцитних запчастин. Фермери та відповідальні працівники сільськогосподарських підприємств, які вже виконали ремонт, можуть формувати інструкції чи кейси, доступні іншим, формуючи на основі цього механізм накопичення знань в даній предметній області.

Запропонована інтелектуальна інформаційна система покликана централізовано акумулювати, систематизувати та надавати користувачам доступ до повного комплексу технічних матеріалів для кожної одиниці техніки. Такий підхід дозволяє скоротити час пошуку необхідної інформації, зменшити кількість помилок під час діагностики та ремонту, уніфікувати підходи до обслуговування техніки в межах підприємства або сервісної мережі.

Ключова відмінність розроблюваної системи – динамічна база знань, яка оновлюється в процесі практичного використання. Сервісні інженери можуть залишати власні коментарі до інструкцій, фіксувати нетипові несправності та запропоновані рішення, що дозволяє системі накопичувати колективний досвід та надавати користувачам не лише офіційні, а й практично перевірені матеріали.

Інтелектуальні функції включатимуть можливості пошуку за ключовими словами, автоматичне визначення релевантних документів на основі опису проблеми, контекстну підказку та інтеграцію з базою типових несправностей. Це значно підвищить продуктивність роботи сервісного персоналу, особливо в умовах сезонного навантаження або кадрового дефіциту.

Практичне впровадження такої системи може бути реалізовано як у межах великого аграрного холдингу, так і для підтримки невеликих сервісних центрів або навчальних закладів. Система здатна підтримувати кілька мов інтерфейсу, різні рівні доступу (механік, інженер, адміністратор) і адаптуватися до техніки від різних виробників.

Таким чином, запропонована інтелектуальна інформаційна система сприятиме зниженню ризиків простою техніки, покращенню якості обслуговування та формуванню єдиного цифрового простору сервісної підтримки сільськогосподарських машин.

Література

1. Kisten M, Ezugwu A. E.-S., Olusanya M. O. Explainable Artificial Intelligence Model for Predictive Maintenance in Smart Agricultural Facilities, in IEEE Access, vol. 12, pp. 24348-24367, 2024, doi: 10.1109/ACCESS.2024.3365586.

2. Rakhra M., Sarkar T., Sharma V., Angra P.K., Kumar A., P. Singh P. An In-Depth Analysis Of Local Mechanic Support For Immediately Apparent Repairs And Scheduled Maintenance Services, 2024 International Conference on Electrical Electronics and Computing Technologies (ICEECT), Greater Noida, India, 2024, pp. 1-7, doi: 10.1109/ICEECT61758.2024.10739024.

УДК 378.147:004:811:111

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ПРОФЕСІЙНІЙ ІНШОМОВНІЙ ПІДГОТОВЦІ МАЙБУТНІХ ФАХІВЦІВ ЦИВІЛЬНОГО ЗАХИСТУ

Наталія ІВАНИШИН
Львівський державний університет безпеки життєдіяльності

У роботі висвітлено роль сучасних цифрових платформ у професійній іншомовній підготовці майбутніх фахівців цивільного захисту. Проаналізовано функціональні можливості освітніх сервісів TeachShare, TWEE, YouGlish, NoteGPT.io та Miro як ефективних інструментів розвитку іншомовної комунікативної, термінологічної й цифрової компетентностей. Підкреслено доцільність інтеграції таких технологій у навчальний процес у закладах вищої освіти цивільного захисту.

Ключові слова: *інформаційні технології, цифровізація освіти, професійна іншомовна підготовка, цивільний захист, освітні платформи.*

The paper highlights the role of modern digital platforms in the professional foreign language training of future civil protection specialists. The functional capabilities of educational services such as TeachShare, TWEE, YouGlish, NoteGPT.io, and Miro are analyzed as effective tools for developing communicative, terminological, and digital competencies. The importance of integrating these technologies into the educational process of higher education institutions in the field of civil protection is emphasized.

Keywords: *information technologies, digitalization of education, professional foreign language training, civil protection, educational platforms.*

Сучасна професійна освіта у сфері цивільного захисту неможлива без використання інформаційно-комунікаційних технологій (ІКТ), які забезпечують доступ до автентичних джерел, сприяють розвитку цифрової грамотності, критичного мислення та комунікативних навичок. Особливого значення набуває інтеграція ІКТ у процес іншомовної підготовки, адже володіння іноземною мовою фахівцем цивільного захисту є не лише засобом професійної комунікації, а й елементом інформаційної безпеки під час міжнародної взаємодії.

Використання освітніх платформ нового покоління у процесі підготовки фахівців цивільного захисту дозволяє поєднувати традиційні педагогічні методи з технологіями штучного інтелекту, автоматизованого тестування, аналітики навчальних даних і колаборативної взаємодії.

Платформа TeachShare призначена для створення, поширення та спільного використання навчальних матеріалів. Вона дає змогу викладачам розробляти інтерактивні завдання, вікторини та тести, які можна адаптувати під конкретні професійні теми, наприклад, «Disaster Risk Management» чи «Emergency Response». TeachShare підтримує створення колективних курсів, де викладачі можуть обмінюватися методиками навчання іноземної мови за професійним спрямуванням, формувати спільні глосарії та бази знань. Це сприяє розвитку комунікації між НПП, які готують фахівців у сфері безпеки.

1.TWEE – це інноваційний сервіс для генерації завдань із вивчення мови на основі будь-якого відео, тексту або аудіо. За допомогою штучного інтелекту система створює вправи різного типу: заповнення пропусків,

множинний вибір, переклад, формування словникових наборів.У контексті підготовки фахівців цивільного захисту TWEE можна використовувати для аналізу автентичних відеоматеріалів НАТО, Європейської комісії з питань цивільного захисту чи міжнародних гуманітарних місій. Це допомагає здобувачам не лише покращувати знання термінології, але й засвоювати мовні моделі, типові для кризових комунікацій і звітів про надзвичайні ситуації.

2.YouGlish – потужний онлайн-інструмент для вдосконалення вимови та розуміння контексту використання фахової лексики. Користувач вводить будь-яке слово чи фразу (наприклад, evacuation route або hazard assessment), і система підбирає відеофрагменти з YouTube, де це слово звучить у природному контексті. Такий підхід дозволяє здобувачам сприймати професійні терміни в реальних комунікативних ситуаціях, розвиваючи навички аудіювання та фонетичну компетентність. Для майбутніх перекладачів і рятувальників це особливо важливо, адже правильна вимова та розуміння слова в контексті можуть мати вирішальне значення під час міжнародних навчань або спільних операцій.

3.Платформа NoteGPT.io використовує технології штучного інтелекту для автоматичного створення конспектів, резюме та глосаріїв із текстів або відеолекцій. У процесі іншомовної підготовки студентів цивільного захисту цей інструмент допомагає структурувати велику кількість термінологічної інформації, створювати персоналізовані словники за темами «Emergency Response Coordination», «Rescue Operations», «Civil Protection Framework» тощо. Крім того, NoteGPT.io сприяє розвитку навичок академічного письма, оскільки допомагає студентам правильно формулювати висновки, підбирати релевантні приклади та перекладати технічні тексти.

4.Онлайн-дошка Miro – універсальний інструмент для візуалізації навчального матеріалу. У процесі навчання іноземної мови вона може використовуватися для створення mind maps, термінологічних карт, сценаріїв діалогів, а також для планування перекладацьких проєктів. У роботі зі здобувачами у сфері цивільного захисту Miro особливо ефективна для групових занять, де потрібно моделювати комунікацію між учасниками рятувальної операції чи аналізувати англомовні документи міжнародних організацій. Платформа забезпечує інтерактивність, візуальну наочність і командну взаємодію, що підвищує мотивацію здобувачів.

Інтеграція цих платформ сприяє розвитку сучасних ключових компетентностей – комунікативної, цифрової, міжкультурної та аналітичної, що формує готовність майбутніх фахівців цивільного захисту діяти в умовах сучасних викликів.

Література

1. YouGlish. How to pronounce English like a native. URL: https://youglish.com/ (дата звернення: 10.11.2025).

2. Twee. AI-Powered tools for language educators. URL : https://twee.com (дата звернення: 10.11.2025).

3. TeachShare. Platform for creating and sharing interactive lessons. URL :https://www.teachshare.com) (дата звернення: 10.11.2025).

УДК 004.8:004.94:72(477)

THE USE OF AI IN PRESERVING WAR-DAMAGED ARCHITECTURE IN UKRAINE

Marta IVASIV
Lviv Polytechnic National University, Lviv

The role of artificial intelligence in recording damage and supporting the reconstruction of Ukrainian cities affected by the war. The article examines modern technologies that help architects and local administrations to quickly assess damage, create 3D models, and propose restoration options. Examples of Ukrainian projects are given, including RE:Ukraine Vision, tools for automated modelling, and developments by Balbek Bureau. The article shows how artificial intelligence contributes to faster, more accurate, and more sustainable recovery, while emphasising that it cannot replace human professional experience and understanding of the cultural context.

Keywords: *architecture, AI, war.*

Роль штучного інтелекту у фіксації руйнувань та підтримці відбудови українських міст унаслідок війни. Розглядаються сучасні технології, які допомагають архітекторам та місцевим адміністраціям оперативно оцінювати пошкодження, створювати 3D-моделі та пропонувати варіанти реставрації. Наведено приклади українських проєктів, зокрема RE:Ukraine Vision, інструментів для автоматизованого моделювання та розробок Balbek Bureau. Показано, як штучний інтелект сприяє швидшому, точнішому та більш сталому відновленню, водночас підкреслюючи, що він не здатний замінити людський професійний досвід і розуміння культурного контексту.

Ключові слова: *архітектура, ШІ, війна.*

The war in Ukraine has caused widespread destruction of cities and cultural heritage. Many buildings that shaped the identity of communities have been partially or completely destroyed. In these circumstances, artificial intelligence has become an unexpectedly powerful tool for documenting the destruction and supporting future reconstruction. Modern AI technologies help architects, local authorities and researchers understand how this can be restored.

One of the most interesting examples is the Ukrainian project RE:Ukraine Vision. It allows users to photograph a destroyed building and instantly see a possible restoration option generated using artificial intelligence and augmented reality. This approach not only creates visual concepts for future reconstruction, but also plays a psychological role — it helps people see that reconstruction is possible. The project makes reconstruction more understandable and accessible, allowing residents to imagine the future of their cities and neighbourhoods.

Another important area is AI modelling. A team supported by Microsoft has created a prototype tool that analyses photographs and drawings, converting

them into detailed three-dimensional models of destroyed buildings. This technology has already been tested on the House of Culture in Irpin. Its purpose is to help local administrations quickly assess the extent of damage, calculate costs, and identify priority objects for restoration. AI significantly speeds up these processes and increases accuracy compared to traditional methods.

The Ukrainian architectural firm Balbek Bureau is also actively developing AI solutions for reconstruction. Architects are training neural networks on thousands of their own visualisations sothat AI can offer realistic and structurally feasible options for restoring destroyed buildings. In the future, users will be able to take photos of ruins and receive several reconstruction options, which will significantly speed up the initial design stage.

Another area of application is the recognition of materials in destroyed buildings. AI can identify bricks, concrete, metal or glass directly from drone images. This makes it possible to calculate which materials can be reused, ensuring a more environmentally friendly and sustainable approach to reconstruction.

Despite significant achievements, artificial intelligence cannot replace architects. It is not capable of understanding the cultural context, historical value or emotions associated with a particular place. However, AI provides specialists with data, models and concepts much faster than before.

Thus, artificial intelligence has become a valuable tool in preserving Ukraine's architectural heritage during the war. It helps document destruction, visualise possible reconstruction options, and make the reconstruction process more efficient. The combination of technology and human creativity provides an opportunity to rebuild destroyed cities and create stronger and more sustainable buildings for the future.

Література

1. RE:Ukraine. RE:Ukraine vision: Virtual image of recovery. https://www.reukraine.org/vision-eng

2. Digital State. Microsoft відзначила український AI-проєкт для реконструкції зруйнованих будівель. https://digitalstate.gov.ua/uk/news/tech/microsoft-vidznachyla-ukrayinskyy-ai-proyekt-dlia-rekonstruktsiyi-zruynovanykh-budivel

3. PRAGMATIKA.MEDIA. Balbek Bureau. https://pragmatika.media/tag/balbek-bureau/

4. LIGA.net. Balbek Bureau. https://www.liga.net/ua/tag/balbek-bureau

5. Rubryka. (2024, December 18). Онлайн-конструктор відбудови: як Balbek Bureau застосовує цифрові інструменти для реконструкції. https://rubryka.com/2024/12/18/onlajn-konstruktora-vidbudovy/

УДК: 004.8:001.89

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В НАУКОВИХ ДОСЛІДЖЕННЯХ

Анастасія ІЛЬКІВ, Андрій ІВАНУСА
Львівський державний університет безпеки життєдіяльності

Об'єкт дослідження – штучний інтелект.

Предмет дослідження – використання штучного інтелекту у наукових дослідженнях.

Мета роботи – виявлення певеваг та недоліків використання штучного інтелекту у наукових дослідженнях.

Робота спрямована на Виявлення певеваг та недоліків використання штучного інтелекту у наукових дослідженнях. Проведено аналіз певеваг та недоліків використання штучного інтелекту у наукових дослідженнях

***Ключові слова**: штучний інтелект, наукові дослідження, машинне навчання, аналіз даних, інтелектуальні системи.*

The object of study – artificial intelligence.

Subject of study – usage of artificial intelligence in scientific research.

Purpose – identifying advantages and disadvantages of using artificial intelligence in scientific research.

The work is aimed studying identifying advantages and disadvantages of using artificial intelligence in scientific research. Were made analysis of advantages and disadvantages of using artificial intelligence in scientific research

***Keywords**: artificial intelligence, scientific research, machine learning, data analysis, intelligent systems*

Тема використання штучного інтелекту є надзвичайно актуальною в сучасному світі. ШІ стає все більш невіддільною частиною повсякденного життя, а його застосування знаходить відображення у різних сферах, від побуту до професійної діяльності. Проте, однією з областей, де ШІ може мати особливо значимий вплив, є наукова сфера, а точніше, процес наукового письма та публікацій. В період розвитку інноваційних технологій постає питання використання штучного інтелекту (ШІ) у науковій діяльності.

Використання ШІ в процесі підготовки та написання наукових робіт допомагає вченим оптимізувати час, аналізувати великі обсяги даних та підвищувати ефективність досліджень. Важливо зрозуміти чи є використання ШІ доцільним в цих процесах. Останніми роками питання про використання ШІ в наукових дослідженнях є актуальним, та привертає багато уваги. Дехто підтримує використання цієї технології, а інші виступають проти. Тож розглянемо, які перспективи відкриває ШІ перед науковцями, а також які проблеми виникають у процесі його використання.

Переваги використання штучного інтелекту у наукових дослідженнях:

генерація та формулювання нових ідей; пошук актуальних джерел; аналіз та обробка великих обсягів інформації; переклад тексту; покращення тексту наукової статті; створення графічного матеріалу; перевірка тексту на плагіат; генерація нових гіпотез; моделювання складних систем; синтез нових матеріалів і засобів; автоматизована обробка зображень і відео; оптимізація експериментів; підвищення точності передбачень; поліпшення управління науковими проектами.

Недоліки використання штучного інтелекту у наукових дослідженнях :

порушення принципів наукової етики та академічної доброчесності; помилкові результати; Конфіденційність даних; Питання безпеки і кіберзагрози; Неточність перекладу тексту; Залежність від технології; Недостовірність даних; Навчання та освіта; Ефект втрати робочих місць; Ліміти та обмеження; Витрати на впровадження; Відсутність інтерпретації; Конкуренція та доступність; Прозорість та відповідальність; Соціокультурні виклики.

Згідно з проєктом законопроєкту «Про академічну доброчесність» [3], академічний плагіат визначається як публікація результатів власної академічної діяльності або текстів і/або результатів, згенерованих автоматичним комп'ютерним програмним забезпеченням, без вказівки на цей факт у самому академічному творі чи його супровідних матеріалах. Якщо виявлено академічний плагіат в оприлюдненому творі, такий твір підлягає відкликанню. У разі вчинення академічного плагіату шляхом передання авторства педагогічним, науково-педагогічним або науковим працівником закладу освіти, наукової установи чи вченим, така особа:

Втрачає науковий ступінь, вчене (педагогічне) звання та/або кваліфікаційну категорію, якщо ці звання чи категорії були присуджені або присвоєні на основі або з урахуванням відповідного академічного твору чи його частини.

Підлягає звільненню із закладу освіти або наукової установи.

У випадку академічного плагіату, скоєного здобувачем вищої освіти через передання авторства на кваліфікаційну роботу, такий здобувач підлягає відрахуванню із закладу вищої освіти або наукової установи.

Використання штучного інтелекту у наукових дослідженнях має потенціал перетворити спосіб збору, аналізу та використання наукової інформації. Можливості використання ШІ в наукових дослідженнях включають автоматизований аналіз даних, пошук наукових статей, підтримку в прийнятті рішень, генерацію нових гіпотез, моделювання складних систем, синтез нових матеріалів, автоматизовану обробку зображень, оптимізацію експериментів та багато інших. Ці можливості розширюють горизонти наукових досліджень і забезпечують більш точні результати. Загальна ідея полягає в тому, що ШІ стає надзвичайно важливим інструментом для наукової спільноти, який може значно полегшити й прискорити проведення досліджень і забезпечити більш точні результати. Проте, важливо ретельно враховувати всі можливі наслідки та ризики, щоб забезпечити відповідальне та ефективне використання цієї технології в наукових дослідженнях. Перед нами стоїть завдання розвивати станда-

рти, етичні норми та стратегії для налагодження балансу між можливостями та викликами ШІ в освіті та наукових дослідженнях.

Література

1. Штучний інтелект при підготовці наукової роботи: можливості та виклики [Електронний ресурс] // Наука та метрика. — 2025. — 25 лютого. — Режим доступу: https://nim.media/articles/shtuchny-intelekt-pri-pidgotovtsi-naukovoyi-roboti-mozhlivosti-ta-vikliki (дата звернення: 18.11.2025)

2. Використання штучного інтелекту при написанні наукової статті [Електронний ресурс] // Наукові Публікації : [веб-сайт]. — 2024. — 12 листопада. — Режим доступу: https://spubl.com.ua/uk/blog/using-artificial-intelligence-when-writing-a-scientific-article (дата звернення: 18.11.2025)..

3. Проєкт Закону про академічну доброчесність [Електронний ресурс] : проєкт Закону України № 10392 від 08.01.2024 // Офіційний портал Верховної Ради України. — Київ, 2024. — Режим доступу: https://itd.rada.gov.ua/billinfo/Bills/Card/43481 (дата звернення: 18.11.2025)

ПЕРСПЕКТИВИ ВИКОРИСТАННЯ БЕЗПІЛОТНИХ СИСТЕМ В УКРАЇНІ ПІД ЧАС ВІДНОВЛЮВАНОГО ПЕРІОДУ

Михайло КАРПУНЕЦЬ, Андрій ГАВРИСЬ
Львівський державний університету безпеки життєдіяльності, м. Львів

Анотація. *Аналіз європейського досвіду застосування безпілотних літальних апаратів у цивільному секторі показав стратегічні перспективи їхньої повномасштабної інтеграції в Україні в післявоєнний період.*

Наразі розвиток цивільних дронів в Україні обмежений через дію правового режиму воєнного стану, що контрастує зі значним прогресом у країнах ЄС. Європейська практика демонструє інноваційні рішення, зокрема використання медичних дронів (SkySaver, Everdrone) для швидкої доставки критичних вантажів та дефібриляторів, застосування безпілотників у пожежогасінні та високоточних системах в аграрному секторі (AgroDroneVision).

На основі аналізу передових, гібридних та модульних технологій (VTOL-дрони від Quantum-Systems) зроблено висновок, що після завершення воєнних дій Україна матиме унікальну можливість здійснити технологічний стрибок. Швидке впровадження безпілотних систем у критичну інфраструктуру та сільське господарство стане ключовим фактором економічного та соціального відновлення, забезпечуючи швидкість, точність та доступ до віддалених територій.

Ключові слова: *безпілотні літальні апарати, критична інфраструктура, цивільний захист, пожежогасіння.*

У країнах Європейського Союзу активно впроваджуються інноваційні технології у сфері безпілотних літальних апаратів (БПЛА). Багато з цих рішень або зовсім не використовуються в Україні, або перебувають на етапі обмеже-

них пілотних проєктів, оскільки є заборона у застосуванні БПЛА під час дії правового режиму воєнного стану [1]. Європейська практика демонструє значне розширення використання дронів у цивільному секторі, державних службах та рятувальних операціях. Одним із найбільш розвинених напрямів є застосування медичних дронів.

У Європі розвивається багато інноваційних безпілотних технологій, які можуть бути корисними для різних сфер, в тому числі в нашій країні у після воєнний період. Наприклад, у рамках програми Horizon 2020 реалізується проєкт SkySaver (Avy) — VTOL-дрон, здатний транспортувати медичні вантажі на великі відстані, такі як кров, дефібрилятори або вакцини. Цей дрон може долати приблизно 150 км, що значно скорочує час доставки в порівнянні з традиційною наземною логістикою [2].

У Швеції розгорнута система автономних дронів компанії Everdrone, які доставляють дефібрилятори (AED) до місць раптової зупинки серця. Такі апарати стартують зі спеціальних станцій Skybases та здатні прибувати до пацієнта на кілька хвилин швидше за карету швидкої допомоги [2]. Це значно підвищує шанси на порятунок життя. Подібних масштабних сервісів швидкої медичної доставки дронами в Україні поки не існує. Цікавим прикладом є використання дронів у пожежних службах Гельсінкі, Фінляндія. Безпілотники обладнані тепловізорами, що дозволяє моніторити осередки пожежі, визначати напрямок поширення вогню та знаходити людей у задимлених приміщеннях. Крім цього, в рамках проєкту AiRMOUR дрони доставляли адреналін на острів, де людині знадобилася термінова допомога [2]. У Швейцарії, Австрії та Італії БПЛА використовуються для доставки дефібриляторів та лікарських засобів туристам і альпіністам у важкодоступних місцях. Це демонструє практичне застосування безпілотників як елементів медичної допомоги у важкодоступних місцях.

На сьогоднішній день в Україні БПЛА також широко використовуються рятувальниками, але поки без створення єдиної національної системи управління безпілотними системами [3, 4].

Аграрний сектор Європи також активно користується сучасними цифровими інструментами. Платформа AgroDroneVision EU поєднує супутникові дані, зображення з дронів, аналіз ґрунту та автоматичне внесення добрив за допомогою штучного інтелекту (ШІ). Аналогічно, SmartIrrigation забезпечує повністю автоматизовані системи поливу на основі датчиків вологості та прогнозів погоди [2].

Серед європейських виробників варто виділити чеський дрон ThunderFly TF-G2, який здатний працювати у складних метеоумовах та використовуватися для наукових і пошукових місій. Німецька компанія Quantum-Systems розробляє високотехнологічні дрони VTOL (вертикальний зліт і посадка), які застосовуються в обороні, а також у цивільних задачах — агромоніторинг, картографування та логістика. Цікавою є також концепція модульних дронів, здатних змінювати свою конфігурацію залежно від вантажу: додавати або прибирати модулі, змінювати кількість пропелерів чи форму корпусу. Це

дає можливість використовувати один дрон для перевезення різних типів вантажів, змінюючи його конфігурацію під потреби завдання.

Європейські науковці також експериментують із гібридними дронами, зокрема воднево-батарейними, як-от дрон NederDrone, який поєднує VTOL-зліт і тривалий горизонтальний політ [2]. Завдяки такій "гібридній" системі живлення він може виконувати довгі місії з мінімальними екологічними витратами.

Обмеження на застосування БПЛА в цивільному секторі України є необхідною мірою в умовах воєнного стану, що істотно стримує розвиток цієї сфери порівняно з ЄС. Проте саме багатство європейської практики (від SkySaver для логістики крові до платформ SmartIrrigation в агросекторі) слугує переконливим доказом величезних нереалізованих можливостей для нашої країни.

Таким чином, у відновлюваний період після завершення воєнних дій, Україна матиме унікальну можливість не просто наслідувати, а й швидко інтегрувати ці передові, гібридні та модульні БПЛА-технології у цивільний сектор — від критичної медичної логістики у важкодоступних районах до високоточного агромоніторингу за допомогою ШІ. Впровадження БПЛА у надання медичної допомоги, рятувальні служби та сільське господарство стане важливим фактором економічного та соціального відновлення, забезпечуючи швидкість, точність та доступ до віддалених територій. Це дозволить Україні здійснити технологічний стрибок, використовуючи безпілотні системи як ключовий елемент ефективного та швидкого післявоєнного відновлення.

Література

1. Гаврись А.П., Лаврівський М.З., Філіппова В.В., Марценюк А. (2024) Аналіз ефективності та перспектив застосування безпілотних літальних апаратів у сфері цивільного захисту. Міжнародний науковий журнал «Грааль науки». – Відень. – Листопад, 2024. – №46. – с.531-546. https://doi.org/10.36074/grail-of-science.29.11.2024.

2. Офіційний сайт Проектів Європейського Союзу. Режим доступу – https://trimis.ec.europa.eu/project/electric-vtol-fixed-wing-drone-urgent-medical-delivery?utm_source.

3. Havrys, A. P., Lavrivskyi, M. Z., Liubovetskyi, O. V., Tarnavskyi, A. B., Kravets, I. I., & Rykhva, V. V. (2025). Проблемні питання інтеграції технологій безпілотних літальних апаратів у сферу цивільного захисту. Вісник Львівського державного університету безпеки життєдіяльності, 31, 165-175.

4. Havrys, A., Veselivsky, R., Pekarska, O., Liubovetskyi, O., Filippova, V., 2025. Support system for management decision-making by heads of hydrological emergency situations liquidation using geo-information technologies. Municipal economy of cities 1, 416–427.. https://doi.org/10.33042/2522-1809-2025-1-189-416-427.

УДК 004.94:528.93:72:7.025 (477)

DIGITAL MODELS AND 3D SCANNING IN PRESERVING ARCHITECTURAL HERITAGE DURING WAR

Vasylyna KIT
Lviv Polytechnic National University, Lviv

Abstract. *Digital models and 3D scanning play a crucial role in documenting, preserving, and restoring architectural heritage endangered by war. They enable accurate recording of damage, support reconstruction efforts, allow virtual access to destroyed sites, and provide evidence of cultural heritage destruction for legal and research purposes.*

Keywords: *digital models, 3D scanning, architectural heritage, war, preservation.*

Анотація. *Цифрові моделі й 3D-сканування відіграють важливу роль у збереженні архітектурної спадщини, що перебуває під загрозою війни. Технології забезпечують точну фіксацію стану об'єктів, сприяють реставрації, надають віртуальний доступ та допомагають документувати руйнування для юридичних цілей.*

Ключові слова: *цифрові моделі, 3D-сканування, архітектурна спадщина, війна, збереження.*

Armed conflicts continue to pose a significant threat to the architectural heritage of many nations. Historic buildings, monuments, religious sites, and cultural landscapes often become collateral damage or deliberate targets, leading to irreversible cultural losses. In this context, digital models and 3D scanning technologies provide effective tools for documenting, monitoring, and restoring architectural heritage at risk. These technologies allow for the creation of highly accurate digital replicas of buildings and structures, supporting archivists, architects, restorers, and international organizations in their work.

One of the primary advantages of 3D scanning is its ability to capture architectural forms with millimeter precision. Methods such as LiDAR scanning, photogrammetry, and structured-light scanning make it possible to record an object's geometry in detail, including small ornamental elements and surface textures. This level of accuracy is particularly valuable when a building is damaged or destroyed during war, as the digital model can serve as a reliable basis for partial or complete reconstruction. Moreover, 3D data can be integrated into Building Information Models (BIM), which further facilitate technical planning and risk assessment.

Digital models also contribute to the creation of long-term, accessible archives of cultural heritage. Even when a physical site becomes inaccessible or is located in an active conflict zone, digital representations enable continued research, educational use, and public engagement. Museums and academic institutions increasingly rely on such digital archives to develop interactive exhibitions and virtual tours that allow global audiences to explore endangered

or destroyed monuments. This approach expands cultural accessibility and preserves knowledge for future generations.

Another important aspect is the role of digital technologies in restoration efforts. After a conflict, restoration teams often face challenges related to assessing the extent of damage and determining the original architectural state of a structure. High-resolution 3D models allow specialists to compare pre- and post-damage conditions, plan interventions, and fabricate missing elements through advanced techniques such as 3D printing or CNC milling. This accelerates restoration work and ensures a higher degree of authenticity in reconstructed components.

Digital technologies also support preventive measures for protecting heritage sites during war. Detailed digital documentation can help evaluate structural vulnerabilities and identify areas at risk of collapse or targeted destruction. These assessments inform protective strategies, including temporary reinforcements, shelter installations, or evacuation of movable cultural elements. The availability of precise digital data improves decision-making and increases the chances of preserving valuable structures.

In addition, 3D scanning plays a vital role in documenting war crimes involving cultural heritage. The destruction of historically significant sites may constitute violations of international law, and reliable digital evidence is crucial for legal investigations. High-accuracy 3D models can demonstrate the extent, nature, and progression of damage, providing objective evidence for courts and international organizations. This strengthens accountability measures and supports global efforts to protect cultural heritage in conflict zones.

Overall, the integration of digital models and 3D scanning into heritage preservation practices offers broad advantages in times of war. These technologies enable precise documentation, support reconstruction and conservation, enhance cultural accessibility, and contribute to legal efforts aimed at protecting cultural identity. As conflicts continue to endanger architectural heritage worldwide, the adoption of advanced digital tools becomes increasingly essential. Their further development and implementation will help ensure that cultural monuments—symbols of collective memory and identity—are safeguarded for future generations.

Література

1. Apollonio, F. I., Gaiani, M., & Sun, Z. (2020). Digital heritage: 3D documentation and conservation. Springer.

2. Remondino, F., & Rizzi, A. (2018). Reality-based 3D documentation of cultural heritage. Journal of Cultural Heritage, 32, 182–200. https://doi.org/10.1016/j.culher.2018.04.008

3. UNESCO. (2022). Protecting cultural heritage in conflict. UNESCO Publishing. https://www.unesco.orgPRAGMATIKA.MEDIA. Balbek Bureau. https://pragmatika.media/tag/balbek-bureau/

УДК УДК 004.89:004.77:631.4

ОБҐРУНТУВАННЯ ТА ПРОЄКТУВАННЯ ІНФОРМАЦІЙНОЇ СИСТЕМИ МОНІТОРИНГУ СТАНУ ҐРУНТІВ НА ОСНОВІ ТЕХНОЛОГІЙ ІНТЕРНЕТУ РЕЧЕЙ ТА ШТУЧНОГО ІНТЕЛЕКТУ

Владислав КЛИМЧУК, Вадим ПТАШНИК
Львівський національний університет ветеринарної медицини та біотехнологій імені С. З. Ґжицького

Обґрунтовано доцільність створення системи Інтернету речей для моніторингу ґрунтів. Проаналізовано особливості її проєктування, недоліки традиційних методів, потреби агросектора, екології та відновлення територій після бойових дій. Розглянуто архітектуру системи та інноваційні можливості її застосування.
Ключові слова: *інформаційні технології, Інтернет речей, моніторинг ґрунтів.*

The paper justifies the feasibility of creating an IoT-based soil monitoring system. It analyzes design features, the limitations of traditional methods, and the needs of agriculture, ecology, and post-war land recovery. The paper presents architecture and innovative capabilities of the proposed system.
Keywords*: information technologies, Internet of things, soil monitoring*.

Сучасний агропромисловий комплекс України переживає трансформацію, що пов'язана з цифровізацією виробничих процесів, ускладненням кліматичних умов та значними технологічними й екологічними викликами. Однією з ключових умов ефективного агровиробництва є системна оцінка й прогнозування стану ґрунтового середовища, від якого залежать урожайність, продуктивність земель, раціональність використання добрив та водних ресурсів. У зв'язку з цим актуальним постає питання розроблення сучасних інформаційних систем моніторингу ґрунтів, здатних забезпечувати високу точність та оперативність аналізу, з урахуванням регіональних особливостей та зовнішніх впливів.

Особливості проєктування IoT-систем в агропромисловому виробництві визначаються низкою специфічних чинників: великою територіальною розгалуженістю полів, наближеністю до районів ведення військових дій, мінливістю мікрокліматичних умов, складністю стаціонарного живлення сенсорних мереж, потребою у стабільній передачі даних на відстань, впливом техногенних і природних завад. IoT-інфраструктура для агропромисловості вимагає використання малопотужних сенсорних вузлів, енергоощадних протоколів зв'язку а також можливості автономної роботи протягом тривалого часу.

Дослідження ґрунтів є важливим не лише для агропромислового комплексу, а й для екологічного моніторингу та оцінювання наслідків військових дій. У сільському господарстві стан ґрунтового покриву визначає продуктивність культур, ефективність поливу, раціональність використання добрив і прогнозування врожайності. У сфері екології дані про показни-

ки ґрунту дозволяють визначати рівень забруднення, деградації, ерозії, накопичення важких металів та інших токсичних речовин. Особливої актуальності дослідження ґрунтів набувають під час широкомасштабних бойових дій: вибухові речовини, рух важкої техніки, пожежі та техногенні катастрофи негативно впливають на структуру та хімічний склад ґрунтів.

Традиційні методи моніторингу ґрунтів ґрунтуються на ручному відборі проб та лабораторних аналізах. Ці методи мають низку недоліків: значні часові витрати, висока вартість, обмежена кількість вибірок, відсутність можливості безперервного контролю та спостереження за динамічними процесами. Також у багатьох регіонах збір даних традиційними методами неможливий через мінування або небезпеку для фахівців, що робить дистанційний моніторинг єдиним безпечним способом отримання достовірної інформації. Затримка між відбором проби та отриманням результатів не дозволяє швидко реагувати на критичні зміни у ґрунтовому середовищі. Необхідність переходу від періодичного до безперервного моніторингу підтверджено у дослідженні [1].

Тому метою дослідження є визначення можливих переваг інформаційної системи моніторингу стану ґрунтів, розробленої на основі технологій Інтернету речей та штучного інтелекту, а також проєктування її архітектури з урахуванням специфіки агропромислового виробництва, екологічних викликів та умов військових дій.

На відміну від традиційних методів, технології Інтернету речей і штучного інтелекту можуть суттєво вдосконалити процес моніторингу ґрунтів завдяки автоматизованому збору даних у реальному часі, виявленню аномалій, глибинному аналізу кореляцій між параметрами, використанню прогнозних моделей. Вони забезпечують масштабованість, гнучкість та можливість інтеграції супутникових індексів, що підвищує точність комплексної оцінки стану ґрунтів і дозволяє розширити застосування системи в екосистемах різних типів.

У контексті обґрунтування доцільності створення такої системи важливо виділити кілька ключових інноваційних аспектів, виявлених у межах дослідження:

Можливість створення нового методу багаторівневої фільтрації та нормалізації IoT-даних, який дозволяє враховувати локальні аномалії та автоматично визначати достовірність сенсорних вимірювань. Це компенсує типові помилки польових датчиків та підвищує точність оцінки параметрів ґрунту.

Розробка моделі прогнозування стану ґрунтів, адаптованої до локальних умов, що використовує методи машинного навчання [2] та персоналізується під конкретні ділянки за принципом few-shot learning.

Створення інтегрального індексу «здоров'я ґрунту», який узагальнює різні параметри в єдиний показник, зручний для порівняльного аналізу та прийняття рішень [3].

Оптимізація механізмів самодіагностики IoT-мережі, здатних виявляти несправності датчиків і прогнозувати можливі відмови, що критично важливо для польових систем.

Аналіз можливих сфер використання інформаційної системи моніторингу стану ґрунтів на основі IoT та ШІ показує її високу актуальність для агропромислового комплексу, екологічного моніторингу, відновлення земель після військових дій, управління ризиками природних і техногенних катастроф, а також для стратегічного планування землекористування. Ймовірні конкурентні переваги системи – автономність, масштабованість, точність, адаптивність, можливість роботи у небезпечних або важкодоступних зонах – стали основою для формування архітектури розроблюваної системи.

Архітектура системи передбачає використання сенсорних модулів для вимірювання вологості, температури, кислотності, електропровідності, рівнів добрив та інших параметрів, контролера (мікрокомп'ютера або мікроконтролера), який здійснює первинну обробку даних, модулів зв'язку для передачі телеметрії, серверної частини з модулями аналітики, машинного навчання та базами даних, а також клієнтського інтерфейсу для візуалізації інформації, формування звітів та рекомендацій. Така архітектура забезпечує гнучкість, відмовостійкість і можливість розширення системи.

Проведене дослідження підтверджує доцільність створення інформаційної системи моніторингу стану ґрунтів на основі технологій Інтернету речей та штучного інтелекту. Система здатна підвищити точність екологічного та агротехнологічного контролю, сприяти раціональному використанню ресурсів, забезпечувати безпечний збір даних у зонах військових дій та підтримувати прийняття управлінських рішень у складних і динамічних умовах.

Література

1. Lalit Sen, Ikroop Verma, Shivanshu Joshi, Punit Singh. A Survey on IOT-Based Smart Farming Systems for Automated Irrigation and Real-Time Soil Monitoring // IJERT. – 2025. – № 13. – Режим доступу: https://www.ijert.org/a-survey-on-iot-based-smart-farming-systems-for-automated-irrigation-and-real-time-soil-monitoring. – Дата звернення: 20.11.2025.

2. Jiang, Ping & Niu, Guizhen & Li, Guangming. Soil Moisture Prediction Based on Long Short-Term Memory Networks and Meteorological Data. – 2024. – Режим доступу: https://doi.org/10.21203/rs.3.rs-4888081/v1. – Дата звернення: 20.11.2025.

3. Ya'nan Fan, Chao Zhang, Wenyou Hu, Khalid Saifullah Khan, Yongcun Zhao, Biao Huang. Development of soil quality assessment framework: A comprehensive review of indicators, functions, and approaches // Ecological Indicators. – 2025. – № 172. – Режим доступу: https://doi.org/10.1016/j.ecolind.2025.113272. – Дата звернення: 20.11.2025.

DATA SCIENCE ТА СИСТЕМИ ШТУЧНОГО ІНТЕЛЕКТУ: АРХІТЕКТУРА ТА ОБЧИСЛЮВАЛЬНІ МОДЕЛІ

Ірина КОВАЛЬЧУК, Роман ГОЛОВАТИЙ
Львівський державний університету безпеки життєдіяльності

У даній роботі досліджуються фундаментальні взаємозв'язки між методологією Data Science (DS) та архітектурою Систем Штучного Інтелекту (ШІ). Описано етапи трансформації сирих даних у знання через обчислювальні моделі. Визначено роль Машинного Навчання (ML) та Глибокого Навчання (DL) як ключових алгоритмічних підходів. Проаналізовано необхідність високопродуктивної інфраструктури для реалізації ітераційного життєвого циклу DS/ШІ, підкреслюючи критичність етапів Feature Engineering та Валідації Моделей. Розглянуто основні типи архітектур нейронних мереж, які є основою сучасних інтелектуальних систем.

Ключові слова: *Data Science, Штучний Інтелект, Машинне Навчання, Глибоке Навчання, Нейронні мережі, Feature Engineering, Обчислювальна архітектура.*

This paper investigates the fundamental relationships between the Data Science (DS) methodology and the architecture of Artificial Intelligence (AI) Systems. It describes the stages of transforming raw data into knowledge through computational models. The role of Machine Learning (ML) and Deep Learning (DL) is defined as key algorithmic approaches. The necessity of a high-performance infrastructure for implementing the iterative DS/AI lifecycle is analyzed, emphasizing the criticality of the Feature Engineering and Model Validation stages. The main types of neural network architectures, which form the foundation of modern intelligent systems, are also considered.

Keywords*: Data Science, Artificial Intelligence, Machine Learning, Deep Learning, Neural Networks, Feature Engineering, Computational Architecture.*

Предметом дослідження є аналіз структури та взаємодії методологічного апарату Data Science (DS) і технологічної реалізації Систем Штучного Інтелекту (ШІ). В епоху великих даних (Big Data) ефективність будь-якої організації прямо корелює зі здатністю перетворювати сирі інформаційні потоки на дієві знання. Тому основне завдання полягає у формалізації процесного циклу, необхідного для створення та ефективної експлуатації інтелектуальних систем, з критичним фокусом на забезпеченні їхньої точності, стійкості та масштабованості при роботі з постійно зростаючими обсягами гетерогенних даних. Цей цикл вимагає тісної інтеграції науково-статистичних методів і передових обчислювальних технологій.

Data Science виступає як науковий фреймворк, що забезпечує методологічну підготовку даних, яка є обов'язковою передумовою для побудови функціональних ШІ-систем. Без якісної підготовки навіть найпотужніші алгоритми ШІ демонструють низьку прогностичну ефективність.

Життєвий цикл DS проекту є ітераційним і починається зі збору та інтеграції гетерогенних джерел. Цей етап включає вирішення складних інженерних задач, пов'язаних з доступом до даних із різних баз, сховищ та потокових систем. Далі слідують критичні етапи очищення, трансформації та усунення шумів. Очищення даних передбачає роботу з пропусками, ду-

блікатами та аномальними значеннями, які можуть суттєво спотворити результати моделювання. Трансформація необхідна для приведення даних до єдиного числового або категоріального формату, що є обов'язковою вимогою для більшості алгоритмів Машинного Навчання.

Найбільш значущим для подальшого моделювання є етап Конструювання Ознак (Feature Engineering). Це творчий і водночас технічно складний процес, де Data Scientist використовує експертні знання для створення нових, більш інформативних ознак із наявних сирих даних. Наприклад, замість використання дати транзакції, може бути створена ознака "час з моменту останньої транзакції". Цей процес безпосередньо впливає на прогностичну силу та продуктивність будь-якої моделі ШІ. Якість конструювання ознак часто визначає перевагу однієї моделі над іншою, навіть якщо вони використовують той самий алгоритм.

Системи Штучного Інтелекту реалізуються через підходи Машинного Навчання (ML), де модель навчається виявляти приховані функціональні залежності у даних без явного програмування кожного правила. Це досягається шляхом мінімізації функції втрат (loss function) під час тренування на великих масивах даних.

Залежно від типу навчальних даних і поставлених цілей, застосовуються різні парадигми навчання:

Навчання з учителем (Supervised Learning): Використовується, коли навчальні дані мають розмітку, тобто вже відомий бажаний результат. Сюди відносяться завдання Класифікації (прогноз категорії, наприклад, "схвалення кредиту" чи "відмова") та Регресії (прогноз безперервного числового значення, наприклад, ціни акцій чи температури).

Навчання без учителя (Unsupervised Learning): Використовується для пошуку прихованих структур і закономірностей у нерозмічених даних. Прикладами є Кластеризація (групування схожих об'єктів, наприклад, сегментація клієнтів) та Зменшення розмірності (скорочення кількості ознак для спрощення моделі, наприклад, методом головних компонент – PCA).

Особливе місце займає Глибоке Навчання (DL). Цей підхід використовує багатошарові нейронні мережі (звідси "глибоке") для автоматичного вилучення ієрархічних ознак, що мінімізує необхідність ручного Feature Engineering. Різні архітектури DL оптимізовані для різних типів даних і обчислювальних завдань:

Згорткові Нейронні Мережі (CNN): Використовують згорткові шари для просторового вилучення локальних ознак. Вони є оптимальними для комп'ютерного зору, розпізнавання об'єктів та обробки зображень.

Рекурентні мережі (RNN) та їхні варіанти (LSTM, GRU): Розроблені для обробки послідовностей, де важливий порядок даних і залежність від часу. Вони застосовуються для аналізу часових рядів, генерації тексту та в класичних завданнях розпізнавання мови.

Трансформери: Завдяки архітектурі, що базується на механізмі уваги (Self-Attention), вони ефективно обробляють глобальні залежності у довгих послідовностях. Трансформери стали технологічною основою для сучасних досягнень в Обробці Природної Мови (NLP), включаючи великі мовні моделі (LLM) та генеративні моделі.

Успіх сучасних інтелектуальних систем критично залежить від двох ключових факторів: якості на етапі підготовки даних Data Science та коректного вибору обчислювальної архітектури ШІ. Нехтування методологією DS призводить до "сміття на вході – сміття на виході", незалежно від складності алгоритму ШІ.

Подальші дослідження мають бути спрямовані на вирішення викликів, пов'язаних із соціальними та технічними аспектами впровадження ШІ:

Інтерпретованість (Explainable AI, XAI): Оскільки складні DL-моделі часто функціонують як "чорні скриньки", існує нагальна потреба в розробці методів, які дозволяють пояснити, чому модель прийняла те чи інше рішення. Це критично важливо для сфер з високими ризиками, таких як медицина, фінанси та юриспруденція.

Ресурсоефективність та Стійкість: Тренування великих моделей ШІ вимагає значних обчислювальних ресурсів та енергії. Майбутні дослідження повинні зосередитися на розробці більш легких та ресурсоефективних моделей (наприклад, Edge AI), а також на методах зменшення моделі (Pruning, Quantization) для забезпечення їхнього відповідального та стійкого використання.

Узагальнення (Generalization): Покращення здатності моделей, навчених на одній вибірці, ефективно працювати з новими, невідомими даними, мінімізуючи проблему перенавчання (overfitting).

Висновки. Таким чином, інтеграція наукової строгості Data Science та потужності технологій Штучного Інтелекту є ключем до створення наступного покоління інтелектуальних, прозорих та ефективних обчислювальних систем.

Література

1. «Що таке Data Science: визначення, основні поняття…» — сайт Sigma Software University. https://university.sigma.software/what-is-data-science/

2. «Мапа розвитку в Data Science, або Як стати дослідником…» — стаття на сайті DOU.ua. https://dou.ua/lenta/articles/how-i-became-data-analyst/

3. «Data Science (Наука про дані)» — сайт ITStep. https://itstep.edu.ua/news/data-science#gsc.tab=0

4. «Як працює Machine Learning / Artificial Intelligence: ШІ проти машинного навчання» — сайт Glazoff. https://glazoff.com/yak-pratsyuye-mashynne-navchannya-shi-shi-proty-mashynnogo-navchannya/

УДК 624.19:624.04:355.58

МОДЕЛЮВАННЯ СТІЙКОСТІ ТУНЕЛІВ ДЛЯ ЗАВДАНЬ ЦИВІЛЬНОГО ЗАХИСТУ

Ігор КОРДІЯКА, Оксана КАРАБИН, Василь КАРАБИН
Львівський державний університете безпеки життєдіяльності

Тунельна інфраструктура є ключовим елементом цивільного захисту, особливо під час військових дій. У зв'язку із високими загрозами вибухів і пожеж, стає важливою оцінка стійкості цієї інфраструктури. Для цієї оцінки можна застосувати метод скінченних елементів і чисельне моделювання вибухової динаміки, що допомагає оцінити напруження та ризики структурних пошкоджень. Моделювання також підтримує прийняття рішень і планування заходів цивільного захисту, а також підвищує ефективність навчань і оперативних процедур.

Ключові слова: *цивільний захист, надзвичайні ситуації, тунель, воєнні загрози, геологічні загрози*

Tunnel infrastructure is a critical component of civil protection, particularly during military operations. It is important to assess its resilience due to the threat of explosions and fires. The finite element method and numerical modeling of explosion dynamics are used to assess stresses and risks of structural damage. Modeling also supports the decision-making process and the planning of civil protection measures. It also improves the effectiveness of training and operational procedures.

Keywords: *civil protection, emergencies, tunnels, military threats, geological threats*

Тунельна інфраструктура набуває критичного значення як стратегічний елемент цивільного захисту, виконуючи функцію захищеної комунікації в умовах повномасштабної військової агресії. Тому всебічна оцінка стійкості тунельної інфраструктури є ключовим завданням для забезпечення безпеки населення. Актуальність оцінки стійкості підземних споруд багатократно зростає через загрозу динамічних навантажень, спричинених обстрілами та вибухами. Крім безпосереднього структурного пошкодження від вибуху, необхідно враховувати, що помірні вибухові навантаження можуть спричинити значне пошкодження вторинних елементів, наприклад, обвал підвісних стель. Це може призвести до блокування шляхів евакуації та виведення з ладу життєво важливих систем. Іншою критичною загрозою, що посилюється військовими діями, є термічні навантаження від пожеж.

Історично, проєктування та будівництво тунелів значною мірою ґрунтувалися на інженерному досвіді. Сьогодні, однак, цей досвід доповнюється високоточним обчислювальним аналізом. Чисельні методи, зокрема метод скінченних елементів (МСЕ) став галузевим стандартом для розрахунку напружень та переміщень у тунелях. Цей метод забезпечує високу точність і гнучкість у моделюванні складних геомеханічних процесів. МСЕ використовується для визначення оптимальної підтримки, здатної забезпечити стійкість системи "тунель-скельний масив", а також для оцінки структурного опору елементів кріплення [1].

Для забезпечення стійкості тунелів перед загрозами пов'язаними із динамічними навантаженнями, зокрема ракетними ударами, терористичними актами, геологічними процесами [2-4], необхідне застосування комплексних методів динамічного аналізу.

Аналіз динамічної відповіді тунелів цивільного захисту під час вибухової вібрації вимагає поєднання польового моніторингу та чисельного моделювання. Удосконалене моделювання, часто виконане за допомогою таких пакетів, як ABAQUS/Explicit, дозволяє створити єдину чисельну модель, що охоплює послідовність подій: вибух, поширення ударної хвилі через ґрунт, взаємодію ґрунту з облицюванням тунелю та його структурну відповідь.

Модель повинна адекватно описувати складну поведінку матеріалів, включаючи використання еластопластичної моделі Друкера-Прагера для ґрунту та моделі пошкодженої пластичності бетону. Аналіз динамічної відповіді, викликаної вибуховими ударними хвилями, демонструє швидке вивільнення тиску вибуху. Після досягнення максимуму, напруження спадає до стабільного рівня. Однак, напруження спочатку зменшується, а потім зростає до стабільного значення завдяки суперпозиції вибухових напружень.

Ключові динамічні характеристики, що аналізуються, включають швидкість вібрації частинок (PPV), переміщення, головні напруження та основну частоту. Частота вібрації тунелю при вибуху зазвичай розподілена в діапазоні Гц. Особлива увага приділяється напруженням. Аналіз показує, що ефективне напруження спочатку зростає, а потім зменшується вздовж осі тунелю. Напруження, що виникає поблизу джерела вибуху, є найбільшим, і його відносне зменшення також значне. Крім того, пікова швидкість частинок (PPV) є критичною метрикою, і вона послідовно зменшується зі збільшенням відстані від центру вибуху. Для оперативного прийняття рішень у сфері цивільного захисту вкрай важливо мати чіткий критерій безпеки, що базується на фізичних властивостях матеріалів. Чисельне моделювання дозволяє встановити цей критерій, аналізуючи стабільність тунелю під дією вибухової вібрації [1, 5].

Важливим елементом моделювання є оцінка стійкості ґрунту навколо облицювання. Це необхідно для розуміння, чи не виникне додаткове статичне навантаження на тунель через обвал ґрунтового масиву. Вимоги до моделювання також повинні враховувати вторинні, неструктурні елементи. Наприклад, аналіз сценаріїв вибуху показує, що помірні вибухові навантаження можуть спричинити значні пошкодження підвісних стель, аж до їхнього обвалу. В умовах надзвичайної ситуації обвал таких елементів може заблокувати шляхи евакуації та пошкодити життєво важливі системи (вентиляцію, освітлення), перетворюючи незначне структурне пошкодження на серйозну загрозу безпеці людей [5]. Таким чином, для забезпечення цивільного захисту моделювання вразливості має охоплювати і ці допоміжні системи.

Моделювання також відіграє вирішальну роль в управлінні ризиками, пов'язаними з реконструкцією та розширенням існуючих тунелів, осо-

бливо коли застосовуються вибухові роботи. Аналіз дозволяє визначити параметри вибуху, що мінімізують динамічний вплив на існуючі структури, контролюючи швидкість вібрації та еволюцію напружень навколо гірничої виробки. Кінцевим кроком у забезпеченні стійкості є перетворення технічних висновків моделювання на практичні організаційні та оперативні процедури. Цей зв'язок між інженерним аналізом і цивільним захистом є циклічним: інженерне моделювання створює кількісні критерії безпеки. Слабкість у будь-якій частині цього циклу, наприклад, нездатність оновити протоколи після отримання нових даних моделювання, нівелює всі технічні переваги. Тому фінальний звіт має містити список рішень та наступних кроків для оператора та служб надзвичайних ситуацій, спрямованих на перегляд та оновлення операційних або реагувальних процедур.

Майбутні програми цивільного захисту вимагають, щоб безпекові навчання проводилися часто, були повномасштабними, із залученням громадськості та вищих посадових осіб. Моделювання катастрофічних сценаріїв є не лише інструментом проєктування, але й критичною основою для планування цих навчань та тренування персоналу реагування.

Таким чином, моделювання стійкості тунелів є незамінним елементом стратегії цивільного захисту, що дозволяє перетворити абстрактні загрози на кількісні інженерні критерії. Застосування МСЕ та розширених динамічних і термічних конститутивних моделей дозволяє інженерам не лише оцінювати стан існуючої інфраструктури, але й проєктувати нові споруди з підвищеною стійкістю до воєнних та геологічних загроз.

Література

1. Li, Y., Wang, Z., Luo, Q., & Wu, T. (2024). Stability analysis of civil air defense tunnel under blasting vibration. Journal of Vibroengineering, 26(4), 892-903.

2. Starodub Y., Karpenko V., Karabyn V., Shuryhin V. Mathematical Modeling of the Earth Heat Processes for the Purposes of Ecotechnology and Civil Safety. Proc. IEEE CSIT 2020, 23-26 September, 2020, Zbarazh-Lviv, Ukraine: 146-149.

3. Карабин, В. В., & Кордіяка, І. М. (2025). Класифікація надзвичайних ситуацій природного характеру геологічної генези. Наука і оборона, (2), 27-30. DOI 10.33099/2618-1614-2025-29-2-27-30

4. Starodub, Y., Karabyn, V., Havrys, A., Kovalchuk, V., Rogulia, A. & Yemelyanenko, S. (2022). Geophysical research in the pre-Carpathian hydrosphere situation for the environmental civil protection purposes. Geofizicheskiy Zhurnal, 44(4), 171–182. https://doi.org/10.24028/gj.v44i4.264847

5. Khan, A., Yong, F., Yifan, J., & Hajivand Dastgerdi, R. (2025). Damage Analysis of a Tunnel Under Rigid and Deformable Impactors. Geotechnical and Geological Engineering, 43(1), 9.

УДК 004.932:004.5:351.74

ВИКОРИСТАННЯ ВБВПЛА (ВИСОКОБЕЗПЕЧНИХ БОРТОВИХ ВБУДОВАНИХ ПЛАТФОРМ) ДЛЯ АВТОНОМНОГО ОБСТЕЖЕННЯ НЕБЕЗПЕЧНИХ ТЕРИТОРІЙ ПІДРОЗДІЛАМИ ДСНС

Руслан КОРОБКА, Артем ПРОЧИЙ, Олександр ХЛЕВНОЙ
Львівський державний університет безпеки життєдіяльності

Розглянуто побудову високобезпечної бортової вбудованої платформи для автономного обстеження небезпечних територій підрозділами ДСНС в умовах воєнного стану. Запропонована система поєднує модулі комп'ютерного зору, сенсори просторового позиціонування та алгоритми автономного ухвалення рішень, працюючи в ізольованому обчислювальному контурі, стійкому до РЕБ та зовнішніх втручань. Використання ARM-процесорів, камер із глобальним затвором, локального аналізу зображень та алгоритмів SLAM забезпечує ефективне картографування території та виявлення вибухонебезпечних предметів.

Ключові слова: *вбудовані системи; БПЛА; комп'ютерний зір; SLAM; ДСНС; автономна розвідка; розмінування.*

The paper presents the development of a highly secure onboard embedded platform for autonomous reconnaissance of hazardous areas by the State Emergency Service of Ukraine under wartime conditions. The proposed system integrates computer vision modules, spatial positioning sensors, and autonomous decision-making algorithms, operating within an isolated computational environment resistant to electronic warfare and external interference.

Keywords: *embedded systems; UAV; computer vision; SLAM; SES; autonomous reconnaissance; demining.*

Сучасні умови воєнного стану в Україні вимагають від підрозділів ДСНС надшвидкого, точного та безпечного обстеження територій, що містять бойові залишки, нерозірвані боєприпаси, мінні загородження та руйнування критичної інфраструктури. Традиційні методи розвідки місцевості — піший огляд, залучення саперних груп або використання наземної техніки — часто пов'язані з високим ризиком для життя рятувальників та значними часовими витратами. У таких умовах інтеграція вбудованих обчислювальних систем у складі безпілотних літальних апаратів (БПЛА) стає ключовим інструментом підвищення оперативності й безпеки роботи.

У дослідженні розглядається побудова високобезпечної бортової вбудованої платформи (ВБВПЛА) для автономного обстеження небезпечних територій. Платформа складається з модулів комп'ютерного зору, систем інерційного та супутникового позиціонування, мікрорадарів ближнього виявлення та підсистеми автономного ухвалення рішень. На відміну від комерційних дронів подвійного призначення, запропонована система використовує ізольований обчислювальний контур, фізично відмежований від каналів зв'язку з оператором, що значно підвищує її стійкість до РЕБ, спроб перехоплення або підміни команд керування.

Архітектура ВБВПЛА базується на ARM-процесорах із низьким енергоспоживанням, модулях камер з глобальним затвором для роботи у динамічних умовах та системі раннього аналізу зображень на борту. Це дозволяє не лише визначати небезпечні об'єкти (міни, снаряди, боєприпаси, вирви, зсуви інфраструктури), а й виконувати попередню семантичну сегментацію місцевості без необхідності передачі відеопотоку оператору в реальному часі. Такий підхід мінімізує обсяг даних, що передаються по незахищених каналах, та знижує ризик перехоплення. Для картографування територій застосовано методи SLAM (Simultaneous Localization and Mapping), адаптовані для роботи в умовах втрати сигналу GPS/GNSS, що є типовим у зонах активного радіоелектронного придушення. Для детекції небезпечних об'єктів використано нейромережеві моделі YOLO-Embedded і MobileNet-Det, оптимізовані під обмежені обчислювальні ресурси. Дані моделі дозволяють виконувати інференс із затримкою до 20–35 мс, що забезпечує безпечний режим польоту та миттєву реакцію на виявлені загрози.

Отримані експериментальні результати демонструють, що впровадження подібних БПЛА у підрозділи ДСНС дозволяє зменшити час первинного обстеження території на 40–60%, а кількість небезпечних контактів особового складу з підозрілими об'єктами — до 70%. Крім того, система легко інтегрується у мобільні командно-штабні пункти, автоматично передаючи оновлену карту загроз на планшети керівників робіт з ліквідації наслідків надзвичайних ситуацій. Запропонована платформа створює основу для формування нового класу роботизованих комплексів для гуманітарного розмінування та дистанційної оцінки безпекової обстановки. Подальший розвиток системи передбачає впровадження роєвих алгоритмів взаємодії між кількома БПЛА, гіперлокальні мережі датчиків та використання енергоефективних моделей ШІ для повної автономізації польотних місій.

Література

1. Unmanned Aerial Systems for Emergency Response. International Association of Fire Chiefs. – 2024. – Режим доступу: https://www.iafc.org/topics-and-tols/uav (дата звернення: 21.11.2025).

2. Шопський О., Головатий Р. Застосування моделей машинного навчання для раннього виявлення надзвичайних ситуацій на основі потокових великих даних // Матеріали конференції. – 2025. – Режим доступу: https://scholar.google.com (дата звернення: 21.11.2025).

3. Босак Г. С., Головатий Р. Р. Інформаційні технології в оперативному реагуванні: аналіз і оптимізація рішень для підрозділів ДСНС України // Цивільний захист в умовах війни: зб. тез доповідей І Міжнар. наук.-практ. конф. – Львів, 2025. – С. 45–48.

4. SLAM Algorithms for Autonomous UAV Navigation: Overview and Current Trends. Robotics & Automation Review. – 2024. – Режим доступу: https://roboticsautomationreview.com/slam-uav (дата звернення: 21.11.2025).

УДК 349.2

ФОРМИ ЦИФРОВИХ ТЕХНОЛОГІЙ У НАДАННІ СОЦІАЛЬНИХ ПОСЛУГ В УКРАЇНІ

Емілія КОСТИШИН
Львівський державний університет безпеки життєдіяльності

Анотація. *Розглянуто основні форми впровадження цифрових технологій у наданні соціальних послуг в умовах децентралізації та ключові цифрові платформи та сервіси, спрямовані на надання соціальних послуг громадянам. Цифрове надання таких послуг розглядається як технологічний інструмент у межах концепції сервісної держави, що дає змогу оперативно реагувати на зміни реальності та потреби громадян.*
Ключові слова: *держава, соціальні послуги, цифрові технології, цифрових платформ, цифрові сервіси. цифровізація соціальних послуг.*

Abstract. *The main forms of implementing digital technologies in the provision of social services in decentralization and key digital platforms and services aimed at providing social services to citizens are considered. The digital provision of such services is considered as a technological tool within the concept of a service state, which allows for a prompt response to changes in reality and the needs of citizens.*
Keywords: *state, social services, digital technologies, digital platforms, digital services. digitalization of social services..*

У сучасних умовах стрімкого розвитку інформаційно-комунікаційних технологій цифровізація соціальних послуг в Україні стала пріоритетним напрямом державної політики, що відображено в численних нормативно-правових актах, урядових ініціативах та програмі цифрової трансформації. З 1 січня 2020 року набрав чинності новий Закон України «Про соціальні послуги» [1], який передбачив низку нововведень у сфері організації та надання соціальних послуг. Основні організаційні положення щодо цифровізації процесу надання соціальних послуг були закріплені у Розпорядженні Кабінету Міністрів України «Про схвалення стратегії цифрової трансформації соціальної сфери» [2].

Цифровізація соціальних послуг охоплює різні форми впровадження цифрових технологій, кожна з яких має свої особливості та переваги.

1. Електронні сервіси (онлайн-платформи та мобільні додатки). Це веб-сайти або мобільні застосунки, які надають громадянам доступ до соціальних послуг без необхідності відвідувати державні установи: єдині державні портали послуг (наприклад, «Дія» в Україні); системи онлайн-запису на прийом до соціальних служб; чат-боти та віртуальні консультанти для надання довідкової інформації. Перевагами електронних ресурсів є: доступність 24/7; економія часу громадян; скорочення або відсутність черг у державних установах.

2. Автоматизація процесів (цифрове управління послугами): автоматична перевірка документів та статусу отримувача соціальної допомоги; роботизовані алгоритми для визначення права на пільги; впровадження CRM-систем у соціальних службах для швидкого оброблення запитів.

3. Цифрова ідентифікація (електронний підпис, BankID, MobileID).

4. Інтеграція баз даних (єдині державні реєстри та обмін даними). Передбачає створення взаємопов'язаних баз даних, щоб зменшити паперовий документообіг і забезпечити швидку перевірку інформації.

5. Прозорість та доступність (боротьба з корупцією та покращення взаємодії з громадянами).

В Україні діють кілька ключових цифрових платформ та сервісів, спрямованих на надання соціальних послуг громадянам.

Єдина інформаційна система соціальної сфери (ЄІССС) − це державна цифрова платформа, створена з метою забезпечення ефективного, прозорого та оперативного надання соціальних послуг та виплат громадянам України. Доступ до більшості послуг можливий онлайн через платформи, які інтегруються з ЄІССС (наприклад, портал «Дія», соціальний портал Мінсоцполітики, електронні кабінети громадян тощо).

Портал «Дія» створений у межах національного проєкту «Держава у смартфоні», забезпечує централізований доступ до широкого спектру державних послуг у цифровому форматі, об'єднує понад 100 електронних сервісів, зокрема у сферах соціального захисту, охорони здоров'я, реєстрації бізнесу, транспорту, освіти тощо.

Єдиний соціальний реєстр (ЄСР) − це державна інформаційна система, яка створюється в Україні з метою централізованого обліку осіб, які мають право на соціальні виплати, пільги та інші види соціальної підтримки.

Автоматизована система обліку внутрішньо переміщених осіб (ВПО) − спеціалізоване програмне забезпечення або комплекс інформаційних технологій, що призначене для ведення централізованого, актуального та достовірного обліку осіб, які були змушені залишити своє місце постійного проживання через збройні конфлікти, надзвичайні ситуації або інші причини.

Електронний кабінет отримувача соціальних послуг доступний на веб-ресурсах Міністерства соціальної політики та місцевих органів влади. Дозволяє громадянам перевіряти статус своїх звернень, отримувати інформацію про виплати та соціальну підтримку.

Соціальний веб-портал електронних послуг Мінсоцполітики − сучасне цифрове рішення для усіх сторін, які залучені до процесу надання соціальної підтримки. На цьому порталі можна подати онлайн-заяву на отримання соціальних послуг, а згодом − також на призначення соціальної допомоги.

Платформа соціальних послуг e-SOCIAL – це інформаційно-аналітична система, створена для управління соціальною підтримкою населення України, розроблена в рамках проекту «Модернізація системи соціальної підтримки населення України» за фінансування Міжнародного банку реконструкції та розвитку.

Державна платформа «Україна для кожної дитини» створена як частина системного підходу до захисту прав дітей, зокрема дітей, які опинилися в складних життєвих обставинах, сиріт, дітей, позбавлених батьківського піклування, а також сімей, які потребують соціальної підтримки. Платформа створена за підтримки міжнародних партнерів, зокрема ЮНІСЕФ, ПРООН, ChildFund Deutschland, а також при активній участі громадських організацій.

Державна платформа про безоплатну систему протезування та засоби реабілітації створена спрямована на підтримку як військових, так і цивільних осіб, які потребують допомоги у відновленні функцій організму та адаптації до нових умов життя.

Система реєстрації гуманітарної допомоги, також відома як Автоматизована система гуманітарної допомоги (АС ГД) створена для забезпечення прозорості та ефективності управління гуманітарною допомогою в Україні.

Отже, цифровізація соціальних послуг в Україні відбувається активними темпами та охоплює широкий спектр сервісів, платформ і реєстрів, що інтегруються в єдину екосистему соціального захисту.

References

1. Про соціальні послуги: Закон України від 17 січня 2019 року 2671-VIII. URL: https://zakon.rada.gov.ua/laws/show/2671-19#top

2. Про схвалення Стратегії цифрової трансформації соціальної сфери: Розпорядження Кабінету Міністрів України від 28.10.2020 р. № 1353-р. URL: https://zakon.rada.gov.ua/laws/show/1353-2020-%D1%80#Text

УДК 528.8.044.6:004

АНАЛІЗ СИСТЕМ КООРДИНАТ І МЕТРИК ДЛЯ ОЦІНЮВАННЯ РОЗМІРІВ ТА РОЗПІЗНАВАННЯ ОТРИМАНИХ З ЛІДАРА ЗОБРАЖЕНЬ

Остап КУЗИК, Олександр ПРИДАТКО, Назарій БУРАК, Андрій КУЗИК
Львівський державний університет безпеки життєдіяльності

Внаслідок специфіки роботи лідара формування масиву точок, отриманого за результатами сканування простору, найпростіше подати у вигляді координат в сферичній системі. Проте аналіз таких зображень, зокрема, кластеризація, потребує переходу до декартових прямокутних координат. Оцінено можливість використання евклідової метрики для аналізу зображень у декартовій системі координат, на осях якої відкладено полярні координати.

Лідар широко застосовують для побудови просторових зображень рельєфів, що є актуальним для сканування місцевості, створення карт, проведення пошукових робіт та інших завдань. Результатом сканування є сукупність масивів точок, які надалі аналізують з метою виділення фрагментів та їх ідентифікації. Особливістю лідара є те, що один кадр зображення містить точки, які розміщені на півпрямих, що виходять з однієї точки, яка розташована у місці розміщення лідара. Якщо точки масиву розташовані на відстанях, які незначно різняться між собою, тоді проблем обробки зображень не виникає. Але у випадку, коли відстані від точок до лідара значно різняться, виникає проблема, зумовлена різною густотою точок, розміщених на різних відстанях. Це ускладнює розпізнавання зображень, оцінювання їх розмірів та групування методами кластеризації. Це зумовлює більш детально застосовувати системи координат і метрики для подальшого аналізу отриманих зображень, зокрема оцінювання розмірів об'єктів та їх розпізнавання.

Проведемо аналіз інформації, яку отримуємо з лідара. Фактичним результатом роботи лідара є двовимірний масив чисел, який містить значення відстаней. Рядками цього масиву є відстані r, які отримані за результатом горизонтального сканування на однаковій висоті. Сусідні елементи рядка отримують за результатом послідовного сканування та повороту променя дазера на деякий невеликий кут φ_0. Якщо у рядках масиву є n значень, а сканування відбувається внаслідок послідовного повороту на φ_0, тоді горизонтальний кут огляду лідара дорівнює $(n - 1)\,\varphi_0$. Аналогічно, якщо стовпець має m значень, а лазер отримує сусідні значення внаслідок повороту у вертикальному напрямку на деякий кут θ_0, тоді вертикальний кут огляду лідара буде $(m - 1)\,\theta_0$. Таким чином, результат сканування лідара у просторі найпростіше подати у сферичній системі координат $Or\varphi\theta$. Без зменшення загальності можемо вважати, що лідар розташований в точці O, а напрямок сканування середнього рядка масиву (у разі непарного n)

є горизонтальним та співпадає з віссю координат *Ox*. Кут φ сканування в горизонтальній координатній площині відкладається між віссю *Ox* та проекцією півпрямої, що сполучає лідар з точкою простору, до якої визначається відстань. Цей кут буде у межах $-\frac{\pi}{2} < \varphi < \frac{\pi}{2}$. У вертикальному напрямку кут сканування θ відкладаємо між горизонтальною координатною площиною та півпрямою, що сполучає лідар з точкою простору, до якої визначається відстань. Межі зміни цього кута будуть на інтервалі $-\frac{\pi}{2} < \theta < \frac{\pi}{2}$. Тому кожна зісканована лідаром точка фактично матиме координати (r, φ, θ.). Від сферичної системи можна перейти до декартової та визначати у цій системі відстані між точками, проводити групування та розпізнавання отриманого зображення, будувати зображення на екрані. Але якщо розташувати точки у декартовій системі координат $Ox_1y_1z_1$ таким чином, що $x_1 = r$, $y_1 = \varphi$ та $z_1 = \theta$, отримаємо можливість також здійснювати аналіз результатів сканування. Причому, якщо відстані до всіх точок є близькими, то використання методів аналізу зображень повинно бути результативним без необхідності стандартного переходу від сферичної до декартової системи координат.

З метою визначення різниці між представленнями точок у декартовій системі координат із застосуванням формул переходу від сферичної до декартової та з безпосереднім відображенням сферичних координат у декартові. Якщо дві точки $M_1(r_1, \varphi_1, \theta_1)$ та $M_2(r_2, \varphi_2, \theta_2)$ у системі координат $O_1x_1y_1z_1$, з'єднати відрізком, то його довжина буде визначатися як

$$l_1 = \sqrt{(r_2 - r_1)^2 + (\varphi_2 - \varphi_1)^2 + (\theta_2 - \theta_1)^2} \quad (1)$$

Параметричне рівняння відрізка M_1M_2 в цій буде мати вигляд:

$$\begin{aligned} r(t) &= r_1 + (r_2 - r_1)t, \\ \varphi(t) &= \varphi_1 + (\varphi_2 - \varphi_1)t, \\ \theta(t) &= \theta_1 + (\theta_2 - \theta_1)t, \end{aligned} \quad (2)$$

де t – параметр, $0 \le t \le 1$. Якщо перейти від сферичної до декартової системи координат

$$x = r\cos\varphi\cos\theta,\ y = r\sin\varphi\cos\theta,\ z = r\sin\theta, \quad (3)$$

тоді відрізок відобразиться у деяку криву, довжина якої буде

$$l = \int_0^1 \sqrt{(x'(t))^2 + (y'(t))^2 + (z'(t))^2}\, dt. \quad (4)$$

Підставивши (3) у (4), отримуємо після спрощення

$$l = \int_0^1 \sqrt{r^2(t)\left(\cos^2\theta(t)\left(\varphi'(t)\right)^2 + \left(\theta'(t)\right)^2\right) + (r'(t))^2}\, dt. \quad (5)$$

Враховуючи (2), відстань l_1 можемо переписати у вигляді

$$l_1 = \int_0^1 \sqrt{(r'(t))^2 + (\varphi'(t))^2 + (\theta'(t))^2}\, dt. \quad (6)$$

Для порівняння l та l_1 прирівняємо підкореневі вирази у (5) та (6). З урахуванням (2) маємо

$$[r^2(t)\cos^2\theta(t)-1](\varphi_2-\varphi_1)^2+[r^2(t)-1](\theta_2-\theta_1)^2=0. \quad (7)$$

Якщо відповідні координати точок M_1 та M_2 різні, то рівність $l = l_1$ буде виконуватися, якщо

$$r^2(t)\cos^2\theta(t)-1=0 \quad (8)$$

і

$$r^2(t)-1=0, \quad (9)$$

лише для $\theta(t)=0$ або загалом у точках перетину поверхні

$$u(r,\theta)=[r^2\cos^2\theta-1](\varphi_2-\varphi_1)^2+[r^2-1](\theta_2-\theta_1)^2 \quad (10)$$

та площини $u=0$. У інших випадках, позначивши $r_{min}=\min\{r_1,r_2\}$, $r_{max}=\max\{r_1,r_2\}$, $m=\min\{(\varphi_2-\varphi_1)^2,(\theta_2-\theta_1)^2\}$, $M=\max\{(\varphi_2-\varphi_1)^2,(\theta_2-\theta_1)^2\}$, $\theta_{min}=\min\{|\theta_1|,|\theta_2|\}$, $\theta_{max}=\max\{|\theta_1|,|\theta_2|\}$, отримаємо оцінку лівої частини (7) зверху:

$$[r^2(t)\cos^2\theta(t)-1](\varphi_2-\varphi_1)^2+[r^2(t)-1](\theta_2-\theta_1)^2 \le \le \begin{cases} M(r_{max}^2(\cos^2\theta_{min}+1)-2), & r_{max}^2(\cos^2\theta_{min}+1)>2 \\ M\left(2-r_{min}^2(\cos^2\theta_{max}+1)\right), & r_{max}^2(\cos^2\theta_{min}+1)<2 \end{cases} = A \quad (11)$$

і знизу

$$[r^2(t)\cos^2\theta(t)-1](\varphi_2-\varphi_1)^2+[r^2(t)-1](\theta_2-\theta_1)^2 \ge \ge \begin{cases} m(r_{min}^2(\cos^2\theta_{max}+1)-2), & r_{min}^2(\cos^2\theta_{max}+1)>2 \\ m\left(2-r_{max}^2(\cos^2\theta_{msn}+1)\right), & r_{min}^2(\cos^2\theta_{max}+1)<2 \end{cases} = a \ge 0. \quad (12)$$

З урахуванням (11) і (12) отримуємо

$$0 \le \sqrt{a} \le |l-l_1| \le \sqrt{A}. \quad (13)$$

Висновок. Використання декартової системи координат з сферичними координатами на її осях для безпосереднього відображення та подальшої обробки результатів сканування лідара, зокрема використання евклідової метрики для кластерного аналізу, є можливим, проте має похибку, яка спричинена відображенням відрізка у деяку криву та різницею їх довжин, яка загалом залежить від координат точок та оцінюється нерівністю (13).

УДК 004.6

ПОКРАЩЕННЯ НАВЧАЛЬНОГО ПРОЦЕСУ ЗА ДОПОМОГОЮ ІНСТРУМЕНТІВ 3D ДРУКУ В ОСОБЛИВИЙ ПЕРІОД

Григорій КУЗНЄЦОВ, Юрій РУДИК
Національний університет „Львівська політехніка", Львів

Розглядаються інструменти 3D друку (настільні FDM принтери), з інтегрованими системами дистанційного моніторингу стану, процесу друку та резервного живлення в умовах перенапруг та нестабільної подачі електроенергії. Показано, що дане поєднання настільного 3D принтеру, моніторингу, безперебійного джерела живлення (БДЖ) дадуть змогу забезпечити підхід який допоможе розвинути технічні навички студентів у проектуванні, створенні та використанні систем стійких до відмов. Це забезпечить безперервну підготовку та виготовлення деталей, зменшення кількості відходів та підвищення обізнаності та інтересу у студентів про інструменти 3D друку. Впровадження такого рішення є актуальним в особливий період.

***Ключові слова**: 3D друк, 3D принтер, моніторинг, безперебійна подача електроенергії, особливий період.*

Tools of 3D printing (desktop FDM printers) integrated with remote monitoring systems for equipment status, printing processes and backup power supply under conditions of voltage surges and unstable electricity are considered. It is shown that the combination of a desktop 3D printer, monitoring tools and an uninterruptible power supply (UPS) makes it possible to provide an approach that helps students develop technical skills in designing, creating and using fault-tolerant systems. This ensures continuity of training and production of parts, reduces the amount of waste, and increases students' awareness and interest in 3D printing tools. The implementation of such a solution is relevant in a special period.

***Keywords:** 3D printing, 3D printer, monitoring, uninterruptible power supply, special period.*

Умови нестабільного електропостачання, що спостерігаються в особливий період, безпосередньо впливають на якість навчального процесу у закладах освіти, особливо у практичній підготовці студентів технічних спеціальностей. Нестабільне електроживлення призводить до безповоротнього переривання 3D друку та навчального процесу, створення проблем у вигляді відходів та можливих пошкоджень обладнання. Настільні 3D принтери чутливі навіть до коротких відключень електроенергії і є залежними від стабільного електропостачання для успішного завершення процесу друку. Тому актуальними є комплексні рішення, які поєднують у собі резервне стабільне живлення, моніторинг та безперебійне керування обладнанням [1-3].

На даний момент, лабораторні роботи є одним із ключових напрямів практико-орієнтованого навчання та важливим інструментом для реалізації студентських проєктів. Освоєння відповідних навичок забезпечує можливість переходу від цифрової моделі до реально виготовленого виробу. За допомогою інструментів 3D друку студенти зможуть ознайомитись з повним технологічним циклом: створенням та підготовкою моделі, налаштуванням 3D принтеру, та подальшим аналізом результатів. Проте під час

особливого періоду, подача електроенергії не є стабільною, що робить довгий друк вразливим і залежним від зовнішніх чинників. Тому основна ціль – це створення захищеної від зовнішніх чинників системи, інтегрованої з моніторингом по відео зв'язку та моніторингом стану, температури вузлів, живлення пристроїв системи.

Порівняно з традиційними лабораторними роботами, де практична частина здебільшого обмежується демонстраційними прикладами або короткочасними експериментами, використання комплексної системи, що включає 3D-принтер, моніторингову підсистему та блок безперебійного живлення (БДЖ), відкриває можливості для моделювання довготривалих технологічних процесів, максимально наближених до реальних умов виробництва. У класичних лабораторіях навіть незначна відмова обладнання, наприклад, через переривання електроживлення, зазвичай призводить лише до необхідності повторного виконання експерименту без істотного впливу на навчальний процес [4]. Натомість у випадку роботи з 3D-принтером подібна ситуація може мати значно серйозніші наслідки: втрату декількох годин технологічного процесу, матеріальних витрат, а також частково або повністю втрачений результат навчальної роботи.

Впровадження резервного живлення та інтегрованих систем моніторингу дозволяє змінити підхід до організації навчального процесу: увага зміщується від пасивного спостереження за відмовами на активне проєктування та реалізацію відмовостійких рішень. Такий підхід не лише забезпечує безперервність виконання складних технологічних експериментів, але й формує у студентів навички аналізу ризиків, планування та управління технологічними процесами в умовах непередбачуваних ситуацій. У результаті інтеграція сучасних апаратно-програмних засобів у навчальний процес значно підвищує освітню цінність лабораторних занять, сприяє розвитку критичного мислення, технічної обізнаності та професійної компетентності студентів, адже вони мають змогу відпрацьовувати прийоми забезпечення надійності та стійкості складних виробничих систем у реальному часі.

Запропонований навчальний комплекс може складатись з FDM принтеру, мікрокомп'ютера (наприклад, Raspberry Pi 3/4/5) або ноутбуку, для реалізації дистанційного моніторингу та керування, мережевий інтерфейс для доступу до систем, а також БДЖ, розрахованого на роботу комплексу протягом заданого часу. Здійснюється збір телеметрії: температури сопла, платформи, сопла, відсоток виконання друку, швидкість, час друку і запланований час завершення друку, кількість спожитої енергії у певний час, навіть теперішнє споживання, і передає це все у веб-інтерфейс. Додаткове підключення датчиків напруги й струму на вхід живлення допоможе контролювати розхід енергії і перемикатись на резервне живлення у випадку знеструмлення [4-7].

Ключовою відмінністю такої системи від простих практичних робіт у тому що студенти наочно бачать прилад, як все працює, можуть взаємодіяти, і які взаємозвязки існують.

Додаткове впровадження системи відеомоніторингу, де камера підключається до мікрокомп'ютера або ноутбука, забезпечує можливість безперервного спостереження за процесом 3D-друку у будь-який час, включно з віддаленим доступом поза межами навчального закладу. Відеоспостереження інтегрується з журналом подій, що формує повноцінну базу даних із історією друку, а за необхідності допускає формування timelapse-відео або організацію прямої трансляції. Такий підхід дозволяє ретельно аналізувати помилки, технічні збої та особливості роботи обладнання, підвищуючи точність оцінки процесу. На відміну від традиційних практичних занять, де експеримент обмежується одноразовим запуском та короткочасними демонстраціями, запропонована система забезпечує тривалість та безперервність навчальної практики, наближаючи її до реальних умов виробничого 3D-друку та сприяючи формуванню навичок комплексного контролю технологічного процесу.

Окремої уваги заслуговує, використання Klipper у поєднанні з вебінтерфейсом Mainsail забезпечує розширені можливості дистанційного моніторингу та керування 3D-друком завдяки перенесенню обчислювального навантаження на одноплатний комп'ютер [4]. Така архітектура дозволяє отримувати точну телеметрію, контролювати параметри друку в реальному часі та швидко реагувати на збої чи зміну стану живлення.

Підбір компонентів комплексу здійснено із врахуванням характеристик принтера, складових системи, зокрема і часу друку при перериванні живлення.

Таким чином, підійшовши з розширеними параметрами комплексу, вдалось сформувати картину проблеми, і способи її вирішення.

Література

1. Rudyk Y, Mykyichuk M, Menshikova O. Information technology criteria for the quality assessing of critical infrastructure by safety indexes. Conference proceedings of the VII International Scientific-Practical Conference "Information Technology for Education, Science and Technics" (ITEST-2024), (Cherkasy, May 23-24, 2024). Cherkasy: ChSTU, 2024. P.191-193

2. Gibson I., Rosen D.W., Stucker B. Additive Manufacturing Technologies: 3D Printing, Rapid Prototyping and Direct Digital Manufacturing. Springer

3. Dewidar M. Remote monitoring of fused deposition modeling 3D printers using embedded systems. International Journal of Engineering Research & Technology, 2020.

4. Kevin O'Connor. Klipper: 3D Printer Firmware Documentation. 2023. URL: https://www.klipper3d.org

5. OctoPrint Project. Remote Monitoring and Control for 3D Printers. 2022. URL: https://octoprint.org

6. Raspberry Pi Foundation. Using Single-Board Computers for Remote Machine Control. Technical Report, 2022.

7. EN 62040-1. Uninterruptible Power Systems (UPS) – General and Safety Requirements. IEC, 2017.

УДК 614.84:004.02

ПРОФІЛАКТИКА ТА ВИЯВЛЕННЯ ЗАГОРАНЬ НА СМІТТЄЗВАЛИЩАХ ЗА ДОПОМОГОЮ ТЕПЛОВІЗІЙНОГО МОНІТОРИНГУ

Андрій КУЗЬМІН
Хмельницький національний університет

Анотація. *У роботі проаналізовано ризики загорання сміттєзвалищ через внутрішні хімічні процеси. Оцінено температурні межі займання. Проведено порівняння тепловізорів і визначено оптимальну модель для раннього виявлення перегрівів. Наведено технічні характеристики та обґрунтовано вибір апаратних засобів для моніторингу сміттєзвалищ та виявлення та профілактики загорань на ранніх етапах.*

Ключові слова: *тепловізор, сміттєзвалище, самозаймання, моніторинг, перегрів.*

Abstract. *The paper analyzes the risks of landfill fires due to internal chemical processes. The temperature limits of ignition are estimated. Thermal imagers are compared and the optimal model for early detection of overheating is determined. The technical characteristics are given and the choice of hardware for monitoring landfills and detecting and prophylactics of fires at the early stages is justified.*

Keywords: *thermal imager, landfill, spontaneous combustion, monitoring, overheating.*

Актуальність теми. На полігонах твердих побутових відходів відбуваються інтенсивні біохімічні процеси, які супроводжуються виділенням тепла та горючих газів. За певних умов у товщі сміттєзвалища формуються «гарячі зони», що можуть призводити до самозаймання. Ранні ознаки перегріву зазвичай не виявляються візуально, тому для моніторингу температури використовують тепловізори. [1–3].

Постановка проблеми. Температурні межі займання. Внутрішня температура у тілі сміттєзвалища може сягати 60–70 °C внаслідок мікробіологічного розкладу органіки. За наявності кисню такі умови є критичними — з температури ~70 °C можливе самозаймання. При ~125–175 °C відбувається тління. Таким чином, ділянки з температурою вище 60 °C потребують негайного втручання. Потрібні підходи, що забезпечують безперервний моніторинг, раннє виявлення відхилень від норм температурних показників та підбір технічних засобів, які це забезпечують.

Мета роботи. Метою є теоретичне обґрунтування доцільності використання тепловізійного моніторингу для виявлення перегрівів, що свідчать про потенційне самозаймання на сміттєзвалищах, проаналізувати температурні межі таких процесів та підбір оптимального типу тепловізора для раннього виявлення загроз загоряння.

Концептуальна база дослідження. Всередині тіла сміттєзвалища відбуваються біохімічні процеси розкладання відходів, які

супроводжуються виділенням тепла. Температура у масі відходів може поступово підвищуватися до 40–70 °C внаслідок мікробіологічного розкладу органіки. За таких умов формуються осередки підвищеної температури, що підсилюються накопиченням горючих газів (метану тощо). Якщо температура й далі зростає і перевищує критичний поріг (~60 °C і більше), такі "гарячі точки" свідчать про ймовірне самозаймання. Відомо, що при ~125–175 °C відбувається вже активне тління субстрату сміття. Таким чином, внутрішнє горіння може розпочатися, коли локальна температура перевищує приблизно 60–70 °C, особливо за наявності доступу кисню. Дослідження показали, що на теплових знімках звалищ ділянки з температурою понад 60 °C однозначно вказують на потенційні осередки самозаймання. Раннє виявлення таких точок дозволяє вжити заходів (перекопування, проливання водою, подача інертного газу тощо) для попередження великої пожежі.

Для безперервного моніторингу полігонів ТПВ використовуються різні типи тепловізійних камер: стаціонарні (монтуються на вежах, щоглах по периметру), дронові (інтегруються на безпілотники для огляду з повітря) та ручні портативні (для інспекції підозрілих зон персоналом). У таблиці 1 наведено результати порівняльного аналізу кількох моделей тепловізорів, які добре зарекомендували себе для екологічного моніторингу сміттєзвалищ.

Таблиця 1 – Порівняльна характеристика сучасних моделей тепловізорів, придатних для моніторингу полігонів ТПВ.

Модель	Виробник	Діапазон температур	Точність	Роздільна здатність	Тип	Ціна
FLIR A700f	Teledyne FLIR	−20…+650 °C	±2 °C або ±2%	640×480	Стаціонарна	~$20 000
Axis Q2901-E	Axis (Швеція)	−40…+550 °C	±5 °C або ±5%	336×256	Стаціонарна	~$2 000
DJI Zenmuse H20T	DJI (Китай)	−20…+550 °C	±2 °C або ±2%	640×512	Дронова	~$10 000
Workswell WIRIS Pro	Workswell (Чехія)	−25…+1500 °C	±2 °C	640×512	Дронова	~$15 000+
Fluke Ti480 PRO	Fluke (США)	−20…+1000 °C	±2 °C або ±2%	640×480	Ручна	~$14 000

Стаціонарні камери (напр. FLIR, Axis) зазвичай інтегруються в систему відеонагляду з аналітикою: вони можуть автоматично визначати "гарячі точки" і піднімати тривогу (сигналізація, оповіщення диспетчера) при перевищенні встановленого порогу температури. Дронові системи (DJI, Workswell) дозволяють оперативно обстежувати велику площу звалища з повітря, будувати теплові ортофотоплани для виявлення аномалій температурного поля по всій території полігону. Ручні тепловізори (Fluke та ін.) корисні для детального обстеження конкретної

ділянки або підтвердження температури при наземному обході, хоча не забезпечують безперервного моніторингу. Для раннього виявлення внутрішніх загорань на сміттєзвалищі найкраще зарекомендував себе стаціонарний тепловізор з високою роздільною здатністю та автоматичною сигналізацією. З наведених моделей оптимальним є FLIR A700f, про що свідчать резульати проведеного аналізу.

Висновки. Тепловізійний моніторинг сміттєзвалищ дозволяє своєчасно виявляти перегріті ділянки, які становлять загрозу самозаймання, та переходити від реактивного реагування до проактивного управління пожежною безпекою. Застосування сучасних стаціонарних тепловізорів забезпечує безперервний контроль температури, знижує ризик масштабних пожеж і формує підґрунтя для впровадження автоматизованих систем екологічного нагляду.

Подальший розвиток підходу передбачає інтеграцію тепловізорів із системами аналітики, автоматичними засобами оповіщення та реагування, а також використання безпілотних платформ для оперативного зонального сканування з метою раннього виявлення та профілактики пожеж на сміттєзвалищах.

Література

1. Pavlova O.O., Kuzmin A. A. The concept of information system for recognition fire at the landfill. (2025) Science and technology Today.№ 12(53). pp. 73-82. https://doi.org/10.52058/2786-6025-2025-12(53)-73-82

2. Кузьмін А.А. Інформаційна веб-орієнтована система для раннього виявлення пожежі на сміттєзвалищах за допомогою комп'ютерного зору. Збірник наукових праць за матеріалами XVI Всеукраїнської науково-практичної конференції «Актуальні проблеми комп'ютерних наук АПКН-2024». Хмельницький. 2024. ст. 329-331

3. M. Kvassay, A. Kuzmin, M. Kostiuk, O. Khlevnoi, H. El Bouhissi. Computer vision-based information system for landfill fire detection. Proceedings of the 6th International Workshop «Intelligent Information Systems and Systems of Information Security» (IntelITSIS 2025). Khmelnytskyi - London, April 4, 2025. Vol. 3963. pp. 198-207

4. Teledyne FLIR. FLIR A700f Advanced Smart Sensor. https://www.flir.com/products/a700f-smart-sensor/

5. Axis Communications. AXIS Q2901-E Temperature Alarm Camera. https://www.axis.com

6. Workswell. WIRIS Pro Thermal Camera. https://www.workswell-thermal-camera.com

7. Fluke Corporation. Fluke Ti480 PRO Thermal Camera. https://www.fluke.com

8. ДСНС України. (2023). Заходи пожежної безпеки на сміттєзвалищах. https://dsns.gov.ua

УДК 004.8:004.4:616.89

АРХІТЕКТУРНІ ПІДХОДИ ДО РОЗРОБЛЕННЯ PWA-ЗАСТОСУНКУ ПСИХОЛОГІЧНОЇ ПІДТРИМКИ ВІЙСЬКОВОСЛУЖБОВЦІВ ІЗ ЗАСТОСУВАННЯМ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ

Валерій КУКУЛЕВСЬКИЙ, Ольга СМОТР
Львівський державний університет безпеки життєдіяльності

Анотація. *У роботі розглянуто архітектурні підходи до створення PWA-застосунку психологічної підтримки військовослужбовців із використанням технологій штучного інтелекту. Обґрунтовано вибір формату Progressive Web Application для роботи в умовах нестабільного інтернет-з'єднання та запропоновано архітектуру «offline-first» із використанням Service Worker, IndexedDB та механізмів синхронізації. Ключовим елементом системи є інтегрований AI-модуль на базі великої мовної моделі (LLM), що забезпечує адаптивні рекомендації та скринінг психоемоційного стану. Особливу увагу приділено питанням безпеки та анонімності. Запропоноване рішення спрямоване на підвищення доступності психологічної допомоги в умовах бойових дій.*

Ключові слова*: PWA, штучний інтелект, психологічна підтримка, військовослужбовці, LLM.*

Abstract. *The paper explores architectural approaches to developing a PWA-based application for psychological support of military personnel using artificial intelligence technologies. The choice of Progressive Web Application format is justified by the need for stable operation under unreliable internet connectivity, and an "offline-first" architecture is proposed, incorporating Service Worker, IndexedDB, and synchronization mechanisms. The core component of the system is an integrated AI module based on a Large Language Model (LLM), providing adaptive recommendations and mental health screening. Special attention is given to security and anonymity. The proposed solution aims to improve accessibility of psychological assistance in combat conditions.*

Keywords: *PWA, artificial intelligence, psychological support, military personnel, LLM.*

В умовах повномасштабної війни в Україні питання збереження ментального здоров'я військовослужбовців набуває критичного значення. Постійний стрес, загроза життю та високі психологічні навантаження призводять до розвитку бойових психічних травм, зокрема посттравматичного стресового розладу (ПТСР). Забезпечення своєчасної та доступної психологічної допомоги часто ускладнюється через перебування військових у зонах з обмеженим доступом до інтернету або неможливістю особистого контакту з фахівцем. У цьому контексті актуальним є розроблення програмних засобів, які поєднують мобільність, автономність та інтелектуальну складову для надання первинної підтримки [1].

На нашу думку інформаційна система у форматі Progressive Web Application (PWA), що забезпечує доступ до інструментів самодопомоги та консультацій з використанням можливостей генеративного штучного інтелекту є одним із доволі ефективних шляхів вирішення цієї проблеми.

Вибір технології PWA обумовлений необхідністю забезпечення роботи застосунку в умовах нестабільного інтернет-з'єднання, що є типовим для зони бойових дій. Для забезпечення стабільної роботи в умовах нестабільного зв'язку пропонується архітектура «offline-first» на базі PWA. Ключові компоненти: Service Worker для кешування контенту й ресурсів; локальна база даних (IndexedDB) для збереження сесій і журналів; шар синхронізації з сервером з механізмом конфліктної розв'язки; проміжний API-шар для контролю доступу до AI [2-4]. Завдяки використанню Service Workers та механізмів кешування, PWA дозволяє зберігати базовий функціонал (наприклад, інформаційні матеріали, техніки дихання, щоденник емоцій) навіть у режимі офлайн. Крім того, PWA є кросплатформним рішенням, що не вимагає розробки окремих нативних додатків для Android та iOS, спрощуючи процес розгортання та оновлення [5]. Також важливо передбачити мінімізацію обсягу даних, що передаються, та асинхронні черги запитів.

Ключовим елементом системи доцільно обрати інтегрований AI-модуль, побудований на базі великої мовної моделі (LLM) Gemini від Google. LLM (Large Language Model). Це модель штучного інтелекту, натренована на величезних масивах текстових даних, яка здатна розуміти контекст і генерувати відповіді природною людською мовою. Вибір моделі Gemini ґрунтується на її високих показниках у розумінні контексту, здатності до генерації емпатійних відповідей та ефективності обробки природної мови. На AI-модуль у проєкті покладатиметься роль первинного асистента, який проводить опитування скринінгу, надає адаптивні рекомендації з саморегуляції та виявляє маркери кризових станів.

Важливим є питання безпеки та анонімності. Особливу увагу доцільно приділити захисту персональних даних, адже цільовою аудиторією є військовослужбовці. Пропонуємо врегулювати це питання врахувавши в архітектурі додатку наявність проміжного серверного шару, який фільтруватиме і модеруватиме відповіді LLM, застосовуватиме систему шаблонів (prompt-guardrails) та керуватиме журналами анонімізовано. Архітектура повинна забезпечувати передачу даних виключно через HTTPS, шифрування чутливих даних на пристрої, обмеження збору метаданих та можливість анонімної роботи (система не вимагатиме обов’язкової реєстрації з використанням особистих даних для базового функціоналу). Окрім того архітектура повинна передбачати наявність каналів зв'язку з живими фахівцями та забезпечувати механізми перемикання на них при виявленні суїцидальних думок або гострих симптомів.

Висновки. Розроблення PWA-застосунку психологічної підтримки військовослужбовців із використанням технологій штучного інтелекту є перспек-

тивним напрямом, що поєднує мобільність, автономність та інтелектуальну складову. Запропонована архітектура «offline-first» забезпечує роботу в умовах нестабільного інтернет-з'єднання, а інтеграція LLM-моделі дозволяє реалізувати адаптивні механізми самодопомоги та скринінгу психоемоційного стану. Такий підхід забезпечує баланс між функціональністю та доступністю, що є критично важливим для надання психологічної підтримки військовим в умовах війни, сприяє підвищенню доступності психологічної допомоги та зниженню ризиків розвитку кризових станів у військових. Поєднання механізмів офлайн-роботи, локального збереження даних та контрольованої AI-інтеграції дозволяє мінімізувати ризики та підвищити доступність сервісу.

Література

1. Гапанович В., Смотр О. Розробка мобільного сервісу надання психологічної допомоги // Інформаційна безпека та інформаційні технології : зб. тез доп. V Міжнар. наук.-практ. конф. ІБІТ 2024. – Львів : ЛДУ БЖД, 2024. – С. 396–399.

2. Grinberg M. Flask Web Development: Developing Web Applications with Python. – O'Reilly Media, 2018.

3. Кордунова Ю. С., Смотр О. О., Кокотко І. Я., Малець Р. Б. Аналіз традиційного та гнучкого підходів до створення програмного забезпечення в динамічних умовах. Управління розвитком складних систем. Київ, 2021. № 47. С. 71 – 77, https://doi.org/10.32347/2412-9933.2021.47.71-77

4. Google AI for Developers. Gemini API Overview [Електронний ресурс]. – Режим доступу: https://ai.google.dev/docs (дата звернення: 19.11.2025).

5. Love J. Progressive Web Application Development by Example. – Packt Publishing, 2019.

УДК 004.8:004.912:316.774

ВИЯВЛЕННЯ ФЕЙКОВИХ НОВИН НА ОСНОВІ МОДЕЛЕЙ МАШИННОГО НАВЧАННЯ

Валентин КУРИЛО
Львівський національний університет ветеринарної медицини та біотехнологій імені С. З. Ґжицького

Здійснено аналіз методів машинного навчання та нейронних мереж для виявлення фейкових новин. Розроблено веб-застосунок, який дозволяє класифікувати новини як правдиві або фейкові, а також здійснювати перенавчання моделей на нових даних.
Ключові слова: *машинне навчання, фейкові новини, нейронні мережі, класифікація текстів, веб-застосунок.*

An analysis of machine learning and neural network methods for fake news detection has been conducted. A web application was developed to classify news as true or fake and to retrain models using new data.
Keywords: *machine learning, fake news, neural networks, text classification, web application.*

У сучасному світі, де інформація поширюється миттєво через соціальні мережі, месенджери та новинні ресурси, проблема фейкових новин набуває особливої актуальності [1]. Неправдива інформація може впливати на суспільну думку, дестабілізувати соціальну ситуацію та використовуватись як інструмент інформаційної війни, особливо в умовах збройного конфлікту в Україні. Тому автоматизація процесу виявлення фейкових новин із використанням технологій машинного навчання є важливим завданням сучасних досліджень у сфері інформаційної безпеки та штучного інтелекту [2].

Метою роботи є розробити ефективну систему для автоматичного виявлення фейкових новин на основі методів машинного навчання та глибинних нейронних мереж, що забезпечує високу точність класифікації текстової інформації. Об’єкт дослідження є процес виявлення фейкових новин у текстових. Предмет дослідження є методи та моделі машинного навчання, що використовуються для класифікації.

Для досягнення поставленої задачі було проаналізовано літературні джерела присвячених проблемі виявлення фейкових новин, були відібрані найактуальніші та найрезультативніші дослідження, що пропонують сучасні методи машинного та глибинного навчання для підвищення точності класифікації новинного контенту.

В таблиці 1 наведено основні задачі, які були проаналізовані в літературних джерелах та методи їх вирішення.

Таблиця 1 – Огляд обраних літературних джерел*

Задача	Методи
Створення системи класифікації фейкових новин із використанням ML та DL	Logistic Regression, Decision Tree, Naive Bayes, SVM, LSTM, BERT
Узагальнення підходів, аналіз архітектур DL і NLP, формування таксономії	LSTM, GRU, CNN, BERT, RoBERTa, XLNet
Інтеграція класичних та DL-моделей для підвищення точності класифікації	Naïve Bayes, SVM, Random Forest, CNN, LSTM, BERT, Word2Vec

Джерело: узагальнено на основі даних [3-5]

Основна увага у проведеному огляді приділялася виявленню тенденцій розвитку у сфері автоматичного розпізнавання дезінформації, визначенню найбільш ефективних моделей для класифікації новин, а також аналізу переваг і недоліків існуючих підходів. Зокрема, досліджено методи логістичної регресії, дерева рішень, SVM, а також сучасні архітектури глибинного навчання, а саме класичним методам машинного навчання та RNN, LSTM, GRU, CNN, BERT, RoBERTa, GPT тощо.

Сучасні підходи до класифікації текстів дозволяють використовувати технології машинного навчання та штучного інтелекту для аналізу змісту новин, виявлення закономірностей у мовних структурах і розпізнавання фейкових матеріалів. Одним із найефективніших напрямів є побудова моделей, здатних автоматично визначати достовірність новинних повідомлень на основі їх текстового змісту. Для цього необхідно мати якісний набір даних, що містить приклади як справжніх, так і неправдивих новин, а також забезпечити належну попередню обробку тексту, а саме очищення, лематизацію та токенізацію.

У даній роботі використано відкритий набір даних, який містить понад 10 700 новинних заголовків, зібраних із Telegram-каналів у період з 24 лютого по 11 грудня 2022 року [6]. Новини мають відповідні мітки - “True” (правдиві) та “False” (фейкові). Для підвищення точності навчання моделі набір даних було збалансовано між двома класами.

Для аналізу застосовано кілька підходів машинного навчання: логістична регресія, метод опорних векторів (SVM), дерева рішень, градієнтне підсилення, а також рекурентні нейронні мережі (RNN, LSTM) і трансформерна модель BERT, які здатні враховувати контекст та глибинні зв’язки між словами. Оцінка ефективності проводилася за допомогою таких метрик, як Accuracy, Precision, Recall та F1-score.

Результати експериментів показали, що найвищі показники точності продемонстрували глибинні моделі, зокрема BERT та LSTM, які здатні краще розуміти семантику тексту. Це свідчить про перспективність вико-

ристання трансформерних архітектур у задачах аналізу українських новин та виявлення фейкових повідомлень.

На основі отриманих результатів було створено веб-застосунок, який дозволяє користувачу вводити текст новини та отримувати миттєвий результат класифікації "правдива" або "фейкова". Для адміністратора передбачено можливість перегляду історії введених новин, аналізу результатів класифікації та перенавчання моделей для підвищення їх ефективності. Система складається з чотирьох основних частин:

– API на Flask (Python) для роботи з моделями;
– бекенд на Nest.js для обробки запитів;
– база даних PostgreSQL для збереження інформації;
– фронтенд на Next.js для взаємодії з користувачем.

Розроблена система має практичну цінність у сфері моніторингу новинного контенту та боротьби з дезінформацією. Її можна інтегрувати у медіасистеми, освітні платформи чи інформаційні агентства для підвищення рівня медіаграмотності користувачів і зменшення поширення неправдивої інформації.

Таким чином, застосування технологій машинного навчання у виявленні фейкових новин є перспективним напрямом розвитку сучасних інформаційних систем. Використання глибинних моделей, таких як BERT, дозволяє досягати високої точності аналізу текстових даних, а розроблений веб-застосунок є дієвим інструментом для практичного використання результатів дослідження.

Література

1. Backlinko. Соціальні мережі: остаточний список статистичних даних користувачів у 2025 році [Електронний ресурс] – Режим доступу: https://backlinko.com/social-media-users

2. Readline. Основні статистичні дані щодо фейкових новин та дезінформації у ЗМІ у 2024 році [Електронний ресурс] – Режим доступу: https://redline.digital/fake-news-statistics/

3. Prachi N., Habibullah M., Rafi E., Khan R. Detection of Fake News Using Machine Learning and Natural Language Processing Algorithms [Електронний ресурс] – 2022. – DOI: 10.12720/jait.13.6.652-661

4. Roumeiotis K., Tselikas N., Nasiopoulos D. Fake News Detection and Classification: A Comparative Study of Convolutional Neural Networks, Large Language Models, and Natural Language Processing Models [Електронний ресурс] – 2025. – DOI: https://doi.org/10.3390/fi17010028

5. Probierz B., Stefański P., Kozak J. Rapid Detection of Fake News Based on Machine Learning Methods [Електронний ресурс] – 2021. – DOI: https://doi.org/10.1016/j.procs.2021.09.060

6. Petyk V. Ukrainian news [Електронний ресурс] – 2022. – Режим доступу: https://www.kaggle.com/datasets/zepopo/ukrainian-fake-and-true-news

УДК 354

ІННОВАЦІЙНІ ПРИСТРОЇ ДЛЯ ОПОВІЩЕННЯ МАЛОМОБІЛЬНИХ ГРУП НАСЕЛЕННЯ ПРО НЕБЕЗПЕКУ

Мар'ян ЛАВРІВСЬКИЙ, Інна ФЕДОРЮК, Христина ПЕТРУШКА
Львівський державний університет безпеки життєдіяльності

Проблема забезпечення доступності середовища для маломобільних груп населення є надзвичайно важливою у сучасному суспільстві. З кожним роком зростає кількість людей, які мають обмежені можливості пересування через інвалідність, похилий вік чи тимчасові фізичні обмеження.

Ключові слова: *маломобільні групи населення, інформування їх по сигналам небезпеки, цивільний захист, оповіщення маломобільних груп населення , безпека , адаптація, доступність.*

The issue of ensuring environmental accessibility for people with limited mobility is extremely important in modern society. Each year, the number of people with restricted mobility due to disability, old age, or temporary physical limitations is increasing.

Keywords: *people with limited mobility, informing them about danger signals, civil protection, alerting people with limited mobility, safety, adaptation, accessibility.*

Міжнародний досвід свідчить про те, що розбудова безбар'єрного простору – це нагальна вимога часу та потужна рушійна сила для розвитку країни. Адже безбар'єрність створює можливості для залучення до активного суспільного життя величезної кількості людей, чий потенціал раніше не використовувався повною мірою. В першу чергу це стосується маломобільних груп населення. Адже вони стикаються з бар'єрами більше за інших.

Маломобільні групи населення – хто це? Кожен з нас в певні періоди життя належить, або може належати до таких людей. Маломобільними в тій чи іншій мірі може вважатися від 30 до 50 відсотків українців. Маломобільні групи населення – це люди, що відчувають труднощі при самостійному пересуванні, одержанні послуги, необхідної інформації або при орієнтуванні в просторі. Таким чином, під дану категорію підпадає доволі велика частка населення.

Маломобільні групи населення є вразливішими у порівнянні з іншими людьми, адже складнощі, які вони відчувають у зв'язку зі своїм станом та незручним середовищем, дуже часто роблять їх залежними від допомоги або терпимості оточуючих. Так само, обмеження може бути викликане відсутністю досвіду або знання.

Сигнали тривоги (сирени) не чути людям із втратою слуху, а смартсповіщення на смартфоні часто недостатньо ефективні — 2 млн нечуючих не отримують адекватного попередження.

Лише ~2,5 % людей з інвалідністю переходять у бомбосховище під час сигналу тривоги, інші залишаються вдома або рухаються по коридорах через відсутність доступної інформації і підтримки

Для маломобільних груп населення існують як загальні, так і спеціалізовані пристрої для отримання сигналів тривоги. До них належать тради-

ційні системи оповіщення (сирени, гучномовці, радіо, телебачення), сучасні системи (спеціальні додатки на смартфонах, сповіщення через SMS) та індивідуальні пристрої (персональні пейджери, браслети, що вібрують), які можуть бути оснащені кнопками для виклику допомоги.

До загальних систем оповіщення можна віднести сирени, гучномовці**,** радіо та телебачення**,** персональні. У сучасному світі технології дедалі більше адаптуються до потреб людей з інвалідністю, зокрема осіб із порушеннями слуху. Важливим напрямом розвитку є створення пристроїв для оповіщення, попередження про небезпеку чи надзвичайні ситуації, а також засобів, які дозволяють таким людям залишатися на зв'язку та почуватися в безпеці.

Нижче наведено низку пристроїв, які можуть бути використані для сповіщення чи аварійних сигналів. Частина з них є медичними або універсальними моделями, що можуть бути адаптовані для осіб із порушенням слуху. Це, зокрема, B7 Medical Alert Wrist Button, Emerge-Alert Медичний браслет, GPS-браслет із SOS (для дітей та літніх людей), Health Alert Медичний голосовий браслет, Smart GPS Tracker Watch SOS Bracelet Video Call, EM-70 Бездротовий браслет аварійної сигналізації, B9 Cut-off Alert Wristband, TM-ALERT (рисунок 1).

а) б)

Рисунок 1 – Пристрої оповіщення: а) EM-70. б)TM-ALERT.

Інформування маломобільних груп населення про сигнали небезпеки є невід'ємною складовою системи цивільного захисту. Ефективність оповіщення визначається не лише технічними засобами, а й готовністю суспільства враховувати потреби кожної людини. Забезпечення рівного доступу до інформації, розробка адаптованих засобів сповіщення, навчання персоналу та населення — це основні умови зниження ризиків під час надзвичайних ситуацій.

Література

1. https://www.if.gov.ua/news/hto-taki-malomobilni-grupi-naselennya-i-chomu-bezbaryernist-stosuyetsya-kozhnogo-infografika
2. https://ud.org.ua/statti/299-malomobilni-grupi-naselennya-khto-tse
3. https://zakon.rada.gov.ua/laws/show/841-2013-%D0%BF

УДК: 004.4:378.147

TOOLS TO SUPPORT PROGRAMMING EDUCATION WITH THE HELP OF MULTI-ROLE AI AGENTS

Mykola LEHKYI, Hanna SHEVCHUK
Lviv Polytechnic National University, Lviv

Theoretically substantiates and experimentally validates a multi-role system of AI agents (Tutor, Evaluator, Coach) for supporting programming education. It presents a "routing → tools → evaluation" architecture, introduces the concept of Pedagogical Support Density, and reports results of a pilot experiment with students of Lviv Polytechnic.

Keywords: *programming education; AI agents; large language model; learning design; pedagogical roles.*

Теоретично обґрунтовано та експериментально перевірено багаторольову систему AI-агентів (Tutor, Evaluator, Coach) для підтримки навчання програмуванню. Описано архітектуру типу «routing → tools → evaluation», концепцію щільності педагогічної підтримки та результати пілотного експерименту зі студентами Львівської політехніки.

Ключові слова: *навчання програмуванню; агенти штучного інтелекту; велика мовна молель; дизайн навчання; педагогічні ролі.*

Rapid development of large language models and AI agent systems changes the conditions of teaching programming in higher education. AI tools can quickly explain errors, refactor code, and generate practice tasks, creating new opportunities for individualized support and instant feedback, but also risks of outsourcing independent work and violating academic integrity. This reveals a gap between spontaneous student use of general-purpose chatbots and the lack of didactically grounded models for integrating AI into programming courses under clear pedagogical and legal constraints.

The community place this problem within the broader regulatory and ethical framework: European and international AI acts and guidelines, together with Ukrainian regulations on academic integrity and personal data protection, require transparency of AI systems, clear delimitation of human and AI contributions, and prevention of manipulative or opaque assessment practices (European Commission, n.d.; European Parliament and Council of the European Union, n.d.; European Union, n.d.; Ministry of Education and Science of Ukraine, n.d.; William Fry, n.d.). Therefore, the research problem is to design a multi-role AI system that supports programming education, improves learning outcomes and remains compatible with these constraints.

The conceptual basis combines insights from higher education pedagogy, intelligent tutoring systems and recent research on generative AI in learning (Dorosh et al., 2024; Kozlovskyi et al., 2020; Mediakov et al., 2025; Mukan et al., 2023; Shihab et al., 2025; Shevchuk, 2022; Yurchak et al., 2024). Programming education is viewed as a guided process where the instructor and AI tools support problem

understanding, solution design, implementation, testing and reflection. A key construct is Pedagogical Support Density (PSD), defined as the relative saturation of the learning process with hints, explanations and micro-interventions from AI: excessively high PSD leads to over-helping, while too low PSD leaves the learner alone with difficulties. The system must therefore allow for configurable PSD levels and policies per task type and stage of learning.

The architecture is implemented as a simple multi-agent pipeline "incoming message → role detection → specialized agent". An input layer receives each student message and metadata; a role-detection component classifies it; then a router directs the request to one of three agents. The Tutor provides short explanations, focused code examples and micro-exercises with partially filled templates, and then analyzes student answers and errors, supporting the cycle "explanation – action – discussion of errors" under PSD constraints. The Evaluator performs rubric-based assessment of code on several criteria (Correctness, C# idioms, Clarity, Robustness, Efficiency), each graded on a 0–3 scale, and combines a numerical score (0–15) with concise, criterion-based recommendations. The Coach interprets scores and telemetry, structures feedback into strengths, areas for improvement, next steps and motivational messages, turning raw results into an understandable individual development plan.

The system was piloted in a real programming course at Lviv Polytechnic National University with 112 students. A mixed-methods design combined system telemetry, rubric-based assessment of student code and an online survey on perceived usefulness, clarity and fairness of the agents.

The results show high acceptability and pedagogical value. The overall usefulness of the system was rated 3.90/5, with 70.6% of responses in the "rather useful" or "very useful" range. The Tutor's explanations received 4.22/5, the fairness and clarity of the Evaluator's assessment 4.29/5, and 91.9% of students positively evaluated the Coach's recommendations. Moreover, 87.5% of students indicated that they would continue to use such agents in their studies. Telemetry confirmed these perceptions: the proportion of successfully solved tasks increased, the median time to complete typical assignments decreased, and the frequency of repeated errors went down.

The proposed multi-role AI system (Tutor–Evaluator–Coach) with controllable PSD and rubric-based assessment is both theoretically grounded and experimentally validated as a tool for supporting programming education under conditions of academic integrity and AI regulation. At the same time, further work is needed on tuning PSD policies, expanding exercise and feedback scenarios, and developing instructor-facing tools for configuring agent behaviour and monitoring the amount of AI support per student. Future research should explore the long-term impact of such systems across several semesters, compare alternative role configurations and support strategies, and adapt the architecture to other software engineering disciplines while preserving the central role of the human instructor and accounting for evolving capabilities and limitations of large language models.

Література

1. Dorosh, V., Vavryk, R., & Stankevych, O. (2024). Development of a sentiment analyzer using ChatGPT for the stock market. Bulletin of Lviv Polytechnic National University. https://science.lpnu.ua/sites/default/files/journal-paper/2024/apr/34347/29.pdf

2. European Commission. (n.d.). AI Act enters into force. Retrieved September 10, 2025, from https://commission.europa.eu/news-and-media/news/ai-act-enters-force-2024-08-01_en

3. European Parliament and Council of the European Union. (n.d.). AI Act: Article 5 – Prohibited AI practices. Retrieved August 25, 2025, from https://artificialintelligenceact.eu/article/5/

4. Kozlovskyi, Y. M., Ortynskyi, V. L., & Dolnikova, L. V. (2020). Pedagogy. Lviv Polytechnic National University Publishing House. https://vlp.com.ua/node/20098

5. Mediakov, O., Martianov, D., Lytvyn, V., Tsymbaliuk, T., & Fedasyuk, D. (2025). SED-UA-small: Ukrainian synthetic dataset for text embedding models. Bulletin of Lviv Polytechnic National University. https://science.lpnu.ua/sites/default/files/journal-paper/2025/may/39142/maket25066219052025ves-406-413.pdf

6. Ministry of Education and Science of Ukraine. (n.d.). Glossary of terms on academic integrity. Retrieved September 13, 2025, from https://mon.gov.ua/static-objects/mon/sites/1/vishcha-osvita/2018/10/25/glyusariy.pdf

7. Mukan, N., Huzii, I., & Lan, H. (2023). The influence of higher education development trends on specialists' training. Academy Vision. https://academy-vision.org/index.php/av/article/download/550/508/514

8. Shevchuk, H. (2022). Adult education in Ukraine: Main principles and perspectives. Current Issues of the Humanities, 49(2), 249–253. https://doi.org/10.24919/2308-4863/49-2-39

9. Shihab, M. I. H., Hundhausen, C., Tariq, A, Haque, S., Qiao, Y., & Mulanda, B. (2025). The effects of GitHub Copilot on computing students' programming effectiveness, efficiency, and processes in brownfield programming tasks. In Proceedings of the ACM Conference on International Computing Education Research (ICER '25). Advance online publication. https://doi.org/10.1145/3702652.3744219

10. William Fry. (n.d.). The time to AI Act is now: A practical guide to the AI Act. Retrieved August 28, 2025, from https://www.williamfry.com/knowledge/the-time-to-ai-act-is-now-a-practical-guide-to-the-ai-act/

УДК 004.3

РЕАЛІЗАЦІЯ СИСТЕМИ ЗБОРУ ТА АНАЛІЗУ ДАНИХ ДЛЯ МОНІТОРИНГУ СТАНУ РЯТУВАЛЬНИКА НА ОСНОВІ ARDUINO

Юрій ЛЕНЬ, Ігор МАЛЕЦЬ
Львівський державний університет безпеки життєдіяльності

У роботі розглянуто розробку персонального датчика рятувальника — компактного автономного пристрою для підвищення безпеки особового складу ДСНС під час виконання робіт у небезпечних умовах. Система базується на мікроконтролері Arduino та наборі сенсорів, що здійснюють контроль температури, наявності шкідливих газів та рухомості рятувальника. Реалізовано алгоритм автоматичного виявлення критичних ситуацій, таких як перегрів, задимлення або знепритомнення працівника, з подальшою передачею тривожного сигналу на базову станцію. Обґрунтовано ефективність використання недорогих сенсорних модулів та радіозв'язку для створення доступної та надійної системи моніторингу.

Ключові слова: *безпека рятувальника, Arduino, датчик руху, газоаналізатор, радіомодуль, моніторинг стану.*

Під час ліквідації наслідків надзвичайних ситуацій рятувальники постійно перебувають у умовах підвищеного ризику: задимлення, токсичні гази, високі температури та можливі травмування. Однією з причин збільшених втрат у таких умовах є відсутність індивідуальних систем моніторингу стану рятувальника, здатних своєчасно повідомити про небезпеку або втрату рухомості.

Персональні сигналізатори, що контролюють зовнішні параметри та фізичний стан працівника, використовуються у багатьох країнах, але їхня вартість залишається високою. Тому створення бюджетного та функціонального аналога на базі Arduino є актуальним завданням у сфері безпеки ДСНС.

Архітектура розробленої системи складається з трьох основних елементів:

1. Носимий модуль рятувальника — містить датчики температури, газу та руху.
2. Мікроконтролер Arduino, який обробляє дані та визначає наявність небезпеки.
3. Базова станція з приймачем, яка отримує попереджувальні сигнали та інформує керівника групи.

Температурний сенсор здійснює контроль перегріву, газовий — наявності токсичних або вибухонебезпечних газів, а акселерометр визначає рухомість рятувальника та фіксує можливе падіння або втрату свідомості.

Передача даних здійснюється через радіомодуль типу NRF24L01 або HC-12. Алгоритм роботи включає періодичний збір показників сенсорів, аналіз порогових значень та формування тривожних повідомлень у разі виявлення небезпечних умов. Такий підхід забезпечує виявлення проблеми ще до того, як вона стане критичною, що підвищує шанси на своєчасну допомогу рятувальнику.

Створення персонального датчика рятувальника є ефективним рішенням для підвищення рівня безпеки при виконанні робіт у зоні надзвичайних ситуацій. Пристрій може бути легко масштабований, модернізований та адаптований для різних умов роботи.

Література

1. https://bababuilds.com/blog/complete-guide-mq-series-gas-sensors/ - MQ Series Sensors information
2. https://cdn.sparkfun.com/assets/f/7/d/9/c/DHT22.pdf - DHT22 (датчик температури який буде використовуватись)
3. https://www.analog.com/media/en/technical-documentation/data-sheets/adxl345.pdf - датчик руху/падіння, що підходить для фіксації нерухомості рятувальника.
4. https://manuals.plus/uk/digi/xbee-pro-900hp-rf-module-manual - документація для бездротової передачі сигналу між сенсорним модулем та базовим модулем.

ЕРА ІНТЕЛЕКТУАЛЬНОГО ВИРОБНИЦТВА: РОЗРОБКА АДАПТИВНОЇ НЕЙРОМЕРЕЖЕВОЇ СИСТЕМИ ZERO-DEFECT ДЛЯ МОНІТОРИНГУ ТА САМОКОРЕКЦІЇ 3D-ДРУКУ

Аліна ЛИН, Роман ГОЛОВАТИЙ
Львівський державний університет безпеки життєдіяльності, м. Львів

Анотація. *У цій роботі викладено опис проєктування та впровадження адаптивної системи Zero-Defect (Нуль Дефектів), що базується на глибоких нейронних мережах, для моніторингу та самокорекції 3D-друку за технологією пошарового наплавлення (FDM) у режимі реального часу. Традиційні методи контролю якості є післяпроцесними та неефективними. Наш підхід використовує Згорткові Нейронні Мережі (CNN) для обробки візуальних та сенсорних даних, миттєво виявляючи дефекти друку (наприклад, зсув шарів, викривлення, недостатня екструзія). Система має механізм зворотного зв'язку, який динамічно коригує параметри друку (температуру сопла, швидкість потоку, швидкість) для усунення виявлених аномалій на місці, з метою значного зменшення витрат матеріалу та досягнення справжнього промислового контролю якості в рамках концепції Індустрії 4.0.*

Ключові слова: *Нуль Дефектів (Zero-Defect), Нейронні Мережі, Моніторинг у Режимі Реального Часу, Самокорекція, 3D-Друк, Комп'ютерний Зір, Пошарове Наплавлення (FDM).*

Annotation. *This work outlines the design and implementation of an adaptive Zero-Defect system based on deep neural networks for real-time monitoring and self-correction in Fused Deposition Modeling (FDM) 3D printing. Traditional quality control methods are post-process and inefficient. Our approach utilizes Convolutional Neural Networks (CNN) to process visual and sensor data, instantly detecting printing defects (e.g., layer shifting, warping, under-extrusion). The system features a feedback mechanism that dynamically adjusts printing parameters (nozzle temperature, flow rate, speed) to mitigate detected anomalies in situ, aiming to significantly reduce material waste and achieve true industrial quality control within the framework of Industry 4.0.*

Keywords: *Zero-Defect, Neural Networks, Real-Time Monitoring, Self-Correction, 3D Printing, Computer Vision, Fused Deposition Modeling (FDM).*

Технології адитивного виробництва (3D-друк) відіграють ключову роль в Індустрії 4.0, забезпечуючи швидке прототипування та виробництво складних деталей. Однак, технологія FDM (Fused Deposition Modeling) залишається вразливою до численних дефектів, спричинених зовнішніми факторами та нестабільністю процесу (наприклад, зміною температури навколишнього середовища, неоднорідністю філаменту). Традиційний контроль якості є постфактумним і призводить до значного відсотка браку та перевитрати ресурсів. Вирішення цієї проблеми вимагає переходу до інтелектуального виробництва з використанням методів штучного інтелекту.Метою роботи є розробка та тестування архітектури програмно-

апаратного комплексу, здатного до автономного виявлення та активної корекції дефектів 3D-друку в режимі реального часу.

Система Zero-Defect базується на двокомпонентному підході: Моніторинг та Корекція. Для збору даних використовуються два типи інформації: візуальні (потік відеоданих з високої роздільної здатності камери, сфокусованої на зоні друку) та сенсорні (телеметрія принтера, така як температура столу/екструдера, швидкість руху та показники вібрації). Для обробки візуальних даних та розпізнавання дефектів застосовується оптимізована Згорткова Нейронна Мережа (CNN), наприклад, модифікація архітектури YOLOv8 або SSD. Мережа тренується на великому датасеті типових дефектів FDM-друку і здатна класифікувати та локалізувати аномалії (як-от зсув шару, викривлення, недостатня екструзія), оцінюючи їхню критичність у режимі реального часу. На виході нейромережі формується вектор аномалії, який включає тип дефекту, його просторове положення та рівень впевненості.

Ключовим елементом роботи є алгоритм адаптивної корекції. На відміну від простого зупинення друку при виявленні помилки, наша система втручається у процес, використовуючи багатокритеріальну модель прийняття рішень (наприклад, модель на основі дерева рішень або регресії), натреновану на зв'язку між параметрами друку та виникаючими дефектами. При виявленні аномалії, такої як недоекструзія, алгоритм плавно змінює параметри: збільшує потік (Flow Rate) або підвищує температуру екструдера. У разі виявлення викривлення (Warping) система може знизити швидкість друку або скоригувати температуру сопла, щоб мінімізувати термічні напруження. Система генерує нові G-код команди, які динамічно вставляються в чергу виконання, замінюючи або модифікуючи заплановані команди. Цей замкнений цикл із зворотним зв'язком забезпечує адаптацію до умов, що змінюються, і є основою для досягнення режиму Zero-Defect.

Успішна реалізація системи Zero-Defect напряму залежить від її здатності працювати з мінімальною затримкою, оскільки корекція має відбуватися швидше, ніж дефект встигне завдати значної шкоди. Це вимагає оптимізації нейромережевої моделі для забезпечення високої швидкості інференсу (inference speed). Для досягнення цієї мети застосовується техніка квантизації параметрів нейронної мережі та використання Edge AI — розміщення обчислювального модуля (наприклад, на базі NVIDIA Jetson або спеціалізованих TPU) безпосередньо біля принтера, а не у віддаленому хмарному середовищі. Це мінімізує затримку передачі даних та забезпечує суворий детермінізм роботи системи. Крім того, інтеграція системи вимагає розробки проміжного програмного забезпечення (middleware), яке б забезпечувало надійний інтерфейс між модулем CNN, алгоритмом корекції

та прошивкою 3D-принтера (наприклад, Marlin або Klipper), що також є важливим програмним завданням.

Висновки. Розроблена концепція системи адаптивного моніторингу та самокорекції на основі глибоких нейронних мереж є критично важливим кроком до реалізації повноцінного інтелектуального виробництва в адитивних технологіях. Впровадження цієї системи дозволить істотно знизити матеріальні та часові втрати, підвищити надійність виробничого процесу та якість кінцевого продукту, що є необхідною умовою для серійного використання 3D-друку в промисловості.

Література

1. Методи Контролю Якості Fdm 3d-Друку На Основі Візуального Моніторингу: Огляд Останніх Розробок. Сухоставський В., Скиба М., Поліщук О., Лісевич С. Хмельницький Національний Університет (2025) — Огляд Методів Візуального Моніторингу Якості Fdm 3d-Друку: Камери, Тепловізори, 3d-Сканери. https://heraldts.khmnu.edu.ua/index.php/heraldts/article/view/1885

2. Застосування Методів Машинного Навчання До Управління 3d Принтером. Бондарчук А. П., Олейніков І. А., Бажан Т. О. Державний Університет Інформаційно-Комунікаційних Технологій, Київ (2024) — Дослідження Застосування Методів Машинного Навчання Для Управління 3d-Принтером
https://tit.duikt.edu.ua/index.php/telecommunication/article/view/2508

3. Використання OctoPrint з Raspberry Pi для керування 3D-принтерами

4. https://www.raspberrypi.com/news/octoprint/.

5. Адитивні Технології: Перспективи І Проблеми 3d-Друку (І Частина). Андрощук Г. (2017) — Аналіз Адитивних Технологій, Перспектив І Проблем 3d-Друку В Україні https://ekmair.ukma.edu.ua/items/8eca51eb-ab95-4640-a17d-973cd902b4ae

УДК 004.8:004.4:005.96

AI-АСИСТЕНТИ В IT: ДОПОМОГА ЧИ ЗАГРОЗА ДЛЯ РОЗРОБНИКІВ ТА ДИЗАЙНЕРІВ?

Вікторія ЛОЗА, Ольга СМОТР
Львівський державний університет безпеки життєдіяльності

Анотація. *У роботі досліджується вплив AI-асистентів на професії у сфері IT, зокрема програмування та дизайн. Проаналізовано, як штучний інтелект змінює робочі процеси, підвищує ефективність спеціалістів і водночас створює нові виклики, пов'язані з автоматизацією технічних та творчих завдань.*

Ключові слова: *AI-асистенти, штучний інтелект, автоматизація, програмування, IT-індустрія.*

Abstract. *The paper explores the impact of AI assistants on professions in the IT field, particularly programming and design. It analyzes how artificial intelligence transforms work processes, enhances specialists' efficiency, and at the same time creates new challenges related to the automation of technical and creative tasks.*

Keywords: *AI assistants, artificial intelligence, automation, programming, IT industry.*

Сучасний розвиток штучного інтелекту (ШІ) радикально змінює сферу інформаційних технологій, формуючи нові підходи до роботи, навчання та творчості [1,2]. Особливе місце серед інновацій займають AI-асистенти: системи, здатні аналізувати великі обсяги даних, автоматизувати процеси, допомагати у програмуванні, дизайні, тестуванні та комунікації. Проте, поряд із численними перевагами постає питання: чи є такі інструменти підтримкою для фахівців, чи вони несуть потенційну загрозу для їхньої професійної ролі?

AI-асистенти сьогодні активно інтегруються у всі напрями IT. Для розробників вони стають незамінними помічниками у написанні коду, пошуку помилок, оптимізації алгоритмів і створенні технічної документації. Прикладом є GitHub Copilot, який на основі аналізу контексту пропонує програмісту фрагменти коду, або ChatGPT, що може пояснювати логіку складних функцій. У середовищах розробки, таких як IntelliJ IDEA чи Visual Studio Code, з'явилися вбудовані AI-модулі, які пропонують підказки, аналізують помилки в реальному часі й допомагають дотримуватися принципів чистого коду. Це дозволяє спеціалісту зосередитися не на рутині, а на структурі проєкту, архітектурі та креативних рішеннях. Порівняльна характерис-тика найбільш популярних з них на сьогодні у спільноті IT розробників наведена у таблиці 1.

Таблиця 1. Порівняльна характеристика AI-застосунків для розробки коду

AI застосунок	Основні функції	Переваги	Обмеження
GitHub Copilot	Автогенерація коду, завершен-ня функцій, інтеграція з IDE	Глибока інтеграція з VS Code, підтримка багатьох мов	Не завжди точний код, потребує GitHub-акаунт
Tabnine	ML-підказки, локальна генерація коду	Працює офлайн, приватність, швидкий автокомпліт	Обмежена генерація складних функцій
Amazon CodeWhisperer	Генерація коду, рекомендації AWS, безпека	Безкоштовний для особистого використання, фокус на AWS	Обмежена підтримка IDE поза AWS
Codeium	Автокомпліт, пошук по доку-ментації, генерація функцій	Безкоштовний, швидкий, підтримка багатьох мов	Менше спільноти, новий продукт
Replit Ghostwriter	Генерація коду в браузері, пояснення коду	Зручний для новачків, вбудований у Replit	Обмежена підтримка складних проєктів
AskCodi	Генерація SQL, документації, тестів	Підтримка специфічних запитів, зручний інтерфейс	Менш ефективний для великих кодових баз
ChatGPT	Пояснення логіки функцій, генерація коду, рефакторинг, навчання	Гнучкий, підтримує багато мов, пояснює складні концепти	Не інтегрований напряму в IDE, потребує копіювання коду
AI-модулі для IntelliJ IDEA / VS Code	Підказки, аналіз помилок у реальному часі, чистий код, рефакторинг	Глибока інтеграція, підтримка принципів SOLID, миттєвий фідбек	Залежність від конфігурації IDE, іноді потребують інтернет підключення

У сфері дизайну роль штучного інтелекту стає не менш відчутною. У програмах Adobe Photoshop та Illustrator інтегровані інструменти Adobe Firefly, здатні генерувати зображення, фони або об'єкти на основі текстового опису. Це суттєво прискорює процес роботи й допомагає створювати оригінальні композиції навіть без тривалого ручного опрацювання.

У Figma з'явилися AI-функції, які автоматично генерують варіанти інтерфейсів, адаптують компоненти під різні екрани, створюють тексти-заповнювачі та навіть пропонують дизайн-рішення на основі аналізу стилю бренду. Таким чином, штучний інтелект стає інструментом співтворчості, який не замінює дизайнера, а підсилює його потенціал і розширює межі експериментів.

ШІ активно впроваджується й у суміжних напрямках — відеомонтажі, музиці, 3D-моделюванні, аналітиці даних. Наприклад, Adobe Premiere Pro автоматично вирівнює звук, знаходить ключові моменти відео або вирізає тло завдяки нейромережам. У Blender і Autodesk AI застосовується для генерації текстур і відновлення моделей. Така автоматизація дозволяє спеціалістам зосередитися на творчій частині, тоді як технічні процеси частково бере на себе алгоритм.

Разом із тим, у професійному середовищі не зникає питання потенційної загрози [3]. Деякі спеціалісти побоюються, що автоматизація поступово витіснить частину посад, особливо тих, що пов'язані з типовими або повторюваними завданнями. Проте більшість експертів сходяться на думці, що штучний інтелект не усуває людину з процесу, а змінює характер її праці. Фахівці нового покоління мають не конкурувати з AI, а навчитися ефективно співпрацювати з ним — формулювати точні запити, аналізувати результати та креативно застосовувати їх на практиці.

Використання AI-асистентів вимагає також нових компетенцій. Важливо розуміти принципи роботи алгоритмів, оцінювати достовірність отриманої інформації, володіти критичним мисленням і етичними навичками. У дизайні, наприклад, постають питання унікальності стилю, авторських прав і збереження творчої ідентичності. У програмуванні — точності, безпеки даних і запобігання генерації шкідливого коду. Таким чином, головним завданням фахівців стає пошук балансу між автоматизацією та людською креативністю.

Попри побоювання щодо втрати робочих місць, саме AI-асистенти відкривають нові перспективи. Вони допомагають молодим спеціалістам швидше навчатися, підвищувати продуктивність і досягати високої якості результату навіть із мінімальним досвідом. ШІ стає не конкурентом, а партнером, який дає змогу професійно зростати, оптимізуючи робочі процеси й розширюючи можливості кожного користувача.

Висновок: AI-асистенти у сфері інформаційних технологій виступають не загрозою, а каталізатором подальшого розвитку галузі, сприяючи формуванню нових форматів взаємодії людини й технологій. Їхнє впровадження забезпечує підвищення ефективності роботи розробників і дизайнерів, зниження когнітивного та операційного навантаження, скорочення часу виконання завдань і поліпшення якості кінцевих результатів. Майбутнє професій у галузі IT визначатиметься не протистоянням людини й машини, а здатністю фахівців інтегрувати інтелектуальні інструменти у власну діяльність, зберігаючи при цьому креативність, гнучкість мислення та гуманітарно орієнтований підхід до розв'язання професійних завдань.

Література

1. Смотр О. (2025). Тенденції застосування штучного інтелекту у процесі підготовки фахівців служби цивільного захисту / О. Смотр // збірник наук. праць ІІ Міжнародної науково-практичної конференції «Актуальні питання підготовки фахівців для сектору безпеки і оборони» (м. Кропивницький, 17 квітня 2025 року). – Кропивницький : ДонДУВС, 2025. – 548-552 с.

2. Will artificial intelligence replace developers? [Електронний ресурс]. – Режим доступу: https://itvdn.com/ua/blog/article/will-artificial-intelligence-replace-developers (дата звернення: 19.11.2025).

3. AI-бум: чи загрожує він класичним професіям в IT? [Електронний ресурс]. – Режим доступу: https://galera.news/ai-bum-chy-zahrozhuie-vin-klasychnym-profesiiam-v-it-15752/ (дата звернення: 19.11.2025).

УДК 004

CRM-СИСТЕМА ДЛЯ ВОЛОНТЕРСЬКОГО ФОНДУ З АВТОМАТИЗАЦІЄЮ ОБЛІКУ ДОНАТОРІВ, ПОЖЕРТВ ТА ЗВІТІВ

Павло МАКАР, Юрій БОРЗОВ
Львівський державний університет безпеки життєдіяльності

Анотація. *Запропонована CRM-система для волонтерського фонду спрямована на автоматизацію обліку донорів, пожертв, зборів, звітів та волонтерів, забезпечуючи централізоване управління всіма даними з можливістю формування PDF-звітів. Використання Spring Boot із архітектурою MVC дозволяє створити масштабовану та ефективну веб-платформу, яка систематизує всі процеси фонду — від залучення донорів до обліку кожної транзакції та формування аналітики.*

Ключові слова: *CRM, волонтерський фонд, пожертви, донори, волонтери, автоматизація, Spring Boot, MVC-архітектура, звітність, PDF-генерація.*

Annotation*. A CRM system for a volunteer foundation is proposed to automate the management of donors, donations, fundraising campaigns, reports, and volunteers. The use of Spring Boot with an MVC architecture enables the development of a scalable and efficient platform that centralizes all operational processes, supports transaction tracking, and generates PDF reports.*

Keywords: *CRM, volunteer foundation, donations, donors, automation, Spring Boot, MVC architecture, reporting.*

Волонтерські фонди відіграють ключову роль у забезпеченні гуманітарної підтримки, організації зборів коштів та координації допомоги в умовах воєнних дій та надзвичайних ситуацій. Ефективна діяльність таких організацій потребує прозорої, структурованої та актуальної інформації про надходження, витрати, активні збори, донаторів та волонтерів. Відсутність централізованої системи управління часто призводить до плутанини, втрати даних, дублювання записів та ускладнює формування коректної звітності.

Розроблена CRM-система на основі Spring Boot реалізована відповідно до архітектури MVC, що забезпечує чітке розмежування логіки: від управління даними до їхньої презентації. Така структура сприяє швидкому розширенню функціоналу, підвищує продуктивність системи та спрощує її обслуговування.

Запропонована CRM-система враховує потребу у веденні детального обліку пожертв, контролю джерел фінансування, автоматизованого формування звітів і швидкого доступу до інформації про активні збори.

Розроблена CRM-система включає в себе наступні рівні: Рівень Model; Рівень Controller; Сервісний рівень.

Рівень Model представляє структуру даних, що включає сутності «Донор», «Пожертва», «Збір», «Звіт», «Волонтер». Кожна сутність відо-

бражає ключові характеристики - персональні дані донорів, суми пожертв, статуси зборів, дані про учасників волонтерської діяльності. Через ORM-підхід у поєднанні з MySQL забезпечується цілісність даних, їхня безпечна обробка та швидкий пошук.

Рівень Controller відповідає за обробку користувацьких запитів та передачу їх до сервісного шару. Завдяки цьому користувачі системи (адміністратори, бухгалтери, координатори зборів) можуть швидко переглядати інформацію про донорів, реєструвати нові пожертви, створювати збори, оновлювати статуси та формувати PDF-звіти.

Сервісний рівень реалізує бізнес-логіку CRM, включаючи валідацію даних, розрахунок загальних сум, формування деталізованої статистики за періоди, а також автоматичне генерування звітності. Це забезпечує прозорість фінансової діяльності та спрощує аудит волонтерського фонду.

Додатково система підтримує інтеграцію з платіжними API, що дає можливість автоматично отримувати інформацію про транзакції та зменшує ризик помилок при ручному введенні даних. Система також може надсилати автоматизовані сповіщення про нові пожертви, оновлення статусів зборів або необхідність формування звіту.

Висновок. Запровадження такої CRM-системи надає можливість підвищити ефективність управління волонтерським фондом, мінімізує ризики втрати даних та покращує якість фінансової звітності, забезпечуючи прозорість для донорів та партнерів.

Література

1. Payne, A., & Frow, P. Strategic Customer Management: Integrating Relationship Marketing and CRM. – Cambridge University Press, 2013.

2. Spring Framework Documentation. – [Електронний ресурс]. – Режим доступу: https://docs.spring.io.

3. Buttle, F., & Maklan, S. Customer Relationship Management: Concepts and Technologies. – Routledge, 2019.

УДК 004.93:004.89

МЕТОДИ МАШИННОГО НАВЧАННЯ ДЛЯ КОМП'ЮТЕРНОГО ЗОРУ ЗА ОБМЕЖЕНОГО ОБСЯГУ ДАНИХ

Богдан МАЛЕЦЬ, Тарас ЗАБОЛОЦЬКИЙ
Львівський національний університет імені Івана Франка

Робота присвячена актуальній проблемі сучасного комп'ютерного зору - забезпеченню ефективного навчання моделей в умовах обмеженого обсягу даних. У тезах розглянуто основні перешкоди для використання традиційних згорткових нейронних мереж, зокрема високу вартість розмітки, питання конфіденційності та рідкість досліджуваних об'єктів.

Проаналізовано ключові методи вирішення проблеми дефіциту даних: перенесення знань (Transfer Learning), навчання на невеликій кількості прикладів (Few-Shot Learning), мета-навчання (Meta-Learning) та самостійне навчання (Self-Supervised Learning). Зокрема, описано принципи роботи Prototypical Networks, алгоритму MAML та методів контрастивного навчання. Зроблено висновок про ефективність цих підходів для адаптації моделей до нових задач в умовах обмежених ресурсів

Ключові слова: *комп'ютерний зір, машинне навчання, обмежені дані, Transfer Learning, Few-Shot Learning, Meta-Learning, Self-Supervised Learning.*

У сучасну епоху цифрової трансформації комп'ютерний зір є одним із ключових напрямів розвитку, що знаходить застосування від медицини до систем безпеки. Однак фундаментальною проблемою залишається необхідність ефективного навчання моделей, коли доступний лише обмежений обсяг даних. Це зумовлено високою вартістю розмітки, конфіденційністю або рідкістю об'єктів дослідження. Традиційні методи, такі як згорткові нейронні мережі, потребують великих масивів даних, тому актуальними стають підходи, здатні працювати в умовах обмежених ресурсів.

Ефективна система аналізу даних в умовах їх дефіциту включає кілька ключових підходів: перенесення знань, навчання на невеликій кількості прикладів, мета-навчання та використання синтетичних даних.

Transfer Learning (Перенесення знань) Цей метод ґрунтується на використанні знань, отриманих моделлю на великому датасеті (наприклад, ImageNet), для нової задачі. Нижні шари мережі, що виділяють ознаки, залишаються незмінними, а верхні донавчаються. Основна ідея описується виразом:

$$f_{new}(x) = g(f_{pretrained}(x)) \quad (1)$$

де $f_{pretrained}(x)$ – ознаки з попередньо навченої мережі, а g(·)– «надбудова», що адаптується під нову задачу. Це дозволяє скоротити ресурси, хоча ефективність залежить від подібності доменів.

Few-Shot Learning (Навчання на невеликій кількості прикладів) Підхід орієнтований на класифікацію нових об'єктів після спостереження лише кількох прикладів. Популярним методом є Prototypical Networks, які формують центроїди класів (прототипи). Прототип класу C_k обчислюється як:

$$C_k = \frac{1}{|s_k|} \sum_{(x_i, y_i) \in S_k} f(x_i) \quad (2)$$

де s_k – множина прикладів класу, а $f(x_i)$ – вектор ознак . Класифікація здійснюється шляхом пошуку мінімальної відстані до прототипу.

Meta-Learning (Мета-навчання) Мета-навчання, або «навчання вчитися», спрямоване на швидку адаптацію до нових задач. Метод MAML налаштовує параметри моделі так, щоб вони адаптувалися за кілька кроків градієнтного спуску. Оновлення параметрів описується формулою:

$$\theta' = \theta - a\nabla_\theta L_{task}(f_\theta) \quad (3)$$

де a – коефіцієнт навчання, а L_{task} – функція втрат конкретного завдання. Цей підхід забезпечує високу швидкість адаптації, але є ресурсомістким.

Self-Supervised Learning (Самостійне навчання) Цей метод формує ознаки без розмітки, використовуючи допоміжні завдання або контрастивне навчання (SimCLR, BYOL). Мета полягає у зближенні представлень аугментацій одного зразка. Функція втрат InfoNCE має вигляд:

$$L(i,j) = -log \frac{exp(sim(z_i, z_i)/\tau)}{\sum_{k=1}^{N} exp(sim(z_i, z_i)/\tau)} \quad (2)$$

де $sim(z_i, z_i)$ – функція подібності (зазвичай косинусна), а τ – температурний параметр.

Література

1. Goodfellow I., Bengio Y., Courville A. Deep Learning. – Cambridge, MA : MIT Press, 2016.

2. Pan S. J., Yang Q. A survey on transfer learning // IEEE Transactions on Knowledge and Data Engineering. – 2010. – Vol. 22, No. 10.

3. Wang Y. et al. Generalizing from a few examples: A survey on few-shot learning // ACM Computing Surveys. – 2020. – Vol. 53, No. 3.

4. Snell J., Swersky K., Zemel R. Prototypical networks for few-shot learning // Advances in Neural Information Processing Systems (NeurIPS). – 2017.

5. Chen T. et al. A simple framework for contrastive learning of visual representations // Proceedings of the 37th International Conference on Machine Learning (ICML). – 2020.

6. Sutton R.S., Barto A.G. Reinforcement Learning: An Introduction. – MIT Press, 2018.

УДК: 004.056.53

ІМПЛІЦИТНІ НЕЙРОННІ ПРЕДСТАВЛЕННЯ (INR) ДЛЯ АУДІОСТЕГАНОГРАФІЇ: «ВБУДОВАНА» ПАМ'ЯТЬ МОДЕЛІ ЯК КОНТЕЙНЕР

Остап-Святослав МАЛЕЦЬ, Ольга СМОТР
Львівський державний університет безпеки життєдіяльності

Анотація. *У роботі розглянуто використання імпліцитних нейронних представлень (INR) як нового підходу до аудіостеганографії, де контейнером для прихованої інформації виступають вагові параметри моделі, а не сам аудіосигнал. Показано, що INR здатні відтворювати звук як неперервну функцію та одночасно зберігати додаткові дані без помітної зміни якості сигналу. Підхід демонструє вищу стійкість і непомітність порівняно з класичними методами.*

Ключові слова. *аудіостеганографія, імпліцитні нейронні представлення, приховані дані, SIREN, параметри моделі.*

Abstract. *This work explores the use of Implicit Neural Representations (INR) as a novel method for audio steganography, where hidden data is embedded directly into the model's parameters rather than in the audio signal itself. INR models represent audio as a continuous function and can store additional information without affecting perceptual quality. The approach offers improved robustness and invisibility compared to traditional techniques.*

Keywords. *audio steganography, implicit neural representations, hidden data, SIREN, model parameters.*

Аудіостеганографія вже багато років є важливою частиною інформаційної безпеки, але класичні методи приховування даних у звукових сигналах (LSB, фазові методи, спектральні модифікації) все частіше демонструють вразливість до сучасних алгоритмів аналізу та компресії. Імпліцитні нейронні представлення (Implicit Neural Representations, INR), що стрімко розвиваються останніми роками, пропонують принципово іншу модель зберігання аудіо — не як дискретного набору значень, а як неперервної функції, параметризованої вагами компактної нейронної мережі. Ці параметри можуть служити прихованим каналом передачі інформації без зміни самого звуку.

INR моделює аудіосигнал як функцію $f(t) \rightarrow a(t)$, де t — час, а $a(t)$ — амплітуда. Нейронна мережа навчається відтворювати значення сигналу у довільній точці часу, використовуючи архітектури SIREN або MLP з Фур'є-позиційним кодуванням. Тобто тим самим замість налаштування і коректування великою кількості даних яку ми отримую від звукового сигналу у вигляді коефіцієнтів нейронної мережі, ми замінюємо їх на формулу яка буде все більше і більше наближуватися до вигляду сигналу та оброблятися нейронними зв'язками. Крім того зявляється можливість парцювати з зразком будь-якої дожини та з будь-якої точки, що спростить подальшу роботу.

Однією з ключових властивостей імпліцитних нейронних представлень є те, що вони зберігають інформацію не у вигляді дискретних зразків, як це роблять традиційні аудіоформати, а у вигляді параметрів нейронної мережі, які апроксимують цілісний, неперервний сигнал. Це принципово змінює те, що ми вважаємо «контейнером» для звуку. У класичних методах контейнер — це або сам аудіофайл, або його оброблена версія. У випадку INR контейнером стає модель, а аудіо — лише функція, яку вона породжує. INR зберігає сигнал через набір ваг θ, які моделюють функцію[1]:

$$a(t) = f(t, \theta) \quad (1)$$

де t— час, а f— багатошаровий перцептрон, найчастіше з синусоїдальними або спектрально-кодованими активаціями. Ці ваги виконують роль особливого “простору пам’яті”: у них компактно закодовано структуру звукової хвилі, її гармонічні компоненти, динаміку та локальні високочастотні особливості. Оскільки аудіосигнал відтворюється як функція, параметри мережі можуть змінюватися в дуже широких межах без жодної помітної зміни звучання. Саме ця надлишковість робить INR придатним носієм прихованих даних.

При інтеграції додаткового повідомлення у модель змінюється не сама хвильова форма, а спосіб, яким мережа її описує. Це відбувається під час тренування шляхом модифікації цільової функції[2], наприклад:

$$L = L_{reconstruction} + aL_{hidden\_message} \quad (2)$$

Перший доданок відповідає за точне відтворення звуку, другий — змушує модель «запам’ятати» певну послідовність бітів. Таким чином у ваговому просторі формується область, прив’язана до прихованого повідомлення, але вона майже не впливає на якість аудіореконструкції. Це нагадує ситуацію, коли дві різні формули можуть описувати ту саму криву, і обидві будуть правильними, хоча внутрішня структура відрізняється. На практиці це означає, що INR дозволяє приховувати інформацію в місці, яке в традиційних аудіосистемах просто не існує.

Класичні стеганографічні методи завжди працюють із зміненою версією аудіо — модифікують молодші біти зразків, фазу або спектральні коефіцієнти, що залишає сліди для аналізу. INR ж дозволяє залишити сам сигнал недоторканим, приховуючи дані у структурі моделі. При цьому модель може витримувати квантизацію, перетворення зразків, конвертацію у різні формати або навіть видалення частини параметрів — приховане повідомлення зберігається, бо воно інтегроване не у конкретні значення, а у просторові взаємозв’язки між вагами.

Прикладом використання може бути приховування криптографічного ключа у моделі SIREN, де модель одночасно відтворює хвильову форму та містить додаткові біти даних. Ще один сценарій — приховування службової інформації або маркерів авторських прав у

параметрах MLP, які залишаються стабільними навіть після квантизації FP16. Окрім того, INR здатні містити часові послідовності, невеликі бінарні файли або метадані, які не зникають під впливом перетворення зразків або перекодування аудіо.

Завдяки поєднанню компактності, неперервності та високої місткості параметрів, INR формують новий підхід до аудіостеганографії, у якому контейнером стає не файл, а сама модель. Це робить метод особливо стійким та адаптивним у сучасних системах кодування звуку.

Література

1. Sitzmann V. et al. Implicit Neural Representations with Periodic Activation Functions, 2020.

2. Chen Z., Zhang H. Neural Fields in Audio Signal Processing: A Survey, 2023.

3. Zhu R. et al. Steganography in Neural Network Weights, 2022.

4. Valle R. et al. Neural Speech Synthesis using SIREN Features, 2022.

5. Meta AI. Neural Audio Codec (EnCodec), 2023.

6. Tancik M. et al. Fourier Features Let Networks Learn High Frequency Functions, 2021.

7. Huang S. et al. Neural Audio Compression with Trainable Codebooks, 2023.

УДК 641.8

БЕЗПІЛОТНІ ЛІТАЛЬНІ АПАРАТИ ЯК ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ В СИСТЕМІ ЦИВІЛЬНОГО ЗАХИСТУ

Анна МАРЦЕНЮК, Андрій ГАВРИСЬ
Львівський державний університет безпеки життєдіяльності

Сучасні технологічні дрони з їхнім вражаючим функціоналом стають дедалі необхіднішими для служб надзвичайних ситуацій. Використання БПЛА в операціях з ліквідації НС постійно збільшується, підтверджуючи їхню незамінну роль у забезпеченні безпеки.
Ключові слова: *цивільний захист, моніторинг і спостереження, аварійно-рятувальні роботи.*

Modern technological drones with their impressive functionality are becoming increasingly indispensable for emergency services. The use of UAVs in emergency response operations is constantly increasing, confirming their indispensable role in ensuring safety.
Keywords: *civil protection, monitoring and surveillance, emergency rescue operations.*

У сучасному світі, де дедалі частіше трапляються збройні конфлікти, техногенні аварії та природні катастрофи, безпілотні літальні апарати (БПЛА, або дрони) відіграють надзвичайно важливу роль у забезпеченні швидкого та ефективного реагування на надзвичайні ситуації. Їхнє значення виходить далеко за межі військових операцій — сьогодні дрони стали невід'ємним інструментом у ліквідації наслідків катастроф природного та техногенного характеру. Основними перевагами БПЛА є здатність оперативно обстежувати великі території, виконувати аерофотозйомку для оцінки масштабів руйнувань, а також доставляти медикаменти й обладнання у важкодоступні або небезпечні зони. Вони особливо цінні у випадках, коли традиційні методи рятувальних робіт є надто ризикованими або малоефективними [1]. Показовим прикладом стала аварія на АЕС «Фукусіма» у 2011 році, коли дрони використовувалися для моніторингу рівня радіації, що дозволило зменшити ризик для персоналу та забезпечити безперервний збір важливих даних із небезпечних ділянок.

Попри значні переваги, використання БПЛА пов'язане з низкою викликів. Їхня ефективність знижується в несприятливих погодних умовах — за сильного вітру, дощу чи снігу. Також існує потреба у вдосконаленні автономних систем керування, щоб зменшити залежність від оператора. Додатковою проблемою є недосконаліть правового регулювання, що ускладнює використання дронів у міжнародних рятувальних операціях. В Україні ризики виникнення надзвичайних ситуацій природного та техногенного характеру залишаються високими, тому постійне вдосконалення сил цивільного захисту, зокрема підрозділів ДСНС, є вкрай актуальним завданням

[2]. Це зумовлює необхідність впровадження системи оперативного моніторингу із використанням безпілотної авіації.

З 2014 року, на тлі воєнно-політичних подій, в Україні активно розвивається парк дронів, а з 2015 року налагоджено серійне виробництво вітчизняних моделей. Сучасні українські БПЛА здатні забезпечувати точні наукові спостереження, моніторинг у реальному часі та своєчасне реагування на надзвичайні події. Їхня головна перевага — відсутність пілота, що дозволяє виконувати завдання в умовах радіаційного, хімічного або біологічного забруднення без ризику для життя людей.

Безпілотні літальні апарати ефективно виявляють пожежі, осередки загоряння, здійснюють пошук людей та об'єктів, а також можуть замінювати пілотовану авіацію у складних або небезпечних умовах. Міжнародний досвід підтверджує доцільність широкого використання БПЛА у діяльності ДСНС України — насамперед для постійного моніторингу території, збору даних та оперативного реагування. Водночас впровадження дронів у систему цивільного захисту перебуває на початковому етапі [3,4]. Для досягнення успіху необхідно визначити пріоритетні напрями їхнього застосування, обрати оптимальні типи апаратів та забезпечити належну підготовку фахівців. Безпілотники для аварійно-рятувальних підрозділів мають бути оснащені системами оповіщення, фото та відеоапаратурою, а також інфрачервоними камерами.

Отже, розробка чіткої концепції створення, розвитку та вдосконалення БПЛА для потреб ДСНС України є стратегічно важливим завданням. Вона дозволить підвищити ефективність реагування на надзвичайні ситуації, мінімізувати людські втрати та зменшити масштаби шкоди від катастроф.

Література

1. Havrys, A., Yakovchuk, R., Pekarska, O., & Tur, N. (2023). Visualization of fire in space and time on the basis of the method of spatial location of fire-dangerous areas. http://doi.org/10.12912/27197050/156971.

2. Havrys, A. P., Tarnavsky, A. B., Lavrivskiy, M. Z., & Veselivsky, R. B. (2017). Rationale use of unmanned aircraft technology as a means of detecting accidents and emergencies situations.

3. Гаврись, А.П., & Марценюк, А. (2024). Застосування дронів при ліквідації надзвичайних ситуацій у світі. Матеріали XIX Міжнародної науково-практичної конференції молодих вчених, курсантів та студентів «Проблеми та перспективи розвитку системи безпеки життєдіяльності». – ЛДУ БЖД. – Львів. – 2024. – с. 27-29.

4. Гаврись А.П., Лаврівський М.З., Філіппова В.В., Марценюк А. (2024) Аналіз ефективності та перспектив застосування безпілотних літальних апаратів у сфері цивільного захисту. Міжнародний науковий журнал «Грааль науки». – Відень. – Листопад, 2024. – №46. – с.531-546. https://doi.org/10.36074/grail-of-science.29.11.2024

УДК 004.92:614.8

ЗАСТОСУВАННЯ АДИТИВНИХ ТЕХНОЛОГІЙ ТА 3D-МОДЕЛЮВАННЯ ДЛЯ РОЗРОБКИ ТА ОПТИМІЗАЦІЇ ОБЛАДНАННЯ ЦИВІЛЬНОГО ЗАХИСТУ

Станіслав МЄЗЄНЦЕВ, Володимир ПИЛИПЕНКО
Львівський державний університет безпеки життєдіяльності

Анотація. У роботі проаналізовано потенціал впровадження адитивних технологій та 3D-моделювання у діяльність підрозділів цивільного захисту. Розглянуто методи ергономічної оптимізації спорядження за допомогою цифрових двійників та перспективи застосування 3D-друку для оперативного ремонту й кастомізації обладнання. Обґрунтовано вибір інженерних матеріалів (композитів, високотемпературних полімерів) для виготовлення функціональних деталей в умовах надзвичайних ситуацій..

Ключові слова: *адитивні технології, 3D-моделювання, 3D-друк, цивільний захист, ергономіка, швидке прототипування, інженерні полімери.*

Abstract. The paper analyzes the potential of implementing additive technologies and 3D modeling in civil protection operations. Methods for ergonomic equipment optimization using digital twins and the prospects of 3D printing for rapid repair and customization are examined. The selection of engineering materials (composites, high-temperature polymers) for manufacturing functional parts in emergency conditions is justified.

Keywords: *additive technologies, 3D modeling, 3D printing, civil protection, ergonomics, rapid prototyping, engineering polymers.*

Сучасні виклики, що стоять перед Державною службою України з надзвичайних ситуацій (далі – ДСНС), вимагають не лише високого професіоналізму особового складу, але й постійної модернізації технічного оснащення. Традиційні цикли виробництва та закупівлі обладнання часто є довготривалими та дорогими. Водночас багато завдань потребують кастомізованих, нестандартних рішень, які неможливо отримати шляхом централізованих поставок. У цьому контексті технології 3D-моделювання та адитивне виробництво (3D-друк), відкривають нові горизонти для підвищення оперативності та ефективності підрозділів цивільного захисту.

Основна проблема полягає у розриві між стандартним, уніфікованим оснащенням рятувальників та унікальними вимогами конкретних надзвичайних ситуацій. Обладнання може бути ергономічно недосконалим, швидко виходити з ладу через поломку дрібних компонентів, а його ремонт чи заміна займає невиправдано багато часу. Метою роботи є аналіз потенціалу застосування технологій 3D-моделювання та 3D-друку для оптимізації та розробки спеціалізованого обладнання ДСНС.

1. Ергономічний аналіз та оптимізація.

Критичним фактором забезпечення ефективності роботи підрозділів цивільного захисту є ергономічна відповідність технічного оснащення та

робочих зон специфіці екстремальної діяльності, оскільки будь-які проєктувальні недоліки здатні спричинити функціональні затримки з потенційно фатальними наслідками. У цьому контексті застосування інструментарію тривимірного моделювання та технології цифрових двійників (Digital Twins) дозволяє реалізувати комплексний підхід до попередньої ергономічної валідації техніки та спеціального спорядження.

Зокрема, інтеграція цифрових антропоморфних моделей (Digital Human Models, DHM) забезпечує можливість проведення детального імітаційного аналізу взаємодії оператора з технічними засобами. В межах таких досліджень здійснюється оцінка зон досяжності органів керування з урахуванням обмежень рухливості, накладених повним комплектом екіпірування та засобами захисту органів дихання, а також аналіз оглядовості з робочого місця водія-оператора під час інтеграції нового обладнання. Окрім того, цифровий інжиніринг дозволяє виявити кінематичні конфлікти при суміщенні різних елементів індивідуального захисту та оцінити ергономіку людино-машинних інтерфейсів (HMI) робототехнічних комплексів. Така методологія уможливлює верифікацію конструктивних рішень та усунення колізій ще на довиробничій стадії, що суттєво оптимізує матеріально-технічні ресурси та скорочує цикл розробки спеціалізованого обладнання.

2. Швидке прототипування та адитивне виробництво.

Адитивне виробництво кардинально змінює підхід до ремонту та оснащення. Замість очікування на забезпечення, необхідні деталі можуть бути виготовлені безпосередньо в підрозділі.

Основні напрямки застосування:

Оперативний ремонт: Створення цифрової бібліотеки 3D-моделей дрібних деталей, що найчастіше ламаються (фіксатори, кришки, кнопки, кронштейни). Це дозволяє відновити працездатність дорогого обладнання (рацій, ліхтарів, медичних приладів) за лічені години.

Кастомізація та адаптація: Розробка та друк унікальних адаптерів. Прикладами є кріплення ліхтаря чи камери на новий тип шолома, тримач для планшета в кабіні оперативного автомобіля або спеціалізовані насадки на інструменти.

Малосерійне виробництво: Виготовлення нішевих виробів, які не виробляються масово, наприклад, компонентів для тренувальних макетів (безпечних копій ВНП), елементів турнікетів або унікальних інструментів для саперів.

3. Аналіз інженерних матеріалів для функціонального друку. Критичним зауваженням до 3D-друку є хибне уявлення про низьку міцність та термостійкість матеріалів. Для хобі-друку часто використовується PLA-пластик, який деформується вже при 60°C. Однак для інженерних завдань ДСНС використовуються зовсім інші полімери:

Інженерні пластики (ASA, PC): ASA (акрилонітрилстиролакрилат) має високу стійкість до ультрафіолету (для зовнішніх кріплень), а PC (полікарбонат) — екстремальну ударостійкість (для захисних корпусів). Їхня термостійкість сягає 90-130°C.

Композитні матеріали (PA-CF, PA-GF): Це "золотий стандарт" для функціональних деталей. Нейлон (PA), армований вуглецевим (Carbon Fiber, CF) або скляним (Glass Fiber, GF) волокном. Такі матеріали поєднують легкість, надзвичайну жорсткість та термостійкість (часто понад 150°C). Вони ідеально підходять для друку кронштейнів, важелів, деталей насосів та компонентів БПЛА.

Високотемпературні полімери (PEEK, ULTEM): Це суперконструкційні пластики з аерокосмічної галузі. Їхня робоча температура перевищує 250°C, вони є вогнетривкими та хімічно інертними. Використовуються для деталей, що можуть мати прямий контакт з гарячими елементами.

Гнучкі полімери (TPU): Термопластичний поліуретан використовується для виготовлення захисних бамперів, ущільнювачів та нековзних накладок на ручки інструментів.

Отже, використання технологій 3D-моделювання та адитивного виробництва є не просто допоміжним, а стратегічно важливим інструментом для підвищення боєздатності підрозділів ДСНС. Вони дозволяють перейти від моделі "очікування постачання" до моделі "виробництва за потребою". Впровадження ергономічного 3D-аналізу дозволяє підвищити безпеку та ефективність рятувальників, а використання сучасних композитних матеріалів для 3D-друку забезпечує створення функціональних, міцних та термостійких деталей, що не поступаються виготовленим традиційними методами.

Література

1. Busachi A. et al. A review of Additive Manufacturing technology for defence applications // Procedia CIRP. 2016. Vol. 55. P. 48–53.

2. Disaster emergency 3D printing humanitarian relief Nepal earthquake // The Guardian. 2015. 30 Dec. URL: https://www.theguardian.com/global-development/2015/dec/30/disaster-emergency-3d-printing-humanitarian-relief-nepal-earthquake

3. Human-Centered Design & Simulation // Siemens Digital Industries Software. URL: https://plm.sw.siemens.com/en-US/tecnomatix/human-centered-design-simulation/

УДК 004.8

ПОРІВНЯЛЬНИЙ АНАЛІЗ СЕРВІСІВ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ГЕНЕРАЦІЇ МУЗИЧНИХ КОМПОЗИЦІЙ

Олеся МИСЬКІВ, Роман ГОЛОВАТИЙ
Львівський державний університет безпеки життєдіяльності, Львів

Анотація. У роботі проведено аналіз ефективності трьох популярних AI-сервісів для генерації музики: Suno, TopMediaAI та Mureka. Основну увагу зосереджено на таких критеріях, як якість вокалу та тексту, доступність безкоштовних версій та гнучкість у роботі з різними жанрами. Описано хід експерименту, що включав створення поп-пісні українською мовою, а також тестування інструментарію на стилях Lo-fi та Epic. Встановлено, що Suno демонструє найкращі результати за сукупністю показників, забезпечуючи високу якість аудіо та демократичну модель ціноутворення.
Ключові слова: *генеративний штучний інтелект, музичний синтез, Suno, TopMediaAI, Mureka, аудіогенерація*

Annotation. This paper presents a comparative analysis of the effectiveness of three popular AI music generation services: Suno, TopMediaAI, and Mureka. The study focuses on criteria such as vocal and text quality, availability of free versions, and flexibility in handling various genres. The experiment involved creating a pop song in Ukrainian, as well as testing the tools with Lo-fi and Epic styles. The findings indicate that Suno demonstrates the best overall results, providing high-quality audio and a democratic pricing model.
Keywords: *generative AI, music synthesis, Suno, TopMediaAI, Mureka, audio generation.*

Технології штучного інтелекту в музичній індустрії досягли рівня, що дозволяє пересічному користувачеві створювати композиції за лічені секунди

Метою роботи є з'ясування практичності, доступності та якості сучасних інструментів для звичайної людини. Об'єктами дослідження обрано три популярні сервіси: Suno, TopMediaAI та Mureka.

Методологія дослідження включала три етапи:

- порівняння якості генерації на однаковому завданні (поп-пісня);
- перевірка гнучкості інструментів на інших стилях;
- аналіз моделі ціноутворення та доступності.

В рамках першого етапу моделям було надано ідентичний промпт: "Весела поп-пісня про студента-програміста, який не може знайти помилку в коді. Жіночий вокал, українською мовою". Аналіз результатів виявив суттєві відмінності в роботі алгоритмів.

TopMediaAI продемонстрував посередню якість: текст виявився нечітким, а вимова — "роботизованою". Крім того, сервіс надав лише один безкоштовний кредит, якого вистачило на дві спроби. Mureka показала ще

нижчий результат: слова у згенерованому треку було майже неможливо розібрати, при аналогічних обмеженнях у безкоштовному доступі.

Натомість Suno забезпечив найкращий результат: чіткий текст, виразний вокал, наявність логічної структури та рими. Вагомою перевагою стала модель кредитування: система надає 50 кредитів на день, при цьому на генерацію було витрачено лише 10.

На етапі тестування гнучкості (Етапи 2 і 3) подальші дослідження проводилися лише на базі Suno, оскільки ліміти безкоштовних кредитів у конкурентів (TopMediaAI та Mureka) були вичерпані після першого тесту. Suno успішно впорався із завданнями у стилях "Calm melancholic Lo-fi" та "Epic dark orchestral", продемонструвавши здатність адаптуватися до діаметрально протилежних жанрів.

Оцінювання та узагальнення результатів. Аналіз сильних сторін ШІ-композиторів показує, що лідери ринку (Suno) забезпечують вражаючу якість звуку та аранжування, а також здатні самостійно генерувати логічні тексти. Головною перевагою є "демократизація" творчості, що робить створення музики доступним для будь-якої людини.

Серед слабких сторін виділено проблему "умовної безкоштовності" більшості сервісів, які працюють у режимі "одноразового демо". Також суттєвим недоліком є відсутність точного контролю: користувач не може внести точкові правки (наприклад, змінити одне слово чи гучність окремого інструменту), що змушує покладатися на повторну генерацію.

Висновки. Результати дослідження дозволяють визначити сервіс Suno абсолютним лідером за всіма критеріями. ШІ-композитори вже стали потужним інструментом для створення фонової музики або розважального контенту. Однак через відсутність точних механізмів контролю генерації вони наразі не можуть повноцінно замінити професійних музикантів.

Література

5. Suno AI. Create music with AI. 20.12.2023. URL: https://suno.com (дата звернення: 09.11.2025).
6. TopMediaAI. AI Music Generator. 2022. URL: https://www.topmediai.com/ai-music-generator/ (дата звернення: 09.11.2025).
7. Mureka. AI Song Generator. 15.08.2024. URL: https://www.mureka.ai (дата звернення: 09.11.2025).
8. Agostinelli A. et al. MusicLM: Generating Music From Text. Google Research, 2023. URL: https://arxiv.org/abs/2301.11325 (дата звернення: 09.11.2025).
9. Литвин В. В., Висоцька В. А. Інтелектуальні системи: підручник. Львів: «Новий Світ-2000», 2023. 406 .

УДК 004.942

ДОСЛІДЖЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЗА ДОПОМОГОЮ 3D-МОДЕЛЮВАННЯ

Марина МОРОЗОВА, Олена СИДОРЕНКО
Національний технічний університет «Харківський політехнічний інститут», м.Харків

Анотація: У роботі розглянуто сучасні дослідження застосування 3D-візуалізацій у галузі інформаційної безпеки. 3D-моделювання може виступати у якості допоміжного засобу для полегшення розуміння складних зв'язків у системах захисту і сприяти ефективному виявленню загроз даним шляхом зменшення когнітивного навантаження на спеціалістів. На основі аналізу наведених досліджень зроблено висновок про перспективність подальшого розвитку 3D-інструментів як елементів сучасної кібербезпеки.
Ключові слова: *3D-моделювання, 3D-візуалізація, 3D-модель, інформаційна безпека, кібербезпека.*

Abstract: The theses review current research on the use of 3D visualizations in the field of information security. 3D modeling can serve as an auxiliary tool that facilitates the understanding of complex relationships in defense systems and supports effective threat detection by reducing the cognitive load on specialists. Based on the analysis of the referenced works, the study concludes that further development of 3D tools as components of modern cybersecurity is a promising direction..
Keywords: *3D modeling, 3D visualization, 3D model, information security, cybersecurity.*

Із зростанням складності сучасних комп'ютерних систем аналітики кібербезпеки стикаються з високим навантаженням на когнітивне сприйняття. Обмеженість традиційних засобів відображення даних впливає на важкість оцінювання рівня інформаційних загроз і подальше формування ситуаційних висновків. Використання 3D-візуалізацій може сприяти покращенню розуміння багатовимірних інформаційних структур, класифікацій поведінки систем та пристроїв.

Сучасні роботи дозволяють оцінити застосовність 3D-моделей для забезпечення відтворення складних системних топологій, виявлення логічних зв'язків або функціональних груп між елементами на прикладі досліджень заходів з кібероборони [1]. На думку науковців, 3D-представлення дозволяє оперувати більшою кількістю логічних та функціональних параметрів, які можуть бути присвоєні елементам системи (просторове розташування, форма, розмір тощо) і, в свою чергу, ефективніше зображати її (показувати групи сегментів, зони ризику, порушення структури, аномалії тощо) [1].

Таким чином, можна виділити переваги 3D-моделювання інформаційних систем і представлення їхніх елементів у вигляді просторових об’єктів з різними характеристиками, що полегшує зорове сприйняття, вивчення і класифікацію цих частин:

1. Наочність положення елементів (мережевих вузлів; компонентів програм, пристроїв або їхніх комплектуючих тощо).

2. Зв’язки між елементами (для демонстрації взаємодії, послідовності чи відповідності).

3. Формування загальної топології системи (для виявлення вразливих місць, прогнозування результатів роботи тощо).

Це дозволяє формувати цілісну структуру, візуально узгоджену з особливостями когнітивного сприйняття людини. На основі аналізу існуючих досліджень, можна дійти до висновку щодо перспективності використання 3D-візуалізацій у різних концепціях інформаційної безпеки комп'ютерних середовищ.

Література

1. Kullman K. Enhancing Cyber Defense Situational Awareness Using 3D Visualizations / K. Kullman, J. Cowley, N. Ben-Asher // Proceedings of the 13th International Conference on Cyber Warfare and Security (8-9 March 2018, Washington). – 2018. – 688 p. (1 Vol) – P. 369–378.

УДК 004.8

METRIC-DRIVEN OPTIMIZATION OF POLYNOMIAL COEFFICIENTS OBTAINED FROM NON-ITERATIVE MODELS

Roman Muzyka, Ivan Izonin
Lviv Polytechnic National University

The paper proposes a metric-driven optimization method for polynomial models synthesized from non-iterative SGTM neural-like structures. By optimizing polynomial coefficients directly under a target regression metric, the approach improves predictive performance while maintaining computational efficiency..

Keywords: *Non-Iterative Learning, Polynomial Optimization, Regression Metrics, Smart Systems.*

Анотація У роботі вперше розроблено метод метрично-орієнтованої оптимізації поліномів, синтезованих з неітеративних нейроподібних структур. Оптимізація коефіцієнтів під цільову метрику регресії забезпечує підвищення точності та збереження малої обчислювальної складності.

Ключові слова: *Неітеративне навчання, Поліноміальна оптимізація, Метрики регресії, Смарт-системи.*

1. Introduction

The development of smart systems and data-intensive applications has increased the need for machine learning methods that combine predictive accuracy with computational efficiency. Traditional deep learning relies on iterative gradient optimization, which is computationally expensive and often unsuitable for systems requiring real-time operation or low-energy consumption. Non-iterative neural-like structures such as the SGTM model [1] and Extreme Learning Machines (ELM) [2] address this limitation by using direct matrix computations instead of iterative backpropagation. These models train extremely quickly and require significantly fewer resources.

Despite their advantages, non-iterative models are usually trained under standard loss functions such as Mean Squared Error (MSE). However, in practice, model performance is evaluated according to domain-specific regression metrics that differ substantially from the training loss. This mismatch may cause the model to perform well according to the training objective but poorly according to the real-world evaluation criterion. Therefore, adapting the final stage of the model to the correct metric becomes essential for achieving meaningful and task-relevant results.

2. Proposed Method

This study proposes a metric-driven post-synthesis optimization technique that is applied after training a non-iterative SGTM neural-like structure. Once the SGTM model has been trained using direct linear-algebraic computation, a linear polynomial approximation of its output is constructed.

This is achieved using the diagonal matrix method described in [3], which makes it possible to extract an explicit polynomial mapping from the trained structure without iterative optimization. Since the SGTM model without preliminary nonlinear input expansion behaves as a linear mapping, the resulting polynomial is also linear, simplifying further optimization.

Instead of retraining the full SGTM structure, only the coefficients of this extracted linear polynomial are optimized. Crucially, this optimization is performed not with respect to the original training loss, but toward a specific regression metric selected by the user. Because the optimization concerns only a small set of coefficients, the computational cost remains extremely low, making the approach well-suited for applications where rapid adaptation and efficiency are critical.

This flexibility allows the proposed method to support a wide range of regression metrics. For example, Mean Absolute Error (MAE) measures the average magnitude of errors and is appropriate when all deviations should be treated uniformly. Root Mean Squared Error (RMSE) penalizes larger deviations more strongly and is used in robotics and automation where rare but severe errors are unacceptable. Coefficient of Determination (R^2) expresses the proportion of variance explained by the model and is widely used in scientific modeling. More specialized metrics include Nash–Sutcliffe Efficiency (NSE), which evaluates predictive performance relative to observed variance, and Kling-Gupta Efficiency (KGE), which additionally considers correlation, variability, and bias. The Index of Agreement (IA) evaluates the degree of agreement between predicted and observed values. In multi-criteria contexts, the Composite Error Index (CEI) integrates several error components into a single value. Because these metrics represent different characteristics of model behavior, the ability to optimize the polynomial directly toward one of them ensures that the final predictor aligns with real-world requirements.

3. Importance of Metric Selection

Regression metrics are not interchangeable: each captures a unique aspect of model error, and selecting the appropriate metric is essential for achieving reliable and interpretable performance in a given domain. Many applications require minimizing the average error magnitude, making MAE suitable due to its simple interpretation and equal weighting of all deviations. MAE is widely used in biomedical signal processing, environmental monitoring, and general forecasting.

In contrast, systems where large prediction errors are dangerous – such as autonomous vehicles, robotic manipulators, or industrial control – rely on RMSE, which amplifies large deviations through squaring. RMSE-based optimization encourages stable, low-risk predictions. Meanwhile, fields that emphasize explanatory power rather than absolute error magnitude frequently use R^2, which indicates the proportion of variance in the observed data explained by the predictor.

Modeling natural processes often requires metrics that capture complex dynamical properties. NSE is popular in hydrology and civil engineering because it evaluates how well the predicted time series follows the observed variability. KGE extends NSE by incorporating correlation, variability, and bias into a unified efficiency measure, making it valuable for environmental modeling and geosciences. When agreement between predicted and actual values needs to be evaluated comprehensively, the Index of Agreement (IA) provides a bounded and interpretable measure of predictive correspondence, used in climate modeling and ecological forecasting.

In multi-output or multi-criteria environments, CEI aggregates several error components into a single metric, enabling unified optimization. Choosing the correct metric ensures that model improvement efforts target the aspects of predictive performance that matter most to the specific application.

The proposed metric-driven polynomial optimization approach enables the model to be aligned with any of these metrics without retraining the underlying SGTM structure. As a result, the final predictor becomes more robust, better tailored to domain-specific requirements, and more accurate within the context of the chosen evaluation criterion.

4. Conclusion

In this study, we demonstrate that metric-driven optimization of polynomial coefficients offers a practical and efficient strategy for improving predictive performance in non-iterative neural-like systems. By extracting a linear polynomial from a trained SGTM model and optimizing it directly with respect to a chosen regression metric, the approach provides strong domain-oriented accuracy while preserving the computational advantages of non-iterative learning. This makes the method well-suited for real-time smart systems and large-scale structured data analysis where both speed and precision are essential.

Література

1. Tkachenko R. An integral software solution of the SGTM neural-like structures implementation for solving different data mining tasks. Lecture notes on data engineering and communications technologies. 2022. No. 77. URL: https://doi.org/10.1007/978-3-030-82014-5_48 (date of access: 01.11.2025).

2. Non-iterative and fast deep learning: multilayer extreme learning machines / J. Zhang et al. Journal of the franklin institute. 2020. Vol. 357, no. 13. P. 8925–8955. URL: https://doi.org/10.1016/j.jfranklin.2020.04.033.

3. Multiple linear regression based on coefficients identification using non-iterative SGTM neural-like structure / I. Izonin et al. Advances in computational intelligence. Cham, 2019. P. 467–479. URL: https://doi.org/10.1007/978-3-030-20521-8_39 (date of access: 03.11.2025).

УДК 371.3

ПЕРСПЕКТИВИ ВИКОРИСТАННЯ AR-ДОДАТКІВ У ТУРИСТИЧНІЙ ДІЯЛЬНОСТІ

Ігор НАЛИВАЙКО, Юлія ГУРАЛЬ
Львівський національний університет ветеринарної медицини та біотехнологій імені Степана Ґжицького, м.Дубляни

Анотація. *Здійснено огляд основних напрямів використання смарт-технологій у туристичній сфері. Наведено приклади практичного застосування технології доповненої реальності для підвищення якості туристичних послуг та вдосконалення туристичного досвіду. Окреслено перспективи покращення процесу управління туристичними маршрутами, об'єктами та туристичними потоками завдяки інтеграції технології доповненої реальності з іншими цифровими інструментами*

Ключові слова: *інформаційні технології, доповнена реальність, туризм, туристичні послуги, цифровізація.*

Abstract*. An overview of the primary directions of smart technology implementation in the tourism sector has been provided. Examples of practical applications of augmented reality technology for improving the quality of tourism services and enhancing tourist experience are presented. The prospects for optimizing the management of tourism routes, tourist attractions, and visitor flows through the integration of augmented reality technology with other digital tools are outlined.*

Keywords: *: information technologies, augmented reality, tourism, digitalization.*

Проблематика Розвиток інформаційних технологій останніми роками суттєво вплинув на цифровізацію туристичної індустрії[1]. Сучасний туризм дедалі активніше використовує мобільні додатки, геоінформаційні системи, навігаційні сервіси, персоналізовані рекомендаційні алгоритми та інші цифрові інструменти. Значна частина туристичних компаній, музейних установ, культурно-історичних комплексів та органів місцевого самоврядування інтегрують інформаційні технології у свою діяльність з метою підвищення привабливості туристичних продуктів та оптимізації взаємодії з відвідувачами.

Цифровізація туризму охоплює широкий спектр процесів: від віртуальних екскурсій та навігаційних сервісів до автоматизованих систем обліку відвідувачів, персоналізованих рекомендацій та інструментів маркетингової аналітики. Експерти туристичного ринку виокремлюють ключові напрями застосування смарт-технологій у туризмі:

Збір та аналіз інформації (GIS-карти, мобільна навігація, системи моніторингу туристичних потоків, аналітика поведінки користувачів).

Управління та прийняття рішень (планування маршрутів, управління туристичними локаціями, підвищення безпеки відвідувачів).

Створення та надання туристичних послуг (цифрові гіди, AR/VR-екскурсії, інтерактивні маршрути, персоналізований туристичний контент).

Технологія доповненої реальності є перспективним компонентом сучасних туристичних сервісів. Під доповненою реальністю розуміють технологію, що накладає комп'ютерно створені віртуальні елементи на реальне оточення користувача, забезпечуючи глибшу, інтерактивну та персоналізовану взаємодію з туристичними об'єктами.

У туристичній діяльності AR відкриває можливості, які складно реалізувати традиційними методами: реконструкцію історичних подій, відтворення архітектурних споруд, що не збереглися, віртуальну взаємодію з експонатами в музеях, детальні коментарі до туристичних об'єктів у режимі реального часу. Використання AR-додатків полегшує орієнтування на місцевості, забезпечує швидкий доступ до інформації та підвищує рівень залучення туристів.

В умовах високої конкуренції між туристичними дестинаціями технологія доповненої реальності дозволяє створювати унікальні туристичні продукти, що поєднують елементи гри, інтерактивності, історичної реконструкції та персоналізованого супроводу. AR може використовуватися у музеях, екопарках, на історичних локаціях, у туристично-інформаційних центрах, на фестивалях, у готелях і транспортних вузлах [2].

Суттєві переваги дає інтеграція AR з іншими смарт-технологіями — геолокацією, цифровими картами, сенсорами, аналітичними системами, а також з генеративним штучним інтелектом, який здатний формувати адаптивні маршрути, перекладати інформацію у реальному часі та надавати персональні рекомендації.

У таблиці 1 наведено основні напрями застосування доповненої реальності у туристичній діяльності.

Таблиця 1

Застосування доповненої реальності у туризмі

Назва	Опис
Інтерактивні екскурсії	AR забезпечує показ додаткових візуальних елементів: 3D-моделей, реконструкцій, анімацій, історичних сцен без встановлення громіздкого обладнання.
Навігація та орієнтування	Турист може отримувати підказки на екрані смартфона: напрямки руху, відстань до об'єктів, рекомендації щодо локацій поблизу.
Музейні AR-експозиції	Дозволяють оживляти експонати, показувати їх у первісному вигляді, доповнювати аудіо- та відеокоментарями.
Маркетинг і промоція дестинацій	AR-рекламні матеріали забезпечують ефект присутності, дозволяють майбутньому туристу "переглянути" місце перед подорожжю.
Підвищення безпеки туристів	Виведення на екран смартфона попереджень, рекомендацій щодо поведінки, даних про небезпечні ділянки маршруту.

Джерело: узагальнено на основі даних [3]

Прикладами використання технології доповненої реальності в туризмі можуть бути: оптичні системи (smart-окуляри), відео-overlays на смартфонах, технології маркерної та маркер-less AR, а також мобільні додатки, що належать до категорії Mobile Augmented Reality. Такі інструменти дозволяють туристам взаємодіяти з культурною спадщиною більш глибоко та інформативно.

Однак ефективність використання AR у туристичній сфері [4] залежить від низки факторів:

1. якість інтернет-покриття та доступ до мобільних мереж;
2. рівень цифрової інфраструктури та технічного забезпечення туристичних об'єктів;
3. фінансові витрати на створення та підтримку AR-контенту;
4. потреба у навчанні персоналу та оновленні туристичних матеріалів.

Незважаючи на певні обмеження, технологія доповненої реальності має потенціал стати важливим драйвером розвитку туристичної галузі, забезпечуючи підвищення якості послуг, покращення туристичного досвіду та конкурентоспроможності туристичних дестинацій.

Література

1. Смарт-технології в агроменеджменті [Електронний ресурс] – Режим доступу: https://blog.agrokebety.com/smart-tehnologii-v-agro-menedgmente-ua blog.agrokebety.com

2. АнтоненкоІ.Я., Журба Ю.Р. Технологія доповненої реальності в туризмі. Матеріали ІІІ Міжнар. наук.-практ. конф. *Сталий розвиток туризму на засадах партнерства: освіта, наука, практика*. м. Львів, 23-24 листопада 2023 р. Львів: ЛТЕУ, 2018. 342 с. С.174-177

3. Ростовцев С.С. Доповнена реальність як конкурентна перевага в туристичному бізнесі. *Perspectives of digital technologies in activities of agrarian enterprises* [Електронний ресурс] – Режим доступу: http://www.econom.stateandregions.zp.ua/journal/2019/1_2019/16.pdf

4. Як AR-технології роблять культурну спадщину ближчою до людей [Електронний ресурс] – Режим доступу: https://reherit.org.ua/yak-ar-tehnologiyi-roblyat-kulturnu-spadshhynu-blyzhchoyu-do-lyudej/

УДК 614.842

ЗАХОДИ БЕЗПЕКИ ПОЖЕЖНО-РЯТУВАЛЬНОЇ ТЕХНІКИ НА ПРИФРОНТОВИХ ТЕРИТОРІЯХ В УМОВАХ ВІЙНИ

Юрій ПАНЧИШИН
Львівський державний університет безпеки життєдіяльності

Анотація. *Під час виконання завдань за призначенням з зоні ведення бойових дії, а саме на прифронтових територіях України, особовий склад пожежно-рятувальних підрозділів постійно перебуває в зоні надзвичайно підвищеної небезпеки. Відповідно, додатковий захист у вигляді захисного контуру та засобів радіоелектронної боротьби значною мірою підвищує ступінь захисту пожежно-рятувальної техніки та особового складу під час слідування та повернення з місця події пожежно-рятувального підрозділу.*

Ключові слова: *захисний контур, FPV дрон.*

Annotation. *While performing assigned tasks in the combat zone, namely in the front-line territories of Ukraine, the personnel of fire and rescue units are constantly in an extremely high-risk zone. Accordingly, additional protection in the form of a protective circuit and electronic warfare means significantly increases the degree of protection of fire and rescue equipment and personnel during the pursuit and return of the fire and rescue unit from the scene.*

Key words: *protective circuit, FPV drone*

Під час виконання завдань за призначенням з зоні ведення бойових дії, а саме на прифронтових територіях України [1], особовий склад пожежно-рятувальних підрозділів постійно перебуває в зоні надзвичайно підвищеної небезпеки. Відповідно, додатковий захист у вигляді захисного контуру та засобів радіоелектронної боротьби (далі - РЕБ) значною мірою підвищує ступінь захисту пожежно-рятувальної техніки та особового складу під час слідування та повернення з місця події пожежно-рятувального підрозділу [2]. Захисний сітковий контур зображено на рис.1, даний засіб підвищує ступінь захисту для техніки, а найголовніше для особового складу від прямого попадання FPV дрона.

Рисунок 1 – Захисний сітковий контур на автоцистерні.

Також, слід взяти до уваги, що пожежно-рятувальна техніка на прифронтових територіях комплектується системою РЕБ, але від FPV дрона на оптоволокні система РЕБ не працює, як зображено на рис.2.

Рисунок 2 – Автоцистерна після ураження FPV дрона на оптоволкні.

Отже, додатковий захист пожежно-рятувальної техніки у вигляді сіткового контуру значною мірою підвищує ступінь захисту для особового складу пожежно-рятувальних підрозділів.

Література

1. Наказ ДСНС України № 375 від 02.04.2024 «Рекомендації про особливості виконання органами управління та підрозділами ДСНС завдань за призначенням у населених пунктах і на територіях під час збройної агресії». Режим доступу: https://dsns.gov.ua/upload/ 2/0/8/0/8/1/6/ rekom.pdf

2. Наказ МВС України від 26.04.2018 № 340 «Про затвердження Статуту дій у надзви-чайних ситуаціях органів управління та підрозділів Оперативно-рятувальної служби цивіль-ного захисту та Статуту дій органів управління та підрозділів Оперативно-рятувальної слу-жби цивільного захисту під час гасіння пожеж». Режим доступу: https://zakononline.com.ua/ documents/show/373496___373561

УДК 004

КРИТЕРІЇ ВИБОРУ ОПЕРАЦІЙНОЇ СИСТЕМИ РЕАЛЬНОГО ЧАСУ ДЛЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ АВТОПІЛОТА БЕЗПІЛОТНОГО ПОВІТРЯНОГО СУДНА

Петросян А.Р., Хоменко Д.П.
Державний університет "Житомирська політехніка"

***Анотація**. В роботі аналізуються критерії вибору операційної системи реального часу для автопілота безпілотних повітряних суден, порівнюються популярні операційні системи реального часу, оцінюється їх детермінованість, затримки та вплив апаратних і програмних факторів, визначаючи доцільність застосування систем жорсткого реального часу для забезпечення стабільного і безпечного польоту та підкреслює значення якісного аналізу планувальника, переривань і коливань затримок часу.*

***Ключові слова:** операційна система реального часу, RTOS, автопілот БПС, UAV, детермінованість.*

***Abstract.** The paper analyzes the criteria for selecting a real-time operating system for the autopilot of unmanned aerial vehicles, compares popular real-time operating systems, evaluates their determinism, delays, and the impact of hardware and software factors, determining the feasibility of using hard real-time systems to ensure stable and safe flight, and emphasizes the importance of a qualitative analysis of the scheduler, interrupts, and time delay fluctuations.*

***Key words:** real-time operating system, RTOS, UAV autopilot, determinism.*

Забезпечення стабільного та безпечного польоту безпілотних повітряних суден (БПС) критично залежить від виконання алгоритмів управління в строго задані часові рамки. Дане завдання покладається на операційну систему реального часу (ОСРЧ), яка виступає фундаментом програмної архітектури автопілота. У зв'язку з цим завдання вибору ОСРЧ, яка відповідає вимогам детермінованості, надійності та продуктивності, стає одним з першочергових при проектуванні систем управління БПС.

ОСРЧ класифікуються за рядом ознак, таких як архітектура ядра, стратегія планування завдань, тип ліцензії та ресурсоємність. Однак ключовим для критичних застосувань є критерій тимчасової передбачуваності, відповідно до якого виділяють три основні класи ОСРЧ:

- системи жорсткого реального часу. Недотримання часових обмежень вважається критичною відмовою і може призвести до катастрофічних наслідків;
- системи стійкого реального часу. У даних операційних системах поодинокі порушення часових обмежень не є фатальними і не мають критичного впливу на функціонування;

- системи м'якого реального часу. Вони застосовується до вбудованих систем, де недотримання визначених часових обмежень не суттєво вплине на пов'язані процеси та загальну роботу системи.

У контексті розробки програмного забезпечення автопілота БПС, де порушення тимчасових обмежень у контурах стабілізації та навігації є неприпустимим [1, 2], домінуючим фактором є застосування операційної системи жорсткого реального часу. Її ключова перевага – забезпечення детермінованої реакції на події, що є запорукою стійкості та безпеки польоту.

У статті [3] представлені кількісні та якісні результати, отримані в результаті аналізу операційних систем реального часу. Досліджувалися системи Windows CE, QNX Neutrino, VxWorks, Linux і RTAI-Linux, які широко використовуються в промислових і академічних середовищах. Оцінки включають найгірші показники часу відгуку, затримка переривань, коливання затримки. Вони підкреслюють, що достовірно виміряти параметри можна тільки за допомогою зовнішнього обладнання – це генератор і осцилограф.

У роботі [4] досліджується явище коливання затримок часу в системах реального часу, що виникає як через апаратні фактори: блокування шини, кешу, конвеєрів, так і через програмні причини: блокування ресурсів, виконання критичних секцій, відключення переривання. Мета дослідження – кількісно виміряти коливання затримок часу на процесорах загального призначення з використанням розширень для операційних систем. Проведено аналіз його впливу на роботу крокових двигунів, а також запропоновано способи зменьшення його впливу на роботу системи.

У роботі [5] проводиться якісне та кількісне порівняння двох широко використовуваних операційних систем реального часу: комерційної µC/OS-III та відкритої FreeRTOS. За допомогою набору тестів автори оцінюють такі параметри, як: затримки обробки переривань, перемикання завдань, роботи з семафорами та мьютексами. Результати показують, що комерційна µC/OS-III не має значної переваги перед FreeRTOS, хоча вона демонструє кращі середні показники в деяких тестах, проте її поведінка менш передбачувана через сильний вплив обробки системних тіків. FreeRTOS поводиться стабільніше, але має деякі проблеми з динамічним управлінням пам'яттю.

Вибір ОСРЧ для програмного забезпечення автопілота БПС, визначається низкою критично важливих факторів. Апаратна платформа характеризується суворими обмеженнями щодо енергоспоживання, обсягу пам'яті та обчислювальної потужності, що виключає застосування ресурсоємних універсальних операційних систем. Ключовими завданнями автопілота є виконання високочастотних керуючих циклів з детермінованими часовими інтервалами, обробка даних з датчиків (акселерометр, гіроскоп, GPS, барометр тощо) з мінімальною затримкою та забезпечення своєчасної реакції на зовнішні впливи. Як показав аналіз, для їх реалізації ОСРЧ по-

винна мати передбачуваний планувальник, мінімальні коливання затримок часу і високу швидкість обробки переривань.

До найбільш поширених відкритих ОСРЧ можна віднести: FreeRTOS, ThreadX, Nuttx, Zephyr. Перші дві відносяться до легких RTOS, а останні дві до повноцінних RTOS з необхідними в більшості випадків модулями. Однак в документації FreeRTOS і ThreadX чітко вказано, що ядро використовує алгоритми, які є детермінованими, тобто час обробки не залежить від кількості виконуваних завдань. Застосування інших RTOS вимагає в деяких випадках оцінки детермінізму самостійно, як зазначено в [3]. Також аналыз показав, контекст переключення задач в одній ОСРЧ может бути різним у зв'язку з апаратними факторами, так і через програмні причини.

Висновки. Проведений аналіз показав, що для програмного забезпечення автопілота БПС критичними є детермінованість, мінімальні коливання затримок і висока швидкість обробки переривань. Системи жорсткого реального часу є найбільш придатними для таких задач, тоді як вибір конкретної ОСРЧ має враховувати апаратні обмеження, архітектуру планувальника та передбачуваність її поведінки в реальних умовах експлуатації.

Література

1. Arsen Petrosian, Ruslan Petrosian, Oleksandra Svintsytska. Test platform for Simulation-In-Hardware of unmanned aerial vehicle on-board computer. Proceedings of the 4rd Edge Computing Workshop. 2024. Vol.3666 . pp. 76-84. URL: https://ceur-ws.org/Vol-3666/paper12.pdf.

2. Петросян А.Р. Організація тестування програмного забезпечення бортового комп'ютера безпілотного повітряного судна. Вчені записки Таврійського національного університету імені В.І. Вернадського. Серія: Технічні науки. 2023. Том 34 (73) №6. С. 127-131. URL: https://doi.org/10.32782/2663-5941/2023.6/19.

3. Aroca R. V., Caurin, G. A real time operating systems (RTOS) comparison. In Workshop de Sistemas Operacionais (WSO). 2009. pp. 2441-2452. URL: https://www.semanticscholar.org/paper/A-Real-Time-Operating-Systems-(-RTOS-)-Comparison-Aroca-Caurin/3dc51976f8fb9408f5c991d457fa27f7b5adb737.

4. Proctor F. M., Shackleford W. P. Real-time operating system timing jitter and its impact on motor control. Intelligent Systems and Advanced Manufacturing, Boston, MA / ed. by P. E. Orban. 2001. URL: https://doi.org/10.1117/12.452653.

5. Behaviour and performance comparison between FreeRTOS and µC/OS-III / L. Peng et al. International Journal of Embedded Systems. 2016. Vol. 8, no. 4. P. 300. URL: https://doi.org/10.1504/ijes.2016.077774.

УДК 004

РОЗРОБКА КОНЦЕПТУАЛЬНОГО ПРОЄКТУ ІНФОРМАЦІЙНОЇ СИСТЕМИ ДЛЯ АВТОМАТИЧНОГО АНАЛІЗУ НАСТРОЇВ У СОЦІАЛЬНИХ МЕРЕЖАХ ДЛЯ ОЦІНКИ РЕПУТАЦІЇ БРЕНДУ

Плюгіна К.А.
Національний університет «Одеська політехніка»

Анотація. *Анотація. Розроблено концептуальний проєкт системи моніторингу бренду. Описано повний цикл обробки даних: від збору через API Twitter до візуалізації у Streamlit. Обґрунтовано використання нейромережі BERT для високоточного аналізу тональності тексту та виявлення прихованих патернів у відгуках користувачів..*
Ключові слова: *аналіз тональності, репутація бренду, BERT, NLP, візуалізація даних.*

Abstract. *A conceptual project of a brand monitoring system is developed. The full data processing cycle is described: from collection via Twitter API to visualization in Streamlit. The use of the BERT neural network for high-precision sentiment analysis and detection of hidden patterns in user reviews is justified. Keywords: sentiment analysis, brand reputation, BERT, NLP, data visualization..*
Key words*: sentiment analysis, brand reputation, BERT, NLP, data visualization.*

У сучасному цифровому просторі репутація бренду є одним із найважливіших нематеріальних активів компанії. Соціальні мережі перетворилися на глобальну книгу скарг та пропозицій, де користувачі щохвилини генерують тисячі повідомлень. Для бізнесу критично важливо не просто фіксувати згадки про себе, а розуміти емоційне забарвлення цих згадок. Оскільки обсяги інформації перевищують людські можливості обробки, виникає потреба у створенні автоматизованих інформаційних систем, здатних аналізувати природну мову. Метою роботи є розробка концептуального проєкту такої системи, яка поєднує швидкість обробки даних із глибиною семантичного аналізу [1].

Концептуальна модель пропонованої системи базується на модульній архітектурі, що забезпечує гнучкість та можливість масштабування. Процес функціонування системи можна розділити на чотири ключові етапи: збір даних (Data Ingestion), попередня обробка (Preprocessing), інтелектуальний аналіз (AI Core) та візуалізація результатів (Presentation Layer).

На етапі збору даних система взаємодіє із зовнішнім середовищем через API соціальних мереж (зокрема Twitter/X). Головним викликом тут є отримання релевантної інформації серед «шуму». Для цього в проєкті передбачено використання складних пошукових запитів, які фільтрують повідомлення не лише за хештегами бренду, але й за геолокацією та мовою користувача. Отримані дані зберігаються у структурованому вигляді

(DataFrame) за допомогою бібліотеки Pandas, що дозволяє ефективно маніпулювати великими масивами текстової інформації.

Етап попередньої обробки є критичним для коректної роботи алгоритмів машинного навчання. «Сирі» тексти з соціальних мереж насичені сленгом, емодзі, помилками та скороченнями. Система автоматично очищує текст від посилань, службових символів та стоп-слів, приводить слова до їхньої початкової форми (лематизація). Це дозволяє зменшити розмірність даних без втрати змісту.

Серцем системи є модуль аналізу тональності, побудований на базі архітектури трансформерів — моделі BERT (Bidirectional Encoder Representations from Transformers). На відміну від застарілих методів, які аналізують слова окремо, BERT розглядає все речення цілком, враховуючи контекст кожного слова в обох напрямках. Це дає змогу системі коректно інтерпретувати складні лінгвістичні конструкції, наприклад, відрізняти фразу «Це просто бомба!» (позитивний відгук) від «Сервіс — повний жах» (негативний), навіть якщо окремі слова можуть мати різне забарвлення. Використання попередньо навченої моделі з подальшим донавчанням (fine-tuning) на специфічному датасеті відгуків забезпечує високу точність класифікації [2].

Завершальним етапом є презентація аналітики кінцевому користувачеві. Для цього в проєкті використано фреймворк Streamlit, який дозволяє створювати інтерактивні веб-додатки. Користувач отримує доступ до дашборду, де відображається динаміка настроїв у часі, хмара слів (найчастіші теми обговорення) та розподіл відгуків за категоріями. Така візуалізація дозволяє менеджерам миттєво оцінювати «здоров'я» бренду та приймати обґрунтовані управлінські рішення [3].

Отже, запропонований концептуальний проєкт демонструє, як поєднання сучасних Python-бібліотек та нейромережевих технологій дозволяє створити ефективний інструмент для захисту та управління репутацією бізнесу.

Література

1. Котлер Ф., Картаджайя Г., Сетьяван А. Маркетинг 4.0. Від традиційного до цифрового. Київ : КМ-БУКС, 2018. 208 с.

2. Rogers A., Kovaleva O., Rumshisky A. A Primer in BERTology: What We Know About How BERT Works. *Transactions of the Association for Computational Linguistics.* 2020. Vol. 8. P. 842–866.

3. McKinney W. Pandas: Powerful Python Data Analysis Toolkit [Electronic resource]. URL: https://pandas.pydata.org/pandas-docs/stable/ (дата звернення: 20.02.2024).

УДК 004.7

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ОСВІТІ: ВИКОРИСТАННЯ ПРОГРАМИ MULTISIM

Назарій ПОНИЧ, Юрій БОРЗОВ
Львівський державний університет безпеки життєдіяльності

Анотація: У тезах розглянуто роль інформаційних технологій в освіті та особливості використання застосування програмного комплексу комп'ютерного моделювання електронних схем та пристроїв Multisim компанії розробника National Instruments як сучасного засобу моделювання та дослідження електронних схем.
Ключові слова: *інформаційні технології, Multisim, освіта, моделювання.*

Сьогодні інформаційні технології розвиваються дуже швидко і суттєво впливають на наше життя, зокрема й на освіту. Завдяки цифровим інструментам навчання стає цікавішим, зручнішим і ближчим до реальних ситуацій. Одним з таких інструментів, який широко використовують у технічних спеціальностях, є програмний комплекс комп'ютерного моделювання електронних схем та пристроїв Multisim. Вона допомагає моделювати електронні схеми і проводити практичні роботи просто на комп'ютері.

Multisim створила компанія National Instruments, яка випустила безкоштовну версію програми версія NI Multisim Analog Devices Edition, яка має лише обмеження по застосуванню кількості елементів в одній схемі. Програма дає змогу будувати електронні схеми, перевіряти їх роботу і вдосконалювати без використання справжніх деталей. Інтерфейс у Multisim простий і зрозумілий, тому з нею легко працювати навіть тим, хто тільки починає вивчати електроніку. Саме тому її часто застосовують у коледжах та університетах під час лабораторних занять.

Основне призначення Multisim полягає у створенні віртуальної лабораторії, де можна точно моделювати роботу електронних схем. У програмі є велика колекція компонентів, які повторюють справжні радіоелементи, а також прилади для вимірювання, схожі на ті, що використовуються в реальних лабораторіях. Завдяки цьому студенти можуть отримувати практичний досвід навіть тоді, коли у навчальному закладі немає дорогого обладнання.

Використання Multisim у навчальному процесі має багато переваг. По перше, це повністю безпечно, адже жодні деталі не можуть згоріти, а обладнання не може вийти з ладу. По друге, програма навчає аналізувати і проєктувати схеми. Студенти можуть досліджувати роботу електронних схем, аналізувати сигнали та проводити експерименти, які в реальних умовах вимагали б багато часу і значних витрат, вносити зміни, спостерігати результати і порівнювати різні варіанти. По третє, робота з Multisim допомагає розвивати важливі навички, які потрібні майбутнім фахівцям у технічних галузях. Для майбутніх інженерів та техніків Multisim є дуже цінним інструметом.

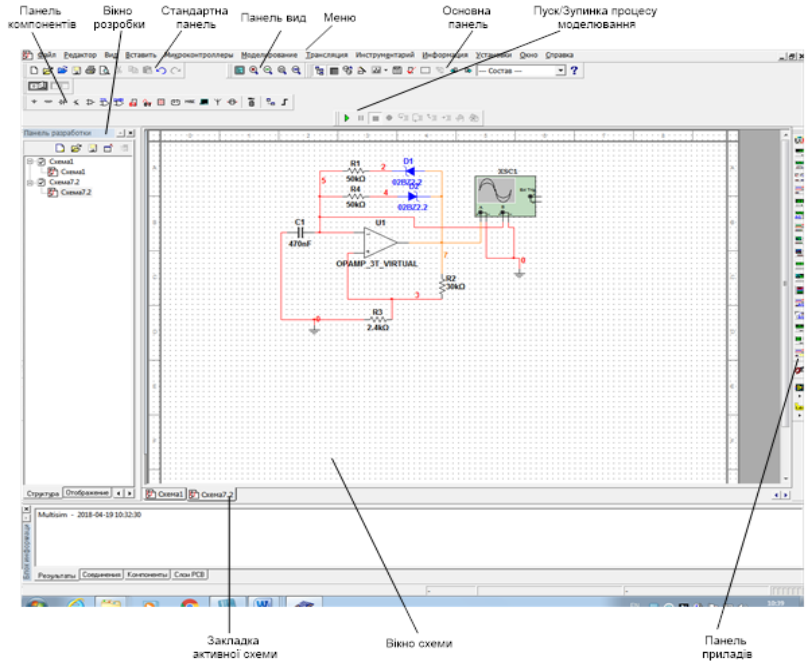

Рисунок 1 – Середовище Multisim

Отже, програмний комплекс комп'ютерного моделювання електронних схем та пристроїв Multisim відіграє важливу роль у сучасній технічній освіті. Використання цієї програми підвищує якість підготовки студентів, розвиває їх професійні вміння і забезпечує доступ до сучасних методів навчання, що відповідають вимогам сьогоднішнього ринку праці.

Література

1. National Instruments**.** *Multisim User Manual.* — Austin: National Instruments, 2020.

2. Гуменюк А. Д., Ковальчук І. П. *Комп'ютерне моделювання електронних схем: Навчальний посібник.* — Київ: Кондор, 2019.

3. Бобров В. С. *Основи електроніки та моделювання.* — Київ: Ліра-К, 2020.

4. Дейнега І. М. *Інформаційні технології в освіті: сучасні підходи та інтеграція в навчальний процес.* — Львів: Сполом, 2021.

5. Obeidat R., McDonald S. "Using Circuit Simulation Software for Enhancing Engineering Education." *International Journal of Engineering Education*, 2020.

УДК 614.8

ОСОБЛИВОСТІ ВИКОРИСТАННЯ ПОЖЕЖНИХ РОБОТИЗОВАНИХ КОМПЛЕКСІВ ДЛЯ ПРОВЕДЕННЯ АВАРІЙНО-РЯТУВАЛЬНИХ РОБІТ

Марія ПОПЧУК, Мар'ян ЛАВРІВСЬКИЙ
Львівський державний університет безпеки життєдіяльності

Анотація. У роботі досліджено переваги та недоліки використання роботизованих комплексів під час проведення аварійно-рятувальних робіт в зонах підвищеної небезпеки. Також розглядаються роботи пожежогасіння, які отримала наша держава від міжнародних партнерів.

Ключові слова: роботизованні комплекси, аварійно-рятувальні роботи, гасіння.

Abstract. The paper examines the advantages and disadvantages of using robotic systems during emergency and rescue operations in high-risk areas. It also examines firefighting operations that our state has received from international partners.

Keywords: robotic systems, emergency and rescue operations, extinguishing.

Однією з основних проблем під час війни, яка розгорнулася на території нашої держави, є військові дії ворога, які спрямовані не лише на об'єкти, які є важливими для нормального функціонування країни, а й на цивільну інфраструктуру. Істотне те, що внаслідок російських ударів, зазвичай, виникає пожежа, яку небезпечно ліквідовувати під час загрози ракетних обстрілів. Рятувальники стикаються з проблемою можливості повторних атак, що унеможливлює швидке реагування на надзвичайні ситуації.

В реаліях сьогодення наша держава отримує підтримку та допомогу від міжнародних партнерів. Одним з прогресивних вирішень проблеми, щодо гасіння пожеж в складних для рятувальників умовах, є роботизовані комплекси. Варто зазначити, що Державна служба України з надзвичайних ситуацій активно використовує новітнє обладнання у різних напрямках реагування на надзвичайні ситуації у зонах підвищеної небезпеки. Багатоцільові роботи мають широкий спектр можливостей, зокрема: гасіння пожеж різної складності, проведення гуманітарного розмінування, робота під час хімічного забруднення, евакуація потерпілих з небезпечної зони тощо.

Хорошими прикладами роботів пожежогасіння є Magirus Wolf R1 (рис.1) та Alpha Wolf R1. Тактичний робот пожежогасіння складається з базової рухомої платформи на гусеничному шасі із гумовим покриттям. Тяговий двигун забезпечує пересування по рівній місцевості без навантаження до 10-15 км/год та зусиллям тяги до 4 т. Всі вузли та частини тактичного робота пожежогасіння мають ступінь вологозахисту IP65, що дозво-

ляє йому проводити роботи не зважаючи на вплив води на електричні комплектуючі. На базову рухому платформу встановлено динамічні, статичні та баштові камери із системою стисненого повітря для очищення камер, які транслюють обстановку навколо робота та передають на планшет. На корпусі тактичного робота пожежогасіння знаходяться два екрана поточного стану робота, які знаходяться позаду біля системи зв'язку, за нормальної експлуатації вони показують логотип та стан заряду акумуляторної батареї, а за умови активації певних опцій показує знак уваги. Керування здійснюється за допомогою дистанційного радіообміну через мобільну панель керування із встановленим планшетом, дальність прийому якого становить 150 метрів. Тактичний робот пожежогасіння має базову опцію системи подачі води або піни із максимальною витратою 2 000 л/хв при тиску 10 бар, дальність подачі струменя води складає до 65 метрів, а для піни – 45 метрів. [1,2]

Рисунок 1 – Роботизовані комплекси Magirus Wolf R1

Ключові переваги комплексу:

- робот витривалий до високих температур та може безперервно працювати протягом 12 годин;
- має високу прохідність для переміщення в складних умовах місцевості (завали, нестійкі конструкції, затоплені території);
- незамінний інструмент для ліквідації найскладніших НС. Він призначений для гасіння пожеж у важкодоступних місцях (склади, підземні паркінги, промислові об'єкти, тунелі), а також при витоках газу, хімічному чи біологічному зараженні;
- окрім гасіння, робот може транспортувати необхідне обладнання та евакуювати потерпілих, що мінімізує ризики для рятувальників.[3]

Серед недоліків та обмежень:

- більшість роботизованих комплексів потребують постійного живлення, що обмежує їх автономність та ефективність під час тривалих операцій;
- виготовлення та обслуговування потребує значних фінансових вкладень, до того ж існує загроза знищення через можливі повторні удари на місцях виникнення надзвичайних ситуацій;
- роботи не завжди здатні адаптуватися до певних змін перебігу ситуації без допомоги оператора.

Підсумовуючи вищесказане, можемо впевнитися в важливості та ефективності використання роботизованих комплексів під час ліквідації наслідків ракетних обстрілів, зокрема гасіння пожеж. Сьогодні наша держава має міжнародних партнерів, які допомагають зміцнювати український сектор робототехніки. Завдяки даній співпраці рятувальники отримують новітнє обладнання, яке дозволяє ефективно проводити рятувальні операції у зонах підвищеної небезпеки.

Література

1. Інструкція з експлуатації. Тактичний робот для місій MAGIRUS WOLF R1. URL: https://cv.dsns.gov.ua/upload/2/3/7/6/4/4/0/0-2-magirus-wolf-r1-ukr-ins-zag.pdf

2. Alpha Wolf R1 - Alpha Wolf. Alpha Wolf . URL: https://www.alpha-wolf.de/en/alpha-wolf-r1/

3. Технології, що рятують рятувальників: У Тернополі представили французький роботизований комплекс «Colossus». ДСНС України. URL: https://tr.dsns.gov.ua/news/ostanni-novini/texnologiyi-shho-riatuiut-riatuvalnikiv-u-ternopoli-predstavili-francuzkii-robotizovanii-kompleks-colossus

УДК 004.8

ПОРІВНЯЛЬНИЙ АНАЛІЗ ОНЛАЙН-ІНСТРУМЕНТІВ ДЛЯ ПЕРЕВІРКИ ІНКЛЮЗИВНОСТІ ДРУКОВАНИХ ПЛАНІВ ЕВАКУАЦІЇ ПРИ ПОЖЕЖІ

Вікторія ПРИДАТКО, Наталія ЖЕЗЛО-ХЛЕВНА, Володимир ПИЛИПЕНКО
Львівський державний університет безпеки життєдіяльності

Проблема доступності інформаційних матеріалів для осіб з інвалідністю є однією з ключових у сфері сучасного інклюзивного дизайну, що безпосередньо стосується забезпечення безпеки. Особливої уваги потребує питання адаптації друкованих планів евакуації – графічних документів, що повинні не лише вірно передавати маршрути руху в безпечні зони, але й робити це у спосіб, який може бути сприйнятий людьми з порушенням зору, у тому числі й тими, хто має повну втрату зору.

В контексті глобальної практики інтеграції принципів універсального дизайну, а також відповідно до стандартів доступності WCAG (Web Content Accessibility Guidelines) та ISO 21542, дедалі більшої уваги набуває аналіз відповідності цих планів вимогам інклюзивності. Стандартні продукти для оцінювання доступності веб-контенту тепер застосовуються й до оцінювання графічних зображень, планів і схем. Однак використання таких інструментів для аналізу планів евакуації має свої особливості, пов'язані з поєднанням графічних елементів, схем, кольорових рішень, типографіки та інформаційної ієрархії.

Таким чином, виникає потреба у порівнянні ефективності онлайн-інструментів, які можуть бути застосовані до перевірки інклюзивності друкованих планів евакуації з урахуванням їхніх ключових графічних і текстових компонентів, орієнтованих на сприйняття людьми з порушеннями зору.

Метою цього дослідження є комплексне порівняння можливостей сучасних онлайн-інструментів перевірки доступності з акцентом на оцінювання інклюзивності друкованих планів евакуації при пожежі.

Для досягнення поставленої мети були визначені такі завдання:

- встановити основні вимоги інклюзивності до планів евакуації при пожежі;
- визначити набір доступних онлайн-інструментів для перевірки доступності контенту (графіки, тексту, кольорових гам);
- розробити алгоритм тестування планів евакуації у цих інструментах;
- провести порівняльний аналіз та узагальнити результати у вигляді таблиці;
- сформулювати практичні рекомендації для проєктувальників, розробників та експертів з інклюзивності.

Дослідження базується на методі адаптованих кейс-тестів, у яких за допомогою онлайн-інструментів було виконано аналіз серії стандартних

зразків друкованих планів евакуації, підготовлених згідно з типовими нормами пожежної безпеки, але з різними параметрами типографіки, схемним оформленням та колірними рішеннями.

План перевірки включав:

1. Автоматичний аналіз контрастності кольорів (тло/графіка/текст).
2. Перевірку читабельності шрифтів з урахуванням розмірів.
3. Аналіз вербалізації.
4. Перевірку відповідності логіки розміщення інформації.
5. Визначення потенційних бар'єрів сприйняття для осіб зі слабким зором.

Для оцінювання було використано набір з 12 планів евакуації, які були умовно розподілені на 4 групи за ключовими ознаками.

Група A: стандартниі варіанти без адаптації.

Група B: адаптовані контрастом, але з малим шрифтом.

Група C: велика кількість графіки без пояснень.

Група D: адаптовані під рекомендації WCAG .

У дослідженні були використані такі веб-сервіси:

1. Contrast Checker — аналізатор фон/текст/графіка з розрахунком рівнів контрасту.
2. Accessibility Insights — комплексний інструмент перевірки WCAG відповідності.
3. WebAIM Color Contrast Checker — веб-інструмент для детального аналізу колірних рішень.
4. Tota11y — візуальний інструмент оцінки доступності графіки.
5. axe Accessibility Scanner — розширення для автоматичного пошуку порушень доступності.

Ці інструменти були обрані за критеріями:

- відкритий або безкоштовний доступ;
- можливість оцінки графіки та кольору;
- підтримка стандартів WCAG;
- функція виявлення бар'єрів доступності візуального контенту.

Аналіз показав, що жоден з онлайн-інструментів повністю не відповідає всім вимогам інклюзивної оцінки друкованих планів евакуації.

Зокрема, Contrast Checker та WebAIM Color Contrast є потужними для оцінювання кольорових рішень, але не дають комплексної оцінки схем і читабельності. Accessibility Insights та axe Scanner мають найширший набір перевірок, але їхнє застосування до графічної інформації потребує адаптації, оскільки вони розроблені в першу чергу для веб-контенту. Tota11y добре ідентифікує потенційні бар'єри графічної інформації, але не забезпечує формальних рекомендацій щодо адаптації.

Усі інструменти є корисними, але для повної оцінки друкованих планів евакуації потрібен комбінований підхід, який поєднує кілька профільних сервісів разом із фаховою експертизою з інклюзивного дизайну.

Результаи аналізу наведені у таблиці 1.

Таблиця 1 – Результати порівняльного аналізу онлайн-інструментів

Параметр / Інструмент	Contrast Checker	Accessibility Insights	WebAIM Color Contrast	Tota11y	axe Scanner
Аналіз контрасту	Так	Так	Так	Частково	Так
Оцінка читабельності	Ні	Так	Частково	Частково	Так
WCAG-валідація	Ні	Так	Ні	Частково	Так
Аналіз графічних елементів	Ні	Частково	Ні	Так	Частково
Виявлення бар'єрів	Обмежено	Так	Обмежено	Частково	Так
Коментарі щодо адаптації	Ні	Так	Ні	Частково	Так
Зручність використання	Висока	Середня	Висока	Середня	Складна

За результатами виконаного аналізу було сформовано низку рекомендацій для розробників планів евакуації при пожежі:

1. За можливості використовувати комбінацію інструментів для аналізу як кольору, так і семантики.

2. Адаптувати інструменти під аналіз графічних елементів поза межами стандартного DOM-контенту.

3. Формувати альтернативні текстові описи (alt-теги) для ключових частин планів.

4. Проводити тестування з фактичними користувачами — слабозорими або незрячими особами.

5. Розробляти спеціалізовані модулі або плагіни для автоматичного аналізу планів евакуації за параметрами інклюзивності.

Проведений порівняльний аналіз виявив, що навні онлайн-інструменти, попри свою корисність у сфері доступності загального веб-контенту, не забезпечують повної оцінки інклюзивності графічних планів евакуації при пожежі з урахуванням потреб людей з порушенням зору.

Результати дослідження підтверджують необхідність розвитку спеціалізованих інструментів та методик, що поєднують перевірку колірних рішень, читабельності, структурної логіки та контекстної інформативності планів евакуації. Використання комбінованого підходу дає змогу підвищити рівень безпеки та доступності для максимально широкого кола користувачів, що узгоджується з принципами універсального дизайну.

Література

1. Пилипенко В. М., Хлевной О. В., Жезло-Хлевна Н. В., Назар Ю. С., Брошко В. І. Інноваційні підходи до створення інклюзивних планів евакуації при пожежі. Вісник Львівського державного університету безпеки життєдіяльності. Львів, 2025. № 32. С. 41-51.

УДК 004.738.5:004.722

МОДЕЛЬ АРХІТЕКТУРИ ІНТЕРНЕТУ РЕЧЕЙ З ДИНАМІЧНИМ ВИБОРОМ КАНАЛІВ ЗВ'ЯЗКУ ДЛЯ СИСТЕМ МОНІТОРИНГУ

Вадим ПТАШНИК, Юрій МИХАЙЛЮК, Назар СИВУЛЯК
Львівський національний університет ветеринарної медицини та біотехнологій імені С. З. Ґжицького, м. Дубляни

У роботі розглянуто багаторівневу архітектуру Інтернету речей та підхід до адаптивної селекції каналів зв'язку в IoT-системах. Описано роль сенсорного, мережевого, крайового та хмарного рівнів, проаналізовано вплив динамічного вибору каналу на надійність, енергоефективність і масштабованість систем моніторингу.

Ключові слова: *Інтернет речей, архітектура IoT, адаптивна селекція каналів, системи моніторингу.*

The paper examines a multilayer Internet of Things architecture and an approach to adaptive channel selection in IoT systems. It explains the role of sensor, network, edge and cloud levels and analyses how dynamic channel choice affects reliability, energy efficiency and scalability of monitoring solutions.

Keywords: *Internet of Things, IoT architecture, adaptive channel selection, monitoring systems.*

Розвиток технологій Інтернету речей призвів до стрімкого зростання кількості підключених до мережі пристроїв та переходу від «Інтернету людей» до «Інтернету речей», де ключову роль відіграють інтелектуальні об'єкти, здатні самостійно збирати, передавати та аналізувати дані. У загальному випадку IoT розглядається як сукупність різнорідних пристроїв, датчиків і контролерів, об'єднаних у єдину інфраструктуру за допомогою різних технологій зв'язку, але з використанням уніфікованого протоколу доступу до глобальної мережі. Така концепція забезпечує перехід до «підключеного життя», коли побутові, промислові, міські та медичні системи інтегруються в єдиний цифровий простір і формують нові моделі взаємодії між людиною, технікою та середовищем.

Ключовою передумовою ефективної роботи Інтернету речей є продумана багаторівнева архітектура. Типово вона включає сенсорний, мережевий, крайовий та хмарний рівні, які разом утворюють завершений цикл оброблення даних: від вимірювання фізичних величин до отримання аналітичних висновків та формування керуючих дій. На нижньому рівні розташовані «речі» – датчики, виконавчі механізми та контролери, які перетворюють параметри середовища на цифрові сигнали, здійснюють попередню фільтрацію та можуть автономно реагувати на зміни умов. Саме на цьому

етапі формується базова інфраструктура IoT-системи, від точності та стабільності роботи якої залежить достовірність усіх подальших розрахунків.

На наступному етапі до оброблення даних залучаються шлюзи та системи збору інформації, що знаходяться на межі світів OT та IT. Вони виконують роль посередників між великою кількістю сенсорних вузлів і хмарною або серверною інфраструктурою, перетворюючи, агрегуючи та попередньо аналізуючи вхідні потоки. Важливою функцією шлюзів є не лише маршрутизація даних, а й їх відбір, стиснення та захист. Завдяки цьому зменшується навантаження на мережу, скорочуються затримки передачі та підвищується загальний рівень безпеки системи, оскільки саме на цьому рівні можна реалізувати механізми шифрування та контролю доступу до критичних ресурсів.

Подальший розвиток архітектури Інтернету речей пов'язаний із широким упровадженням крайових обчислень. Крайова аналітика дозволяє переносити частину обчислювального навантаження ближче до джерела даних, що особливо важливо для систем реального часу та промислових додатків, де навіть незначні затримки можуть бути критичними. Крайові пристрої аналізують потоки телеметрії локально, приймають оперативні рішення щодо керування обладнанням, а в хмару передають лише агреговані або подієві дані. Це підвищує стійкість системи до збоїв мережі, зменшує обсяги переданої інформації та сприяє економії енергоресурсів.

Хмарна платформа або центр обробки даних завершує архітектуру IoT-системи, виконуючи роль «мозку», в якому накопичуються, зберігаються та глибоко аналізуються великі масиви інформації. У хмарі реалізуються сервіси довгострокової аналітики, прогнозування, візуалізації, а також механізми машинного навчання, що дозволяють виявляти приховані залежності, типові сценарії поведінки системи та аномальні ситуації. Завдяки інтеграції з прикладними сервісами й веб- або мобільними інтерфейсами користувачі отримують змогу оперативно оцінювати стан об'єктів, налаштовувати алгоритми реагування та приймати обґрунтовані управлінські рішення.

Практичне значення такої багаторівневої архітектури добре ілюструє приклад медичної системи моніторингу стану здоров'я пацієнтів похилого віку. У подібних рішеннях на фізичному рівні використовуються датчики життєвих показників та параметрів довкілля, що забезпечує безперервний контроль критичних параметрів організму та умов перебування. Комунікаційний рівень відповідає за надійну передачу даних до хмарних сервісів, де відбувається аналіз, виявлення відхилень, формування попереджень і рекомендацій для лікарів або родичів. Прикладний рівень забезпечує зручний доступ до інформації для різних типів користувачів через спеціалізовані інтерфейси, підтримуючи при цьому високі вимоги до безпеки та конфіденційності медичних даних.

Окремим напрямом підвищення ефективності роботи IoT-систем є адаптивна селекція каналів зв'язку. На відміну від статичних схем, де параметри комунікації обираються один раз і залишаються фіксованими, адаптивний підхід передбачає безперервний аналіз стану мережі, рівня завад, параметрів сигналу, затримок та енергоспоживання. На основі цих показників система автоматично обирає оптимальний канал або навіть технологію зв'язку – від Wi-Fi та Bluetooth до LoRaWAN, NB-IoT чи інших LPWAN-рішень. Це дозволяє забезпечити стабільний зв'язок у динамічних умовах, мінімізувати втрати пакетів і зменшити кількість повторних передач.

Адаптивна селекція каналів набуває особливого значення для енергообмежених IoT-пристроїв, що живляться від батарей і мають працювати тривалий час без обслуговування. Динамічне налаштування параметрів зв'язку та вибір менш енергоємних режимів при сприятливих умовах дозволяє суттєво подовжити термін автономної роботи. Водночас у разі погіршення якості каналу система може переключитися на більш надійну, хоча й більш ресурсоємну технологію, забезпечивши цілісність і своєчасність передавання критичних даних. Таким чином, досягається баланс між якістю сервісу, енергоспоживанням і вартістю комунікаційних ресурсів.

З технічної точки зору механізми адаптивного вибору каналів можуть реалізовуватися на різних рівнях мережевої моделі. На фізичному рівні це коригування частоти, модуляції або потужності передавача; на канальному та мережевому рівнях — вибір альтернативних маршрутів або протоколів; на прикладному рівні — реалізація логіки прийняття рішень на основі даних, що надходять як від сенсорних вузлів, так і від хмарних сервісів аналітики. У сучасних системах усе частіше використовуються інтелектуальні методи, зокрема алгоритми машинного навчання, які здатні прогнозувати зміни стану каналу та завчасно ініціювати його перемикання.

У підсумку можна зазначити, що комплексний підхід до побудови архітектури Інтернету речей у поєднанні з адаптивною селекцією каналів зв'язку формує підґрунтя для створення стійких, масштабованих і економічно ефективних IoT-рішень. Чітке розмежування функцій між сенсорним, мережевим, крайовим та хмарним рівнями, а також впровадження гнучких механізмів керування передаванням даних дозволяють забезпечити необхідну надійність, безпеку й якість сервісу навіть в умовах швидкозмінного середовища та великої кількості підключених пристроїв. Саме такі підходи визначатимуть подальший розвиток Інтернету речей і його інтеграцію в ключові сфери діяльності людини — від охорони здоров'я та промисловості до міської інфраструктури та «розумного» довкілля.

УДК 532.5.6

МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ КОНЦЕНТРАЦІЇ ВУГЛЕКИСЛОГО ГАЗУ ДЛЯ УПРАВЛІННЯ СИСТЕМОЮ ПРИПЛИВНО-ВИТЯЖНОЇ ВЕНТИЛЯЦІЇ ПРИМІЩЕНЬ

Софія РЕВУЦЬКА, Тарас ГЕМБАРА
Львівський державний університет безпеки життєдіяльності, м. Львів

Анотація. Розроблена математична модель динаміки концентрації вуглекислого газу (CO_2) у закритому приміщенні з урахуванням неоднорідних джерел виділення. Модель враховує наявність постійних працівників та змінну кількість відвідувачів, чисельність яких описано періодичною (синусоїдальною) функцією часу та за статистичними законами. Для опису процесу масообміну використано рівняння балансу концентрації CO_2 з урахуванням припливу зовнішнього повітря та інтенсивності внутрішніх джерел та програмне забезпечення Scilab.

Ключові слова: математична модель, вуглекислий газ, статистичнні закони, Scilab програми.

Abstract. A mathematical model has been developed for the dynamics of carbon dioxide (CO_2) concentration in an enclosed space, taking into account non-uniform emission sources. The model accounts for the presence of permanent staff and a variable number of visitors, whose number is described both by a periodic (sinusoidal) function of time and by statistical laws. The mass transfer process is described using a CO_2 concentration balance equation that incorporates the supply of outdoor air and the intensity of internal sources, and is implemented in the Scilab software environment.

Keywords: *mathematical model, carbon dioxide, statistical laws, Scilab software.*

Концентрація вуглекислого газу (CO_2) у закритих приміщеннях є одним із основних інтегральних показників якості внутрішнього повітря. Перевищення допустимих значень концентрації CO_2 (близько 1000 ppm для тривалого перебування людей згідно з нормами вентиляції) призводить до погіршення самопочуття, зниження працездатності, появи головного болю та відчуття задухи [1-3]. Тому на етапі проєктування та експлуатації систем вентиляції важливо мати надійні інструменти для прогнозування динаміки концентрації CO_2. Особливо важливим є кількісний аналіз нестаціонарної концентрації CO_2 у захисних спорудах цивільного захисту, в яких під час військового військового стану є ризики порушень нормальної роботи припливно-витяжних систем вентиляції через припинення електропостачання, з іншого боку цілком автономні системи мають обмежений енергетичний ресурс.

Для математичного моделювання вмісту вуглекислого газу у приміщенні з припливно-витяжною вентиляційною системою використали метод усереднених параметрів мікроклімату у будь-якій точці приміщення [1]. Прийнявши, що $C = C(t)$ – концентрація CO_2 в 1 м^3 повітря в приміщенні в момент часу t, склали рівняння балансу, яке включає приплив CO_2 та його втрати за рахунок роботи вентиляційної системи за проміжок часу dt. Отже математична модель базується на диференціальному співвідношенні [2],, яке описує відносний приріст CO_2 протягом часу dt :

$$dC = \frac{n_0 V_1 + V_p C_2 - V_p C}{V} dt, \quad (1)$$

де n_0 –кількість людей, V_1 – об'єм CO_2, який видихає людина на м^3, C_2 - концентрація CO_2 на м^3 у повітрі, що надходить зовні, V_p – потужність вентиляційної системи, V – об'єм приміщення.Дослідили припливно - витяжну систему обмінної вентиляції в приміщенні 20м×10м висотою 3м, де перебувають 25людей (кількість людей не змінюється, що вважаємо стаціонарним режимом), з початковим вмістом CO_2 0,02 %. Кожна людина видихає 24 літри CO_2 за годину Вентиляційна система постачає по припливному каналу з зовнішнього середовища 15 м^3 чистого повітря з вмістом 0, 02 % CO_2 за хвилину (потужність системи по кожному каналу) і в такому ж об'ємі видаляє по витяжному. Співвідношення (1) зводиться до лінійного диференціального рівнянням з відповідними початковими умовами, розв'язавши яке, отримали його частковий розв'язок. В результаті чисельного експерименту отримали зростання вмісту CO_2 через 120 хв. – до 0,083%, а вихід на стаціонарний режим складає 240хв. на рівень 0,087%, а такий вміст вже порівняно не є задовільним. Тому встановили можливість збільшення потужності системи вдвічі, до 30 м^3 на хвилину за допомогою аналогічного обчислювального алгоритму. Отримали, що незважаючи на роботу вентиляторів, вміст CO_2 в приміщенні від умовного початку, через 15 хвилин зростає до 0,038%, 30 хв. – до 0,046%, 60 хв. – до 0,052%, 120 хв. – до 0,053% і далі практично не зростає, а таку якість повітря, наприклад в захисній споруді, можна вважати задовільною. Розглянули складніший випадок, якщо наявна кількість людей в приміщенні n змінюється з часом і є функцією $n=n(t)$, що відповідає нестаціонарному режиму роботи системи. На рис.1 представлено результати обчислень на основі створеного Scilab-коду. Для верифікації математичної моделі необхідно порівнювали результати розрахунків із експериментальними даними для тільки для сценаріїв А та В, похибка не перевищувала 10%. Для цього був використаний багатофункціональний прилад Xintest HT-2000, який поєднує функції детектора CO_2, термогігрометра та вбудованого логера Прилад має достатню точність через використання NDIR-сенсора, робота якого ґрунтується на вибірковому поглинанні інфрачервоного випромінювання молекулами CO_2 у вузькій спектральній області. Також проведені розрахунки (рис.1) для $n=n(t)$ періодичної (за законом синуса) сценарій С, та за статистичним законом (за Марковською моделлю). Порівняння результатів свідчить про важливість врахування нестаціонарного закону для $n(t)$.

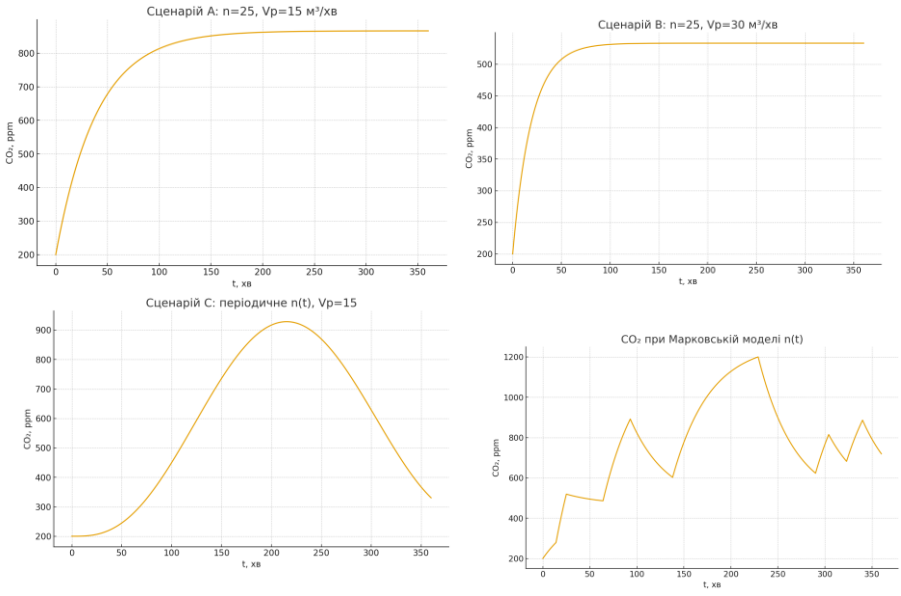

Рисунок 1 – Результати програмних розрахунків в середовищі Scilab за різними сценаріями.

Література

1. Гембара Т. В., Марич В. М. Диференціальне рівняння управління припливно – витяжною системою вентиляції за вмістом CO_2 у приміщенні. Зб. наук. праць IV Всеукраїнської науково–практичної конференції викладачів та фахівців–практиків «Охорона праці: освіта і практика» –Львів: ЛДУ БЖД, травень 2024, С.34-35.

2. Гембара Т. В., Марич В. М., Трусевич О.М. Математичне моделювання роботи системи припливно – витяжної вентиляції в стаціонарному та нестаціонарному режимах. Зб. наук. праць V Всеукраїнської науково–практичної конференції викладачів та фахівців–практикі.в «Охорона праці: освіта і практика» –Львів: ЛДУ БЖД, травень 2025, С.79-81.

3. Persily A.K., de Jonge L. Carbon dioxide generation rates for building occupants // Indoor Air. – 2017. – 27(5). – P. 868–879.

УДК 004.891.3

АДАПТИВНЕ УПРАВЛІННЯ СПОВІЩЕННЯМИ З ВИКОРИСТАННЯМ МЕТОДІВ ШТУЧНОГО ІНТЕЛЕКТУ

Роман РИЗІК, Романна МАЛЕЦЬ
Львівського національного університету імені Івана Франка, Львів

Анотація. *Система адаптивного управління сповіщеннями використовує методи штучного інтелекту для класифікації та пріоритизації помилок у IT-сервісах. Завдяки NLP і асинхронній обробці вона зменшує інформаційне навантаження, усуває втому від сповіщень та забезпечує оперативне реагування на критичні події.*

Ключові слова: *автоматизація, сповіщення, класифікація, штучний інтелект, інформаційні системи*

Abstract. *The adaptive notification management system uses artificial intelligence methods to classify and prioritize errors in IT services. Thanks to NLP and asynchronous processing, it reduces information overload, eliminates notification fatigue, and ensures rapid response to critical events.*

Keywords: *automation, alerts, classification, artificial intelligence, information systems*

Сучасні інформаційні системи генерують значні масиви журналів подій, що містять повідомлення різної важливості. Надмірна кількість сповіщень створює ефект втоми, через що оператори ігнорують або пропускають критичні події. Традиційні методи, зокрема фіксовані інтервали розсилки та порогові значення метрик, недостатньо ефективні, оскільки не враховують зміст і контекст помилки. Це обумовлює потребу у використанні методів штучного інтелекту, які здатні аналізувати текст повідомлення та визначати його критичність.

У роботі пропонується система адаптивного управління сповіщеннями, що поєднує NLP моделі зі службами асинхронної обробки даних. Архітектура включає модуль отримання повідомлень на основі FastAPI, сервіс класифікації з використанням zero shot моделі сімейства Transformer, базу даних MongoDB для зберігання результатів аналізу, а також Celery і Redis для реалізації механізмів асинхронної обробки і планування.

Система використовує три послідовні алгоритми: попередню фільтрацію та класифікацію повідомлень, оцінку їхнього впливу, а також планування часу надсилання. Критичні повідомлення доставляються негайно, тоді як події зі слабшим впливом групуються і надсилаються пакетно. Такий підхід дозволяє зменшити когнітивне навантаження і підвищити оперативність реагування.

Проведене тестування показало високу точність класифікації критичних подій, коректну роботу алгоритмів групування та відправлення, а та-

кож зменшення кількості несуттєвих сповіщень. Запропонована система може бути інтегрована у різні IT середовища та легко масштабуватися.

Перспективні напрями розвитку включають перехід на потокові протоколи для отримання повідомлень, донавчання моделей на доменних логах та розширення доступних каналів доставки сповіщень.

Література

1. Atlassian. Understanding and fighting alert fatigue // Incident management for high-velocity teams [Електронний ресурс]. 2025. Режим доступу: https://www.atlassian.com/incident-management/on-call/alert-fatigue#What-is-alert-fatigue

2. Ohly S., Bastin L. Effects of task interruptions caused by notifications from communication applications on strain and performance [Електронний ресурс] // Journal of Occupational Health. 2023. Режим доступу: https://academic.oup.com/joh/article/65/1/e12408/7479297

3. Jackson J. Alarms Survey: Perceptions, Issues, Improvements, and Priorities of Healthcare Professionals [Електронний ресурс] / Healthcare Technology Foundation. 2011. Режим доступу: https://www.aami.org/docs/default-source/foundation/alarms/2011-htfalarmssurveyfinal.pdf

4. Grafana. Alert rule evaluation // Grafana documentation [Електронний ресурс]. 2025. Режим доступу: https://grafana.com/docs/grafana/next/alerting/fundamentals/alert-rule-evaluation/

5. Logpai. Loghub [Електронний ресурс]. 2023. Режим доступу: https://github.com/logpai/loghub

УДК 355.23:004.9

ВІРТУАЛЬНІ ТРЕНАЖЕРИ ТА СИМУЛЯЦІЙНІ ТЕХНОЛОГІЇ У ВІЙСЬКОВІЙ ОСВІТІ

Вікторія РОМАНЮК
Національний університет оборони України, м. Київ

Анотація. *У статті розглянуто роль віртуальних тренажерів та симуляційних технологій у вдосконаленні військової освіти. Показано їх вплив на розвиток професійних компетентностей, критичного мислення й умінь прийняття рішень у складних бойових умовах.*

Ключові слова: *віртуальні тренажери, симуляційні технології, військова освіта, підготовка військовослужбовців, цифрове навчання.*

Abstract. *The paper examines the role of virtual simulators and simulation technologies in improving military education. Their impact on the development of professional competencies, critical thinking, and decision-making skills in complex operational contexts is highlighted.*

Keywords: *virtual simulators, simulation technologies, military education, servicemen training, digital learning.*

Сучасна військова освіта потребує інноваційних підходів до підготовки фахівців, здатних ефективно діяти в умовах інформаційно-комунікаційного середовища, швидкої зміни технологій та бойових реалій. Одним із найрезультативніших напрямів цифровізації освітнього процесу є застосування віртуальних тренажерів та симуляційних технологій, що забезпечують моделювання професійних ситуацій максимально наближених до реальних [2].

Віртуальні тренажери дають змогу формувати навички управління технікою, озброєнням і комунікаційними системами без ризику для життя, економлячи ресурси й час. Застосування таких систем у навчальному процесі сприяє розвитку рефлексивних умінь, самоконтролю, підвищенню мотивації до навчання та формуванню командної взаємодії [1].

Крім того, використання тренажерних систем сприяє створенню безпечного навчального простору, де здобувачі освіти можуть експериментувати, допускати помилки й повторювати завдання без негативних наслідків. Це особливо важливо для формування впевненості у власних силах і розвитку професійної стійкості, яка є базовою рисою військового фахівця. Віртуальні тренажери також забезпечують можливість колективного навчання, де курсант може виконувати роль як виконавця, так і командира, що підвищує гнучкість та адаптивність підготовки.

Окрім цього, сучасні тренажерні комплекси дозволяють відтворювати як стандартні навчальні ситуації, так і нештатні події, що вимагають від курсантів миттєвого реагування та застосування творчого мислення. У такому контексті навчання набуває дослідницького характеру, а здобувачі освіти виконують роль активних учасників моделювання бойових чи опе-

ративних сценаріїв, а не пасивних спостерігачів. Це сприяє розвитку критичного аналізу, швидкості прийняття рішень і здатності працювати в умовах стресу – ключових складових військової професійної компетентності.

Симуляційні технології реалізують принцип «навчання через дію» (*learning by doing*) і дозволяють курсантам аналізувати результати своїх рішень у віртуальному середовищі. За допомогою імітаційних систем можливо відпрацьовувати бойові сценарії, кризові ситуації, логістику, евакуаційні та пошуково-рятувальні операції [4].

У поєднанні з інтелектуальними аналітичними модулями такі технології перетворюють процес навчання на динамічну систему зворотного зв'язку. Результати дій курсантів автоматично оцінюються за низкою параметрів – точність, швидкість, ефективність, дотримання тактичних норм — що робить тренування максимально наближеним до бойових умов. Це дає змогу не лише оцінити знання, а й формувати поведінкові алгоритми реагування у кризових ситуаціях.

Завдяки використанню штучного інтелекту у віртуальних тренажерах можливо не лише моделювати поведінку супротивника, а й адаптувати складність завдань до рівня підготовленості кожного курсанта. Це створює умови для індивідуалізації навчання, підвищує його ефективність і сприяє формуванню самостійності у прийнятті рішень. Додатковою перевагою є накопичення та аналітична обробка даних про результати тренувань, що дозволяє викладачам об'єктивно оцінювати прогрес здобувачів освіти та коригувати навчальні програми.

Серед сучасних прикладів інтеграції симуляційних технологій у військову освіту можна виокремити системи VBS4 (Virtual Battlespace), Steel Beasts, ARMA Reforger VR, які підтримують створення багатокористувацьких сценаріїв, що дозволяє одночасно тренувати кілька підрозділів у реалістичному цифровому середовищі [5].

Такі системи активно використовуються у країнах-членах НАТО для спільної підготовки персоналу різних рівнів — від тактичного до стратегічного. Вони забезпечують міжвідомчу взаємодію підрозділів у симульованих умовах бойових операцій, сприяючи уніфікації процедур управління, комунікації та прийняття рішень. Саме тому впровадження подібних технологій в українську військову освіту є не лише технічним, а й стратегічним кроком у напрямі сумісності з освітніми та професійними стандартами НАТО.

Особливе значення мають VR- та AR-технології, що створюють ефект присутності у бойових умовах. Вони застосовуються для тренування операторів безпілотних літальних апаратів, саперів, медиків, командирів підрозділів. У поєднанні з аналітичними системами та штучним інтелектом симуляційні рішення сприяють об'єктивному оцінюванню рівня підготовленості військовослужбовців [2].

Використання доповненої реальності (AR) дозволяє інтегрувати цифрові елементи в реальний простір навчальних полігонів, що підвищує ступінь занурення у навчальну ситуацію. Наприклад, AR-окуляри можуть

відображати візуальні індикатори цілей, маршрути пересування чи результати умовного ураження. Таке поєднання фізичного та віртуального простору сприяє розвитку просторового мислення, тактичного бачення і командної взаємодії.

Важливо також зазначити, що віртуальні тренажери сприяють формуванню міждисциплінарних навичок – аналітичних, технічних і комунікативних. Вони дозволяють інтегрувати елементи STEM-освіти у військову підготовку, роблячи її більш практично орієнтованою та науково обґрунтованою. Це відкриває перспективи для співпраці між військовими закладами освіти та ІТ-сектором, зокрема у розробці спеціалізованих симуляторів для різних військових спеціальностей.

Запровадження віртуальних тренажерів та симуляційних технологій у систему військової освіти України відповідає вимогам «Концепції розвитку військової освіти в Україні» [3] та стратегічним орієнтирам НАТО щодо стандартизації процесів підготовки персоналу. Це сприяє підвищенню якості навчання, оптимізації ресурсів і підготовці фахівців, здатних діяти в умовах гібридних загроз та цифрової трансформації оборонної сфери.

Таким чином, поєднання симуляційних технологій, віртуальних тренажерів, VR/AR-інструментів і аналітичних платформ формує комплексну систему підготовки нового покоління військових фахівців, які мислять критично, діють злагоджено й ефективно використовують цифрові ресурси в умовах реального бою.

Література

1. Бєляєв, В. П. Симуляційні технології у підготовці військовослужбовців. *Інформаційні технології в освіті*. 2021. Вип. 49. С. 33–41. DOI: https://doi.org/10.15561/18168421.2021.49.05

2. Коваленко, І. О. Цифровізація військової освіти: виклики та перспективи. *Військова освіта*. 2022. № 1(45). С. 12–18. DOI: https://doi.org/10.33099/2617-1783-2022-45-1-12-18.

3. Міністерство оборони України. *Концепція розвитку військової освіти в Україні*. Київ: МОУ, 2023. URL: https://www.mil.gov.ua/content/education/konczepcziya_vijs%60kovoi_osviti_2023.pdf (дата звернення: 12.11.2025).

4. Dudley, J. Simulation-based learning in modern defense education. *Journal of Military Learning*. 2020. Vol. 4, No. 2. P. 23–31. URL: https://www.armyupress.army.mil/Journals/Journal-of-Military-Learning/ (дата звернення: 12.11.2025).

5. NATO Allied Command Transformation. *Education and Training Opportunities in the Alliance*. Norfolk, VA, 2023. URL: https://www.act.nato.int/publications (дата звернення: 12.11.2025).

УДК 614.84

СПЕЦИФІКА ПІДГОТОВКИ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ ДО ІНФОРМАЦІЙНО-РОЗ'ЯСНЮВАЛЬНОЇ РОБОТИ

Олександр САВЧЕНКО, Юлія БЕЗУГЛА,
Анастасія МІХАЙЛІЧЕНКО, Уляна ТАНАСІЙЧУК
Національний університет цивільного захисту України

Abstract. *Continuously carry out informational and explanatory work to ensure the safety of the population's livelihood, a necessary skill for the DSNS health service provider. The work outlines the specifics of preparing health workers for general knowledge of the National Health Center of Ukraine before carrying out such work with the population.*

Key words *information and explanation work, public safety, interactive learning***.**

Анотація. *Вміння проводити інформаційно-роз`яснювальну роботу з питань безпеки життєдіяльності населення необхідний навик співробітника ДСНС. В роботі наведено специфіку підготовки здобувачів вищої освіти НУЦЗ України до проведення такої роботи з населенням.*

Ключові слова *інформаційно-роз`яснювальна робота, безпека населення, інтерактивне навчання.*

Проведення інформаційно-роз`яснювальної роботи регламентується [1-3]. При її проведенні можна використовувати наступні інструменти:

- публікації;
- навчальні заняття, модулі та презентації;
- інтерактивне навчання;
- театральне та сценічне мистецтво;
- ігри та конкурси;
- аудіо- та відеоматеріали;
- інтерактивні ресурси;
- соціальні ЗМІ;
- телекомунікації [4,5].

Протягом тривалого часу публікації були улюбленим засобом поширення інформації серед населення. Маючи майже безмежну гнучкість, публікації можуть видаватися у форматі друкованих чи цифрових матеріалів, а також випускатися у різних формах та форматах. Вони можуть використовуватися як реклама (рекламні щити та плакати), з метою підтримки інформаційної взаємодії (навчальні матеріали або ігри), а також виконувати багато інших додаткових функцій.

Рішення про вибір найкращого варіанта друкованих матеріалів залежить від:

- цільової аудиторії;
- обсяг інформації, яку необхідно поширити;

- кількості необхідних для поширення копій;
- способу розповсюдження;
- довговічності друкованої продукції.

Практично всі друковані матеріали можна донести до широкої аудиторії у формі веб-сторінок для інтерактивного перегляду або завантаження на персональний комп'ютер. Інформаційні повідомлення можуть бути оптимізовані для розповсюдження через мобільні телефони або інші портативні електронні пристрої.

Незалежно від того, чи є публікація друкованою або ж поширюється в електронному вигляді, вона повинна бути інформативною та переконливою. Чим більше інтерактивних елементів містять матеріали, тим вони ефективніші, з точки зору активного залучення читача та сприяння зміні його поведінки. Публікації можуть бути розроблені для особливої цільової аудиторії, містити основні інформаційні повідомлення та рекомендації, а також детальнішу інформацію для підготовки інструкторів або самопідготовки. Деякі матеріали розробляються для одноразового використання, а інші використовуються постійно.

Навчальні заняття, навчальні модулі та презентації належать до традиційних способів представити значний обсяг знань у рамках стандартних освітніх зусиль. Важлива інформація часто поширюється в ході серйозних заходів, таких як зустрічі, семінари та вебінари (інтерактивні семінари), які спочатку були розроблені для структурування та підтримки очного навчання співробітників, добровольців, студентів, викладачів та членів спільнот. Впровадження нових елементів, до яких належать інтерактивні вправи, активне навчання та використання соціальних мереж, ще більше підвищує значущість, перевагу та ефективність використовуваних підходів.

Навчання на основі використання можливостей персональних комп'ютерів або інтерактивних можливостей (для чого необхідний комп'ютер або планшет та доступ до Інтернету) – два способи отримання доступу до можливостей колективного навчання. Можливості інтерактивного навчання широко вивчені. У вищій школі та бізнес-спільнотах воно підтвердило свою ефективність, оскільки учні, які використовували інтерактивні методи навчання, показували вищі результати, ніж традиційні слухачі.

Ігри та конкурси пропонують ще одну захоплюючу можливість "навчання з розвагою". Для малих груп можна використовувати настільні ігри. Крім того, можна організовувати конкурси малюнків на асфальті, що завжди дуже видовищно. Творчі конкурси також можна організувати у змаганні, запросивши до участі шкільні та регіональні команди. Для їх проведення можна використовувати такі завдання, як розробка оформлення плакатів, написання питань для вікторин, написання оповідань, пісень та віршів, постановка сценок чи творення слоганів.

Три основних типи аудіо- та відеопродукції розрізняються за тривалістю, способами поширення та рівнем професіоналізму:

- соціальна реклама на радіо та телебаченні;
- короткі аудіо- або відеоролики;
- аудіо та відеоматеріали більшої тривалості.

Один із найпростіших та найдешевших способів для здійснення інформаційно-роз`яснювальної роботи є використання офіційних сайтів. До них відносяться офіційний сайт ДСНС, офіційні сторінки Головних управлінь ДСНС тощо. Прикладом такого ресурсу може бути офіційний сайт НУЦЗ України.

До соціальних медіа належать всі ті інтерактивні інструменти, які дозволяють людям спілкуватися один з одним без необхідності традиційної організаційної підтримки. До них відносяться: соціальні мережі, месенджери тощо. Революція в галузі електронних комунікацій спрощує та здешевлює можливості для поширення інформації.

Використання телекомунікацій має на увазі безліч різних можливостей. До них відносять: автоматичні системи надсилання текстових повідомлень. Розсилка повідомлень має велике значення для раннього оповіщення.

Немає єдиного, найефективнішого способу поширювати інформаційні повідомлення. Таким чином, успіх зазвичай досягається шляхом комбінування різних інструментів.

Розглянуті інструменти рекомендуються для використання при проведенні інформаційно-роз’ясювальної роботи з питань безпеки життєдіяльності населення.

Література

1. Про медіа: Закон України від 13.12.2022 р. № 2849-IX. Дата оновлення: 02.07.2023. URL: https://zakon.rada.gov.ua/laws/show/2849-20#Text.

2. Кодекс цивільного захисту України від 02.10.2012 р. № 5403-VI. Дата оновлення 05.10.2023. URL: https://zakon.rada.gov.ua/laws/show/5403-17#Text.

3. Про затвердження Порядку здійснення навчання населення діям у надзвичайних ситуаціях: Постанова Кабінету Міністрів України від 26.06.2013 р. № 444. URL: https://zakon.rada.gov.ua/laws/show/444-2013-%D0%BF#Text.

4. Палієнко А.В. Специфіка сприйняття медіа інформації//Витоки педагогічної майстерності. 2014. Випуск 14. С 202-208.

5. Особливості підготовки здобувачів вищої освіти НУЦЗ України до інформаційно-роз`яснювальної роботи з питань безпеки життєдіяльності населення / Савченко О.В., Безугла Ю.С. // Бюлетень Національного університету цивільного захисту України. Присвячений 95-річчю заснування закладу. – Х.; НУЦЗУ, 2023. – С.115-119.

УДК 378:37

ОСОБЛИВА РОЛЬ ШТУЧНОГО ІНТЕЛЕКТУ В КІБЕРБЕЗПЕЦІ

Віталій СВІТЛИЧНИЙ
Харківський національний університет внутрішніх справ, Харків, Україна

***Анотація**. Робота присвячена вивченню впливу технологій штучного інтелекту на систему кібербезпеки протягом 2024–2025 років. Розглянуто питання масштабування автоматизованих кіберзагроз, зміни характеру атак під впливом генеративних технологій та методи захисту ШІ-систем від зловмисних дій. Встановлено, що шкідливий автоматизований трафік досяг позначки 49% від загального обсягу мережевої активності, а застосування генеративних алгоритмів суттєво підвищило результативність маніпулятивних соціальних атак. Проаналізовано рекомендації ENISA, статистику Imperva і Arkose Labs, а також методологічні підходи NIST AI RMF та MITRE ATLAS як базові інструменти протистояння сучасним кіберризикам.*

***Ключові слова**: штучний інтелект, кібербезпека, бот-трафік, генеративні моделі, AI RMF, MITRE ATLAS*.

***Abstract.** The work is dedicated to the infusion of artificial intelligence technologies into the cybersecurity system over the period 2024–2025. The paper examines the scaling of automated cyber threats, changing the nature of attacks with the influx of generative technologies and methods for protecting BI systems from malicious actions. It was found that low-speed automated traffic reached 49% of the total number of borderline activities, and the use of generative algorithms significantly increased the effectiveness of manipulative social attacks. The recommendations of ENISA, statistics from Imperva and Arkose Labs, as well as the methodological approaches of NIST AI RMF and MITER ATLAS were analyzed as basic tools for confronting current cyber crises.*

***Keywords:** piece intelligence, cybersecurity, bot traffic, generative models, AI RMF, MITER ATLAS.*

Вступ. Протягом останніх років технології штучного інтелекту стали ключовим елементом як у розробці захисних стратегій, так і в організації кіберзлочинів. Еволюція генеративних алгоритмів надала зловмисникам можливості формувати переконливі фішингові послання, небезпечний програмний код та фальсифіковані мультимедійні матеріали з неймовірною достовірністю. Паралельно захисні комплекси все частіше інтегрують ШІ-компоненти для безперервного спостереження, розбору поведінкових патернів та оперативного реагування на інциденти безпеки.

Мета роботи полягає в систематизації інформації 2024–2025 років щодо впливу інтелектуальних технологій на безпеку цифрових систем та виявлення дієвих способів протидії новітнім загрозам. Для досягнення поставленої мети проведено аналітичний огляд досліджень провідних світових організацій у галузі інформаційної безпеки.

Викладення основного матеріалу. Дослідження ґрунтується на вивченні матеріалів міжнародних експертних центрів з кібербезпеки. Першочергову увагу приділено аналітичним матеріалам ENISA, які відображають еволюцію загроз за період липень 2023 – червень 2024 року [1, 8, 10]. Додатково опрацьовано статистичні звіти компаній Imperva і Arkose Labs стосовно динаміки автоматизованого мережевого трафіку [5, 6].

Отримані дані свідчать про занепокійливу ситуацію: протягом 2024 року обсяг шкідливих автоматизованих запитів сягнув 49% від загального трафіку, тоді як певні цифрові платформи реєстрували до 73% небажаної активності ботів [5, 6]. Це вказує на те, що більшість взаємодій з окремими сервісами здійснюється не справжніми користувачами, а програмними агентами. Такі bot-системи демонструють зростаючу складність архітектури та спроможність долати традиційні бар'єри ідентифікації, що підтверджують дослідження методів виявлення через аналіз унікальних характеристик веб-оглядачів [7, 9].

Особливу небезпеку представляють генеративні ШІ-технології. Відповідно до висновків Gartner, вони утворили один з найвагоміших факторів зростання кіберризиків протягом 2024 року [4]. Генеративні алгоритми уможливлюють виробництво високоякісних фішингових повідомлень, які відтворюють комунікаційний стиль конкретних компаній чи осіб, причому у великих обсягах. ENISA констатує, що подібні можливості спричинили стрімке підвищення ефективності атак соціальної інженерії [1, 8].

Одночасно формується принципово новий напрямок загроз – кібератаки, спрямовані безпосередньо проти ШІ-систем. База знань MITRE ATLAS каталогізує різноманітні методики таких втручань [3]. До них належать: маніпуляції з вхідними запитами до моделей (prompt injection) з метою витягування конфіденційних відомостей, впровадження шкідливої інформації до тренувальних масивів (data poisoning) і намагання реплікувати комерційні моделі шляхом масованих звернень (model extraction).

Для протистояння описаним викликам формуються комплексні методології. NIST представив концептуальну модель керування ризиками ШІ (AI RMF), яка упорядковує підходи до оцінювання та зменшення небезпек [2]. Практична реалізація передбачає adversarial-перевірку моделей на опірність атакам [7], багатофакторну верифікацію користувачів, безперервне відстеження нетипової активності систем та систематичне вдосконалення захисних рішень [9, 10].

Висновки Вивчення матеріалів 2024–2025 років демонструє, що інтелектуальні технології трансформують ландшафт кібербезпеки. Зловмисники активно застосовують ШІ для масштабування атак – зростання автоматизованого трафіку до рівня 49–73% є переконливим свідченням цього [5, 6]. Генеративні системи забезпечують створення маніпулятивних матеріалів такої правдоподібності, що їх ідентифікація як фальшивих стає вкрай проблематичною.

Водночас ШІ-технології перетворюються на ефективний захисний механізм. Системи, побудовані на принципах машинного навчання, спроможні обробляти масивні інформаційні потоки в режимі реального часу, ідентифікувати нестандартні патерни та прогнозувати загрози на випередження. Застосування методологій NIST AI RMF [2] та MITRE ATLAS [3] забезпечує структурований механізм управління ризиками та розпізнавання небезпек.

Проте технологічний інструментарій сам собою не вирішує всіх проблем. Adversarial-тестування [7], постійний контроль [9, 10] та оперативна модернізація захисних систем потребують скоординованих зусиль спеціалізованих команд. Крім того, людський компонент зберігає критичне значення – саме експерти ухвалюють кінцеві рішення у неоднозначних ситуаціях та гарантують етичність застосування ШІ-інструментів у сфері кіберзахисту.

Література

1. ENISA. ENISA Threat Landscape 2024: July 2023 – June 2024. Luxembourg: ENISA, 2024.

2. NIST. Artificial Intelligence Risk Management Framework (AI RMF). Gaithersburg: NIST, 2024.

3. MITRE Corporation. ATLAS – Adversarial Threat Landscape for AI Systems [Електронний ресурс]. 2024–2025. Режим доступу: https://atlas.mitre.org

4. Gartner. Top Cybersecurity Trends for 2024. Stamford: Gartner, 2024.

5. Arkose Labs. Bad Bot Traffic Continues To Surge Across the Internet in 2024. 23.01.2024.

6. Imperva. 2024 Bad Bot Report. Imperva Inc., 2024.

7. Venugopalan H. та ін. FP-Inconsistent: Detecting Evasive Bots Using Browser Fingerprint Inconsistencies. ArXiv:2406.07647, 2024.

8. IndustrialCyber. ENISA Threat Landscape 2024 Identifies Key Cybersecurity Threats. 2024.

9. Em360Tech. Top 10 Bot Management Software Solutions for 2024. 04.06.2024.

10. Cyble. EU Cybersecurity in 2024: Insights from ENISA's Latest Report. 05.12.2024.

УДК 004.4:004.75:004.738.5

ПОРІВНЯННЯ ПІДХОДІВ REST, GRAPHQL ТА GRPC У КОНТЕКСТІ ВИМОГ ДО API

Олена СЕНИК, Павло ЛУБ
Львівський національний університет ветеринарної медицини та біотехнологій імені С.З. Ґжицького, м. Львів

Анотація. *У дослідженні розглянуто підходи до створення API за допомогою REST, GraphQL та gRPC. Проаналізовано особливості кожної технології, сфери застосування, переваги та недоліки. Наведено короткі висновки порівняння на основі практичної реалізації..*
Ключові слова: *API, REST, GraphQL, gRPC, запити, ефективність.*

Abstract. *The research investigated approaches to API development utilizing REST, GraphQL, and gRPC. The characteristics, application domains, benefits, and drawbacks of each technology were analyzed. Brief comparison conclusions based on practical implementation were presented.*
Keywords: *API, REST, GraphQL, gRPC, queries, efficiency.*

У сучасних програмних засобах API відіграє ключову роль, адже є інструментом для взаємодії між сервісами, додатками, сайтами тощо. Технології REST, GraphQL і gRPC – це різні підходи до реалізації API. Сьогодні REST є найпоширенішою архітектурою завдяки простоті, зручності і широкій сумісності. GraphQL вирішує проблему роботи зі складними даними, а також зменшує запити і кількість непотрібних даних. Серед трьох згаданих технологій gRPC є найменш поширеною. Вона створена на основі протоколу HTTP/2 і використовує бінарний формат для передачі інформації, що забезпечує високу продуктивність і низьку затримку. Порівняння цих підходів є актуальним, адже кожна технологія має свої обмеження, що впливає на вибір оптимальної технології залежно від заданих умов створення застосунку.

В межах дослідження важливо розглянути ефективність технологій з усіх сторін. Серед показників для оцінювання ключовими є метрики продуктивності (response time, throughput, latency), обробка складних вкладених структур тощо. Важлива частина – це зручність розробки, яка складається з налаштування технологій, гнучкості, можливості розширення функціоналу, зрозумілої документації та інших. REST поширена в простих традиційних додатках, GraphQL може ефективно працювати з великою кількістю вкладених сутностей, а gRPC дає можливість швидко передавати дані. Отже, визначення метрик і показників для тестування дозволить отримати цілісну картину під час дослідження.

Для повноцінного порівняння ефективності технологій REST, GraphQL та gRPC необхідно розробити єдине API з однаковою бізнес-логікою. За допомогою дослідження можна виявити чіткі конкретні сценарії, де кожна технологія є по своєму ефективна. Незважаючи на значну

кількість статей щодо вибору оптимальної технології, часто бракує візуальних тверджень і порівнянь. Для видимого порівняння варто використати таблиці, діаграми, засоби для тестування (JMeter, PostMan) тощо.

Результати тестування відображатимуть сильні та слабкі сторони кожної технології. Прогнозованим висновком цього аналізу є твердження, що вибір оптимального рішення залежить від заданих умов роботи. Отже, REST варто використовувати в простих традиційних веб застосунках, GraphQL корисна в сервісах, де багато пов'язаних даних і необхідний гнучкий доступ до них, а gRPC потрібен в системах з швидким обміном даних (онлайн ігри, відеотрансляції тощо), тобто потокових сервісів і високонавантажених систем.

Література

1. What is an API (Application Programming Interface). GeeksforGeeks. URL: https://www.geeksforgeeks.org/software-testing/what-is-an-api/ (дата звернення: 02.10.2025).

2. REST vs GraphQL vs gRPC. Design Gurus. URL: https://www.designgurus.io/blog/rest-graphql-grpc-system-design (дата звернення: 18.10.2025).

3D-ДРУК ЯК ІНСТРУМЕНТ ШВИДКОЇ РОЗРОБКИ ЕЛЕМЕНТІВ РОБОТОТЕХНІЧНИХ СИСТЕМ ДЛЯ ОБОРОННИХ ПОТРЕБ

Ілля Січко , Іван КОВТУН, Вадим МАЛЬЦЕВ
Харківський національний університет внутрішніх справ

Abstract: *The application of 3D printing forrapid development and manufacture of components for defense robotics systemsis considered. The advantages of additive technologies in prototyping, cost reduction, increased flexibility, and the ability to quickly create elements of UAVs and ground platforms in various conditions are demonstrated.*

Keywords: *3D printing, additive technologies, robotics, defense systems, prototyping, UAVs, robotic platforms, materials science, rapid manufacturing.*

Анотація*. Розглянуто застосування 3D-друку для швидкої розробки та виготовлення компонентів робототехнічних систем оборонного призначення. Показано переваги адитивних технологій у прототипуванні, зменшенні вартості, підвищенні гнучкості та можливості оперативного створення елементів БпЛА й наземних платформ у різних умовах..*

Ключові слова: *3D-друк, адитивні технології, робототехніка, оборонні системи, прототипування, БпЛА, роботизовані платформи, матеріалознавство, швидке виготовлення.*

Сучасні воєнні конфлікти характеризуються високою інтенсивністю технологічного розвитку, зміною тактик ведення бойових дій та постійною потребою у швидкій модернізації технічних засобів. У таких умовах особливого значення набувають інструменти та технології, що дозволяють опера-

тивно створювати, адаптувати та відновлювати елементи техніки, зокрема робототехнічних і безпілотних систем оборонного призначення. 3D-друк, або адитивне виробництво, став однією з найбільш перспективних і затребуваних технологій останнього десятиліття, оскільки він забезпечує можливість швидкого створення прототипів, індивідуальних деталей і повноцінних конструкцій без потреби у великих виробничих ресурсах або складному обладнанні. Саме здатність забезпечувати високу оперативність у розробці й виготовленні компонентів робить 3D-друк важливим інструментом підвищення ефективності військових підрозділів, що працюють у змінних або обмежених умовах. Адитивні технології дозволяють створювати деталі складної геометрії, оптимізовані під конкретні завдання, а також швидко усувати технічні несправності шляхом друку запасних частин, що дає змогу зменшити залежність від централізованих ремонтних баз [1, С. 7].

Використання 3D-друку у робототехнічних системах охоплює широкий спектр напрямів — від виготовлення корпусних елементів до створення індивідуальних функціональних вузлів. Для безпілотних літальних апаратів адитивні технології стали одним із ключових інструментів, що дає змогу виготовляти легкі, міцні та аеродинамічно оптимізовані елементи, які не завжди можливо реалізувати за допомогою традиційних методів. Особливо важливою є можливість створення індивідуальних рішень — наприклад, корпусів під конкретні типи камер, кріплень для антен, адаптованих хвостових та крилових елементів, а також конструкцій для швидкої зміни конфігурації БпЛА відповідно до поточної операційної потреби. У роботизованих наземних платформах 3D-друк також відіграє значну роль у створенні механічних конструкцій, корпусів для сенсорів, захисних оболонок та навіть елементів маніпуляторів. Досить часто підрозділам доводиться працювати з обладнанням, яке було пошкоджене або вийшло з ладу внаслідок інтенсивної експлуатації, і в таких випадках можливість надрукувати нову деталь на місці значно скорочує час простою. Також важливою перевагою є те, що підрозділи можуть створювати абсолютно нові елементи для адаптації систем під специфічні умови рельєфу, завдань чи тактичної обстановки [2, С. 138].

Застосування сучасних матеріалів у 3D-друці відіграє важливу роль у підвищенні ефективності надрукованих конструкцій. Окрім стандартних полімерів, у військовій сфері активно використовуються композитні матеріали з покращеними характеристиками — зокрема, полімери з армуванням вуглецевим волокном, скловолокном або кевларом. Такі матеріали забезпечують набагато вищу міцність, стійкість до механічних навантажень, температурних коливань та вібрацій, що робить їх придатними для створення конструктивних елементів, які раніше виготовляли лише методом фрезерування або лиття. Застосування адитивного виробництва у поєднанні з оптимізацією геометрії деталей дозволяє зменшити їхню вагу без втрати функціональності, що є критично важливим для безпілотників і мобільних роботизованих платформ. Крім того, багато сучасних принтерів є

портативними, не потребують спеціальних умов для роботи та можуть бути розміщені у пересувних майстернях, ремонтних пунктах або укриттях. Це дозволяє забезпечувати оперативне технічне обслуговування прямо у зоні виконання завдань, що значно підвищує автономність військових підрозділів і їхню здатність швидко відновлювати техніку [3, С. 29].

Узагальнюючи, інтеграція 3D-друку в оборонну робототехніку відкриває широкі можливості для підвищення ефективності, гнучкості та адаптивності військових систем. Адитивні технології дають змогу скоротити виробничі цикли, зменшити витрати, підвищити рівень автономності та оперативності технічного забезпечення. Робототехнічні комплекси можуть модернізуватися значно швидше, адже будь-які зміни в конструкції можна протестувати практично миттєво, а нові деталі — виготовити безпосередньо на місці. У сучасних умовах, коли темп розвитку бойових технологій постійно зростає, а зміни на полі бою відбуваються швидко, саме можливість оперативно адаптувати техніку стає вирішальним фактором. З огляду на швидкий розвиток адитивних технологій і матеріалів можна прогнозувати, що їх роль у секторі оборони та безпеки лише зростатиме, а 3D-друк стане одним із ключових інструментів технічного забезпечення робототехнічних систем у майбутньому [4, С. 138].

Література

1. ПАЩЕНКО, В. В., ГАНЖУГА, М. М. Сучасні адитивні технології для швидкого прототипування та виробництва військової техніки. *Технологічний аудит та резерви виробництва*. 2022. Vol. 6, No. 3(68). С. 6–10.

2. ФЕДОРЕНКО, В. В., РУБАН, М. І. Особливості використання адитивних технологій при створенні та експлуатації безпілотних літальних апаратів. *Науковий вісник Національного авіаційного університету. Серія: Технічні науки*. 2023. № 2(37). С. 135–142.

3. РЕПЕТЕЙ, А. В., ГУСЄВ, Д. А. Дослідження застосування полімерних композитів в адитивному виробництві для створення елементів військового призначення. *Проблеми машинобудування*. 2022. № 4(99). С. 28–34. DOI: 10.15407/probmach2022.04.028.

4. ПЕТРЕНКО, О. В., ДМИТРУК, П. М. Перспективи застосування адитивних технологій для забезпечення потреб оборонно-промислового комплексу України. *Проблеми науки*. 2024. № 1(24). С. 136–142.

УДК 004.4:004.9:614.8

ВИКОРИСТАННЯ ТЕХНОЛОГІЙ 3D МОДЕЛЮВАННЯ ТА 3D ДРУКУ ДЛЯ ПІДГОТОВКИ ЗДОБУВАЧІВ ОСВІТИ

Юлія СЛОБОДЯН, Юлія БУРДЕЙНА, Назар БУРАК
Львівський державний університет безпеки життєдіяльності

Анотація. У статті розглянуто застосування технологій 3D моделювання та 3D друку в освітньому процесі Львівського державного університету безпеки життєдіяльності. Показано, що створення цифрових моделей та фізичних макетів аварійного обладнання, елементів конструкцій і небезпечних об'єктів дозволяє формувати в здобувачів освіти інженерні компетентності та практичні навички, необхідні майбутнім рятувальникам. Використання 3D друку для виготовлення макетів осередків пожеж, газових клапанів, технічних вузлів і вибухонебезпечних предметів забезпечує безпечне середовище навчання та імітацію реальних сценаріїв без додаткових витрат на натурні тренування. Підкреслено важливість розвитку 3D лабораторій у ЗВО сфери цивільного захисту.

Ключові слова. *3D моделювання, 3D друк, рятувальники, ЛДУБЖД, навчальні макети, адитивні технології, підготовка кадрів.*

Annotation. *The paper examines the use of 3D modeling and 3D printing technologies in the educational process of the Lviv State University of Life Safety. It demonstrates that creating digital models and physical replicas of emergency equipment, structural elements, and hazardous objects strengthens the engineering competencies and practical skills required by future rescuers. The application of 3D printing for producing models of fire scenes, valves, mechanical components, and explosive objects provides a safe learning environment and enables realistic scenario simulation without the need for costly field training. The relevance of developing 3D laboratories within civil protection institutions is highlighted.*

Keywords *3D modeling, 3D printing, rescuers, LSULS, training models, additive technologies, emergency education.*

Сучасні підрозділи ДСНС виконують широкий спектр робіт — від пожежогасіння та рятування постраждалих до ліквідації наслідків вибухів, хімічних аварій і техногенних катастроф. Для ефективної підготовки майбутніх рятувальників університет потребує інструментів, які дозволяють моделювати реальні об'єкти та ситуації без значних матеріальних витрат і безпеки ризику. Одним із таких інструментів є технології 3D моделювання та 3D друку.

Впровадження 3D лабораторії у навчальний процес ЛДУБЖД дозволяє створювати точні копії аварійного обладнання, вузлів техніки та елементів критичної інфраструктури, які студенти можуть використовувати під час тренувань. Зокрема, моделювання конструктивних елементів будівель, засувок, пожежних гідрантів, з'єднувальних муфт, редукторів, газових клапанів та запірної арматури забезпечує можливість детально вивчати роботу цих систем без ризику виходу з ладу оригінального облад-

нання. 3D друк дозволяє відтворювати навчальні макети осередків пожеж, вентиляційних шахт, фрагментів завалених конструкцій та вибухонебезпечних предметів. Такі макети використовуються під час тактико-спеціальних занять, де здобувачі освіти відпрацьовують алгоритми пошуку постраждалих, ідентифікації небезпечних об'єктів та вибору безпечних маршрутів у зоні руйнувань.

Технології 3D моделювання також застосовуються для створення симуляційних сценаріїв — наприклад, реконструкції пожежних осередків у гуртожитках, промислових приміщеннях чи електрощитових. Отримані цифрові моделі дають можливість аналізувати поширення полум'я, поведінку конструкцій при нагріванні та потенційні маршрути евакуації. Це суттєво підвищує якість підготовки майбутніх рятувальників, адже дозволяє вивчати складні сценарії без проведення дорогих натурних тренувань. Окремо варто відзначити використання 3D друку в навчанні фахівців з хімічного та вибухотехнічного захисту.

Здобувачі освіти можуть працювати з друкованими макетами балонів з небезпечними речовинами, корпусів боєприпасів чи елементів вибухових пристроїв, не наражаючись на небезпеку. Це забезпечує глибоке розуміння будови об'єктів та формує практичні навички без ризику для життя. Таким чином, інтеграція технологій 3D моделювання та 3D друку у навчальний процес ЛДУБЖД забезпечує підвищення якості професійної підготовки, розширення інженерних компетентностей здобувачів освіти та створює безпечне середовище для відпрацювання практичних навичок, необхідних у діяльності рятувальників.

Література

1. 3D Printing for Training and Simulation in Emergency Services. – FireTech Journal. – 2024. – Режим доступу: https://firetechjournal.com/3dprint-training (дата звернення: 11.11.2025).

2. Зачко О.Б., Головатий Р.Р. Мультиагентна модель управління безпекою при плануванні проектів створення об'єктів з масовим перебуванням людей // Вісник НТУ «ХПІ». Серія: Стратегічне управління, управління портфелями, програмами та проектами. – Х.: НТУ «ХПІ», 2017. – № 2 (1224) – С. 46-51.

3. Шопський О., Головатий Р. Застосування моделей машинного навчання для раннього виявлення надзвичайних ситуацій на основі потокових великих даних. – 2025. – Режим доступу: https://scholar.google.com (дата звернення: 21.11.2025).

4. Introduction to Additive Manufacturing Technologies. – National Institute of Standards and Technology (NIST). – 2024. – Режим доступу: https://www.nist.gov (дата звернення: 11.11.2025).

УДК 167.7; 004.81

АВТОМАТИЗОВАНЕ УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ СИСТЕМАМИ: РОЛЬ ДАНИХ У РЕАЛЬНОМУ ЧАСІ

Смик Д., Бурак Н.
Львівський державний університет безпеки життєдіяльності

Анотація. *Дослідження присвячене ролі даних у режимі реального часу в автоматизованому управлінні інформаційними системами, описано основні архітектурні підходи до оброблення потоків даних та їх вплив на якість управлінських рішень. Наведено динаміку обсягу світового ринку аналітики потокових даних у 2019–2024 рр. та коротко окреслено основні практичні виклики впровадження таких систем.*

Annotation. *The study focuses on the role of real-time data in automated management of information systems, describing the main architectural approaches to streaming data processing and their impact on the quality of managerial decisions. The paper presents the dynamics of the global streaming analytics market in 2019–2024 and briefly outlines the key practical challenges of implementing such systems.*

Keywords automated information systems management; real-time data; streaming data analytics.

Автоматизоване управління інформаційними системами є одним із ключових напрямів розвитку сучасної цифрової економіки, оскільки забезпечує прийняття управлінських рішень на основі актуальних даних з мінімальною затримкою [1]. У контексті зростання обсягів інформації, ускладнення бізнес-процесів та підвищення вимог до безперервності функціонування підприємств особливої ваги набувають технології оброблення даних у режимі реального часу. Вони дають змогу скоротити часовий розрив між виникненням події, її фіксацією, аналізом і реагуванням, що безпосередньо впливає на ефективність діяльності організації. Режим реального часу в цьому випадку виступає не лише технічною характеристикою, а й важливою управлінською перевагою, яка визначає конкурентоспроможність суб'єктів господарювання. Саме тому дослідження ролі даних у реальному часі в системах автоматизованого управління має як теоретичне, так і прикладне значення.

Управління, засноване на даних у режимі реального часу, передбачає безперервне надходження, оброблення та інтерпретацію інформації з мінімальною часовою затримкою. На відміну від традиційних підходів пакетної обробки, коли аналіз здійснюється періодично й часто із суттєвим відставанням, потокове опрацювання дає змогу реагувати практично миттєво та передумови для формування адаптивних, самокерованих

систем, здатних змінювати власні налаштування, алгоритми чи порогові значення без прямого втручання оператора. Дані, які надходять у реальному часі, дозволяють виявляти аномалії, тенденції та критичні відхилення на ранніх етапах, коли наслідки ще можна мінімізувати. У результаті дані перетворюються з пасивного ресурсу на активний елемент управлінської парадигми, який визначає якість і швидкість прийняття рішень.

Значну роль у цьому відіграє зниження впливу людського фактору, який традиційно є джерелом помилок, затримок або суб'єктивних оцінок. Автоматизовані системи, що працюють із потоками даних, перебирають на себе рутинні операції з перевірки, фільтрації та попередньої оцінки інформації, звільняючи персонал для виконання більш складних аналітичних і стратегічних завдань, що підвищує узгодженість і повторюваність управлінських рішень, оскільки вони ґрунтуються на єдиній, синхронізованій інформаційній базі. Додатковою перевагою є прозорість процесів: ключові показники та стан системи можуть відстежуватися в будь-який момент часу, що полегшує аудит, контролінг і внутрішній моніторинг. Отже, режим реального часу сприяє переходу від інтуїтивної до доказової моделі управління.

Функціонування автоматизованого управління інформаційними системами, заснованого на потокових даних, безпосередньо пов'язане з особливостями архітектури цих систем. Сучасні рішення дедалі частіше будуються на основі розподілених, хмарних або гібридних інфраструктур, у яких окремі компоненти системи розміщені на різних обчислювальних вузлах, але взаємодіють як єдине ціле та забезпечують масштабованість, тобто можливість нарощувати обчислювальні ресурси в міру зростання навантаження, а також підвищує відмовостійкість, оскільки вихід з ладу окремих елементів не призводить до зупинки всієї системи. Важливою складовою такої архітектури є розподілені сховища даних, що дозволяють розміщувати інформацію ближче до джерела її формування й тим самим скорочувати затримки під час передавання та оброблення.

Також принциповим аспектом є організація потокового обміну повідомленнями та подіями між компонентами системи. Спеціалізовані програмні платформи забезпечують постановку подій у черги, їх упорядкування, буферизацію й доставлення до модулів, які виконують аналітику, контроль чи керуючі дії, що дає змогу обробляти значну кількість одночасних подій, підтримуючи стабільний час реагування. У поєднанні з засобами аналітичної обробки даних у пам'яті це дозволяє виконувати складні розрахунки, класифікацію, прогнозування чи оцінку ризиків без звернення до тривалих пакетних процедур.

Стрімкий розвиток технологій оброблення даних у режимі реального часу підтверджується статистичними показниками світового ринку аналітики потокових даних. Зокрема, аналітичні дослідження свідчать, що

глобальний ринок такої аналітики у 2019 році оцінювався приблизно у 7,74 млрд доларів США, а до 2027 року очікується зростання до понад 52 млрд доларів США [2]. На рисунку 1 представлена динаміка обсягу світового ринку аналітики потокових даних у 2019–2024 рр.

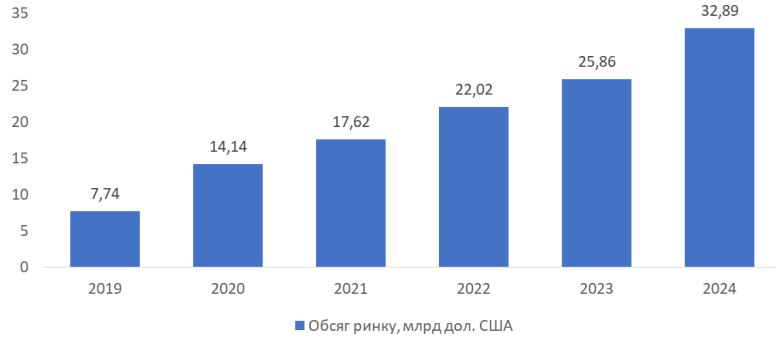

Рисунок 1 – Динаміка обсягу світового ринку аналітики потокових даних у 2019–2024 рр.

Отже, ринок технологій оброблення даних у режимі реального часу перебуває на етапі інтенсивного росту. Перехід від традиційних централізованих моделей до розподілених, edge-орієнтованих рішень зумовлює переформатування підходів до побудови інформаційних систем. Організації вимушені переглядати інфраструктурні стратегії, моделі зберігання та аналітики, а також політики безпеки даних. Статистичні дані підтверджують, що роль даних у реальному часі в автоматизованому управлінні інформаційними системами буде лише посилюватися.

Попри визначені переваги, впровадження автоматизованих систем управління на базі даних у реальному часі супроводжується низкою суттєвих викликів. Однією з головних проблем є інтеграція нових рішень із наявними системами, які часто не підтримують високі швидкості оброблення чи потокові інтерфейси, що потребує ґрунтовної модернізації інфраструктури, перегляду архітектурних підходів і, нерідко, значних капітальних інвестицій. Додаткову складність становить необхідність забезпечення низької латентності при зростанні кількості джерел даних і обсягу трафіку. Іншою важливою проблемою є підготовки персоналу, оскільки для роботи з такими системами потрібні нові компетентності у сфері аналізу даних, програмної інженерії та кібербезпеки [3].

Проведене дослідження підтвердило, що дані у режимі реального часу стають ключовим ресурсом для підвищення ефективності автоматизо-

ваних інформаційних систем, забезпечуючи швидкість, точність і доказовість управлінських рішень. Розподілені архітектури, потокові платформи та модульні інфраструктури дають змогу обробляти великі обсяги даних із мінімальною затримкою та підтримувати стабільність роботи систем у високонавантажених умовах. Динаміка світового ринку аналітики потокових даних за 2019-2024 рр. демонструє стрімке зростання, що підкреслює глобальний попит на рішення реального часу та їхнє стратегічне значення для цифрової трансформації. Водночас упровадження таких систем супроводжується викликами, пов'язаними з інтеграцією в наявну інфраструктуру, забезпеченням низької затримки, захистом даних і потребою у кваліфікованих фахівцях. Отже, технології оброблення даних у реальному часі визначають напрям подальшого розвитку сучасних інформаційних систем і створюють підґрунтя для переходу до більш автономних, адаптивних і стійких моделей управління.

Література

1. Тінтурін С. Г. Методологія використання штучного інтелекту в автоматизації управління інформаційними системами. Комп'ютерно-інтегровані технології: освіта, наука, виробництво. 2024. № 57. С. 45–52.

2. Precedence Research. Streaming Analytics Market Size, Share, and Trends 2024 to 2034. URL: https://www.precedenceresearch.com/streaming-analytics-market (дата звернення: 20.11.2025).

3. GeeksforGeeks. Real-Time Data Processing: Challenges and Solutions for Streaming Data. URL: https://www.geeksforgeeks.org/data-engineering/real-time-data-processing-challenges-and-solutions-for-streaming-data/ (дата звернення: 20.11.2025).

УДК 004.8 + 504

АДАПТИВНЕ ОНЛАЙН-НАВЧАННЯ ГІБРИДНИХ МОДЕЛЕЙ ДЛЯ ФОТОПАСТОК В УМОВАХ НЕВИЗНАЧЕНОСТІ

Юрій СОРОЧИЧ[1], Сергій СТРЯМЕЦЬ[1], Олександр ХЛЕВНОЙ[2]
[1]Національний університет «Львівська політехніка»
[2]Львівський державний університет безпеки життєдіяльності

Моніторинг біорізноманіття за допомогою фотопасток є ефективним інструментом для оцінки популяцій рідкісних видів, однак у реальних умовах змішаних екосистем виникають значні невизначеності: розмиття зображень через туман, низький контраст у нічний час, часткове перекриття об'єктів та морфологічна схожість між видами. Традиційні моделі на основі згорткових нейронних мереж (CNN), такі як ResNet-50 чи YOLOv5, досягають точності 80–85 %, але їх статичність обмежує адаптивність до динамічних умов, що призводить до помилок у класифікації (до 70–75 % у складних випадках). Гібридні моделі з нечіткою логікою підвищують стійкість до шуму на 15 %, однак брак механізмів безперервного (онлайн) навчання ускладнює їх застосування в автономних системах фотопасток.

Для вирішення наведених вище проблем було запропоновано гібридну архітектуру для адаптивного виявлення видів (рисунок 1), яка поєднує попередньо навчену глибоку згорткову нейронну мережу (CNN), таку як ResNet-50 або YOLOv5, з легким логістичним шаром.

Рисунок 1 – Блок-схема гібридної архітектури

Попередньо навчена CNN відповідає за екстракцію вектора ознак X з вхідного зображення, де X є елементом простору реальних чисел розмірності n, тобто $X \in \mathbb{R}^n$. Цей вектор представляє ієрархічні характеристики зображення, включаючи низькорівневі (краї, текстури) та високорівневі (форми тіла, голови). Після екстракції ознак логістичний шар обчислює ймовірність належності об'єкта до цільового класу за формулою $P = \sigma(W \cdot X + b)$, де σ – сигмоїдна функція активації, W – ваговий вектор, X – вектор ознак, b – зміщення. Ваги W оновлюються в онлайн-режимі за допомогою градієнтного спуску з урахуванням нечіткого коефіцієнта μ, який модулює крок навчання: $W_{t+1} = W_t - \eta \cdot \mu \cdot \nabla L$. Функція втрат L визначається як середньоквадратична помилка $L = (1/2)\,(P - Y)^2$, де Y – справжня мітка (1 для цільового виду, 0 для фону). Коефіцієнт μ, що варіюється від 0,75 до 1,0, обчислюється за евристичними правилами, які враховують

рівень розмиття (наприклад, за метрикою Laplacian), контрасту (за RMS-контрастом) та схожості ознак (за косинусною відстанню до еталонних векторів). Такий підхід дозволяє моделі адаптуватися до динамічних умов, таких як сезонні зміни освітлення чи часткове перекриття об'єктів, типових для біотопів Розточчя.

Симуляції проведено на наборі з 1000 гіпотетичних знімків, згенерованих за допомогою нормального розподілу $N(\mu X, \Sigma X)$, де параметри μX (середнє) та ΣX (коваріаційна матриця) отримано з витягу ознак попередньо навченої моделі ResNet-50 на відкритому наборі даних iWildCam, що містить реальні знімки з подібних екосистем. Цей набір імітує варіативність умов: 82% знімків – з низьким шумом ($\mu \approx 1{,}0$), 18% – з високою невизначеністю ($\mu \in [0{,}75,\ 0{,}85]$), що відповідає частоті туману, нічних зйомок чи схожості видів у Розточчі. Мітки Y відповідали 15% виявлення цільового виду (зубра), що відображає рідкісність таких видів у природі. Для статистичної валідації експерименти повторено 30 разів з різними ініціалізаціями, з використанням t-тесту для перевірки значущості відмінностей ($p < 0{,}001$). Оцінювалися динаміка ймовірності класифікації, норма вагового вектора, значення нечіткого коефіцієнта та порівняння зі статичною моделлю ResNet-50 без адаптивного шару. Реалізовано в Google Colab з бібліотеками TensorFlow, NumPy, scikit-learn.

Адаптивна модель досягла середньої точності 90% після 800 ітерацій (приріст +18% порівняно зі статичною CNN, де точність стабілізувалася на рівні 72%). Ймовірність класифікації P зростала нелінійно від 0,55 до 0,90, з середнім приростом 0,002 на ітерацію, що підтверджує ефективність градієнтного спуску. Норма вагового вектора стабілізувалася на рівні 2,2 після 600 ітерацій, з дисперсією ±0,15, що вказує на збіжність процесу. Нечітка корекція активувалася у 18 % випадків, запобігаючи нестабільності, зокрема при тумані чи нічній зйомці, де точність без корекції падала до 68 %. Гістограма нечіткого коефіцієнта підтвердила бімодальний розподіл: 82% – чіткі знімки з $\mu \approx 1{,}0$, 18% – невизначені з $\mu \in [0{,}75,\ 0{,}85]$, з середнім $\mu = 0{,}94 \pm 0.08$. Порівняння зі статичною моделлю показало статистично значущу перевагу (t-тест, $p < 0{,}001$), з F1-score 0,90 ± 0,01 проти 0,69 ± 0,02. Результати демонструють стабільність і ефективність моделі в умовах, подібних до біотопів Розточчя.

Таблиця 1 – Порівняння моделей (середнє ± стандартне відхилення)

Модель	Точність (%)	Precision	Recall	F1-score
Статична	72,1 ± 1,8	0,70	0,68	0,69
Адаптивна	90,3 ± 0,9	0,91	0,89	0,90

Таким чином, гібридна модель з онлайн-навчанням і нечіткою корекцією забезпечує стійкість до невизначеностей, перевищуючи статичні CNN за точністю та швидкістю адаптації. Підхід перспективний для автономних систем моніторингу в змішаній екосистемі Розточчя. Подальші дослідження передбачають валідацію на реальних даних та інтеграцію з ГІС.

Література

1. Fergus, P., Chalmers, C., Matthews, N., Nixon, S., Burger, A., Hartley, O., Sutherland, C., Lambin, X., Longmore, S., & Wich, S. (2024). Towards context-rich automated biodiversity assessments: Deriving AI-powered insights from camera trap data. *Sensors*, *24*(24), Article 8122. https://doi.org/10.3390/s24248122

2. Ференц Н. М., Хомин І. Г., Горбань І. М., Горбань Л. І. Рідкісні види флори і фауни природного заповідника «Розточчя» та сучасні загрози щодо їх збереження // *Науковий вісник Національного університету біоресурсів і природокористування України*. Серія : Лісівництво та декоративне садівництво. 2012. Вип. 171(1). С. 229–235.

3. Sorochych, Y., Striamets, S., Khlevnoi, O., & Zhezlo-Khlevna, N. (2025). Застосування гібридних моделей у моніторингу екологічних спільнот. Вісник Львівського державного університету безпеки життєдіяльності, 31, 50-59. https://doi.org/https://doi.org/10.32447/20784643.31.2025.06

УДК 004.056:351.746.1(043.2)

РОЗРОБКА ПРОГРАМНОГО РІШЕННЯ ТА МЕТОДОЛОГІЇ АНАЛІЗУ КОМПАНІЙ НА ОСНОВІ МЕТОДІВ OSINT

Сергій СТАЙКУЦА, Анна СЕЛЮКОВА
Державний університет інтелектуальних технологій і зв'язку

Анотація. *У сучасному інфопросторі методи OSINT застосовуються як у національній безпеці, так і бізнесі. Автор пропонує програмний комплекс на основі 13-крокової моделі OSINT-розслідування компаній, що включає аналіз реєстраційних даних, санкційних списків, судових справ, інтелектуальної власності тощо. Досліджено використання OSINT у бізнес-розвідці та оцінці корпоративних ризиків, його актуальність, ключові сфери й застосування..*

Ключові слова: *OSINT, корпоративне середовище, відкриті джерела інформації, розвідка, інформаційна безпека, аналіз інформації.*

Abstract. *In today's information space, OSINT methods are used in both national security and business. The author proposes a software package based on a 13-step model of OSINT investigation of companies, which includes analysis of registration data, sanctions lists, court cases, intellectual property, etc. The use of OSINT in business intelligence and corporate risk assessment, its relevance, key areas and applications are explored.*

Keywords: *OSINT, corporate environment, open sources of information, intelligence, information security, information analysis..*

У складному та конкурентному бізнес-середовищі компанії шукають ефективні стратегії для збереження лідерства, розвитку та конкурентної переваги. Одним з таких рішень може бути інтеграція OSINT у бізнес-аналітику, що стратегічно змінить підходи до збору даних і подальшого прийняття рішень. Застосування OSINT в бізнес-аналітиці революціонізує спосіб, у який компанії збирають інформацію та приймають обґрунтовані рішення. Так, правильно зібрана та проаналізована публічна інформація про контрагентів допоможе оцінити їх надійність, виявити потенційні офшори, реальних бенефіціарів, санкції, судові справи, банкрутства та репутаційні, ESG-ризики тощо [2].

Однак, під час упровадження OSINT, бізнес стикається з певною низкою труднощів. Передусім, відчувається нестача кваліфікованих команд і методологій для збору та перевірки даних. Крім того, OSINT залишається роздробленим між численними платформами, реєстрами та інструментами, що відрізняються надійністю, мовною підтримкою та правовим статусом.

Мета дослідження полягає у створенні сучасного українського програмного комплексу на основі розробленого контрольного списку із перевірки компаній на основі відкритих джерел, який буде відображати комплексний підхід щодо аналізу та обробки інформації [1].

Загальні принципи функціонування запропонованого програмного комплексу можна описати наступним чином. Вся взаємодія з програмою виконується через графічний інтерфейс, точніше – web-сайт. Основою програми є додаток Flask, який управляє маршрутизацією, відображенням вмісту та взаємодією з користувачем. Дані для кожного кроку зберігаються у форматі JSON, що включає номер кроку, назву, опис, пов'язані посилання та додаткові підрозділи. На рис. 1 можна побачити головну сторінку рішення.

Ключовою особливістю ПЗ є функція пошуку, яка здійснюється за допомогою маршруту /search. Користувачі можуть ввести ключове слово або фразу, які потім порівнюються з назвою та описом кожного кроку, мітками всіх доданих ресурсів та підрозділів. Для забезпечення надійності логіка пошуку враховує потенційні невідповідності в структурі даних, наприклад, такі як наявність або відсутність полів розділів або посилань. Результати збираються і відображаються в агрегованому вигляді, показуючи відповідні кроки і прямі збіги в них. На рис. 2 представлено блок-схему програмного рішення.

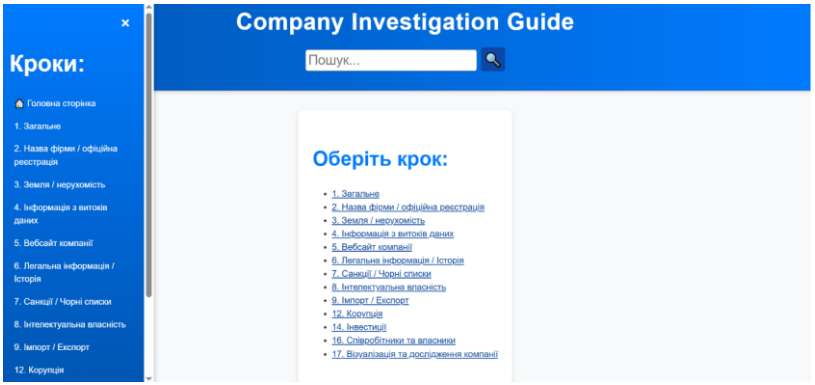

Рисунок 1 – Головна сторінка web-сайту

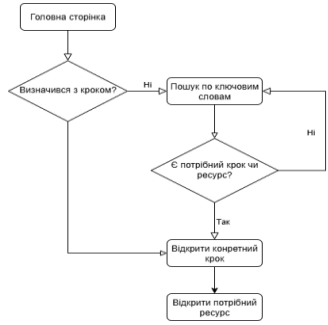

Рисунок 2 – Схема напрямків дослідження в рамках контрольного чек-листу

Наприклад, користувач, який шукає «OFAC», отримає результати, що вказують на кроки, пов'язані з перевіркою санкцій, з прямими посиланнями на базу даних санкцій OFAC в Opendatabot. Натискання на будь-який результат переводить користувача на детальну сторінку для цього конкретного кроку контрольного списку.

Підсумовуючи, варто відзначити, що робота є важливим кроком у напрямку формування уніфікованих підходів щодо дослідження компаній на основі OSINT. Відкриті джерела надають потужні інструменти для аналітиків, журналістів і бізнесу, а за умови достовірності та правильного контексту, отримана інформація буде конкурувати з даними закритих розвідувальних каналів [3].

Література

1. Стайкуца С. В., Пастухов Д. В., Селюкова А. Б., Дослідження інформаційного середовища сучасних компаній методами та інструментами OSINT. Наука, технології, інновації: вектори трансформації. : Матеріали науково-практ. конф., м. Ужгород, 24–25 жовт. 2025 р. Одеса, 2025. С. 106–110.

2. Owl G. Leveraging OSINT: Reducing International Business Risk with Golden Owl™ Solutions. Medium. URL: https://goldenowl.medium.com/leveraging-osint-reducing-international-business-risk-with-golden-owl-solutions-79eef4aec43f.

3. Hassan N. A., Hijazi R. Open Source Intelligence Methods and Tools. Berkeley, CA : Apress, 2018. URL: https://doi.org/10.1007/978-1-4842-3213-2.

УДК 004.94:528.9:351.86

ГЕОІНФОРМАЦІЙНА ВІЗУАЛІЗАЦІЯ НАДЗВИЧАЙНИХ ПОДІЙ ЯК ІНСТРУМЕНТ ПІДТРИМКИ УПРАВЛІНСЬКИХ РІШЕНЬ У СФЕРІ ЦИВІЛЬНОГО ЗАХИСТУ

Олег СТАСЬО, Назарій БУРАК
Львівський державний університет безпеки життєдіяльності

Анотація. *У статті розглянуто роль геоінформаційних систем (GIS) як інструменту підтримки управлінських рішень у сфері цивільного захисту. Показано переваги GIS для просторового аналізу, візуалізації надзвичайних подій і підвищення ефективності реагування на них*

Ключові слова: *геоінформаційна система, візуалізація, цивільний захист, управлінські рішення, надзвичайні події, просторовий аналіз, інформаційні технології.*

Annotation*. The article examines the role of Geographic Information Systems (GIS) as a tool for supporting management decisions in the field of civil protection. The advantages of GIS for spatial analysis, visualization of emergencies, and improving the efficiency of response actions are highlighted.*

Keywords *geographic information system, visualization, civil protection, management decisions, emergencies, spatial analysis, information technologies.*

Сучасна система цивільного захисту функціонує в умовах високої динаміки та невизначеності надзвичайних подій. Для ефективного реагування необхідні не лише аналітичні методи, а й засоби візуалізації, які дозволяють оперативно оцінювати ситуацію у просторі та часі. Одним із найпотужніших інструментів для цього є геоінформаційні системи (GIS), що забезпечують просторовий аналіз даних і підтримку прийняття рішень на різних рівнях управління

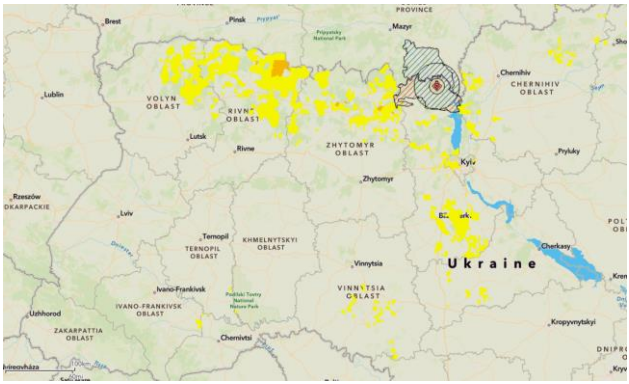

Рисунок 1 – GIS візуалізація поширення цезію-137 після Чорнобильської катастрофи [1]

Геоінформаційна система (GIS) — це сукупність програмних, апаратних та інформаційних засобів, призначених для збирання, зберігання, аналізу й відображення даних, пов'язаних із географічними координатами. Її головною особливістю є можливість поєднання аналітичної інформації з просторовим контекстом, що робить GIS ефективним інструментом у багатьох сферах, зокрема у цивільному захисті.

Використання GIS у системах управління надзвичайними ситуаціями дозволяє:

- візуалізувати місця виникнення подій на карті та оцінювати масштаби їхнього поширення;
- визначати зони ризику та потенційно небезпечні території;
- планувати оптимальні маршрути евакуації та підрозділів реагування;
- аналізувати просторово-часові тенденції появи надзвичайних подій;
- забезпечувати інтеграцію з іншими інформаційними ресурсами (бази даних, системи моніторингу, аналітичні модулі).

Окрім аналітичної функції, GIS виконує важливу роль на етапах реагування та ліквідації наслідків надзвичайних ситуацій. Вона дозволяє оперативно отримувати дані про обстановку, розташування об'єктів інфраструктури, комунікацій, евакуаційних шляхів і ресурсів. Це забезпечує ефективну координацію дій підрозділів, планування логістики та мінімізацію часу реагування. Таким чином, GIS виступає невід'ємним елементом інформаційної підтримки кризового управління.

У межах безпеко-орієнтованих інформаційних технологій GIS може виступати підсистемою візуалізації, яка забезпечує:

- перетворення результатів аналітичних розрахунків у зрозумілі карти та діаграми;
- підвищення інформативності звітів і презентацій для органів управління;
- підтримку процесу прийняття рішень у реальному часі.

Особливої актуальності набуває інтеграція GIS з аналітичними та прогнозними модулями, що базуються на ймовірнісно-статистичних методах. Такий підхід дозволяє створювати карти ризику, визначати ймовірність виникнення подій у певних регіонах, відображати результати статистичного аналізу у наочній геопросторовій формі. Це суттєво розширює можливості аналітика або керівника, який отримує не лише числові показники, а й їх візуальне представлення, що сприяє швидшому ухваленню управлінських рішень.

Впровадження GIS у практику цивільного захисту є важливим кроком у напрямі цифрової трансформації управління ризиками. Завдяки поєднанню просторового аналізу, моделювання сценаріїв розвитку подій і візуалізації ре-

зультатів GIS стає ключовим елементом системи ситуаційної обізнаності та основою для створення інтегрованих центрів управління безпекою.

Література

1. Harvard Ukrainian Research Institute. The Chernobyl/Chornobyl Project : MAPA Digital Atlas of Ukraine [Електронний ресурс] / Harvard Ukrainian Research Institute ; GIS-ресурс. – Cambridge, MA : Harvard Univ., 2022. – Режим доступу : https://www.gis.huri.harvard.edu/chornobyl ; дата звернення 15.11.2025.

2. Longley P. A., Goodchild M. F., Maguire D. J., Rhind D. W. Geographic Information Systems and Science : 3rd ed. – Chichester : Wiley, 2015. – 576 с.

3. Chang K. T. Introduction to Geographic Information Systems : 9th ed. - New York : McGraw-Hill, 2016.-656 с.

4. Keim D., Kohlhammer J., Ellis G., Mansmann F. Mastering ‘Big Data’ Visualization : Methods and Tools for Visual Analytics. – London : Springer, 2010. – 315 с.

5. Сівак В. І. Геоінформаційні системи у забезпеченні управління ризиками надзвичайних ситуацій : монографія. – Київ : Наук. думка, 2021. – 304 с.

УДК 004.681:004.451.28

СИСТЕМА ЦИФРОВОГО УПРАВЛІННЯ ПЕРСОНАЛОМ ОСВІТНЬОЇ УСТАНОВИ З ВИКОРИСТАННЯМ SPRING FRAMEWORK

Наталія СТЕПАНЧУК, Каріна ЖЕЛОНКІНА, Роман ГОЛОВАТИЙ
Львівський державний університет безпеки життєдіяльності

Анотація. *У роботі представлено розробку інформаційної системи управління кадровими процесами закладу освіти на основі Spring Framework. Система забезпечує автоматизацію обліку персоналу, підвищення ефективності адміністрування, безпеку даних та підтримку цифрової трансформації освітнього середовища.*
Ключові слова: *система управління кадрами, Spring Framework, заклад освіти, безпека даних, цифровізація, автоматизація.*

Abstract. *The paper presents the development of an information system for managing personnel processes in an educational institution using Spring Framework technologies. The system enhances personnel data automation, strengthens security, improves administrative efficiency, and supports the digital transformation of the educational environment.*
Keywords: *human resources management system, Spring Framework, educational institution, security, digital transformation, automation.*

Цифровізація сучасних освітніх установ висуває нові вимоги до ефективного управління кадровими процесами, що обумовлює необхідність впровадження комплексних інформаційних систем. Такі системи мають забезпечувати автоматизоване ведення кадрової документації, оперативний обмін інформацією між структурними підрозділами, контроль доступу до конфіденційних даних, інтеграцію з іншими сервісами закладу та підтримку аналітичних функцій для прийняття обґрунтованих управлінських рішень. Традиційні підходи до обліку персоналу – з використанням паперових носіїв або ізольованих електронних документів – вже не відповідають сучасним вимогам щодо швидкості обробки, точності та надійності даних. У цьому контексті створення єдиної цифрової системи управління кадровими процесами стає ключовим елементом модернізації управлінських процедур та підвищення ефективності роботи освітніх установ.

Spring Framework є однією з провідних платформ для розробки корпоративних систем на Java, що дозволяє реалізувати модульну, масштабовану та надійну архітектуру. Його екосистема включає Spring Boot, Spring Security та Spring Data JPA, що забезпечують повний життєвий цикл роботи з даними - від введення та перевірки інформації до її безпечного зберігання, обробки та формування звітності. Spring Boot стандартизує архітектуру застосунку та спрощує процес розгортання, тоді як Spring Data JPA гарантує стабільну роботу з реляційними базами даних, що є критично важливим для систем обліку персоналу та збереження кадрової інформації у структурованому вигляді.

Реалізація REST-орієнтованих інтерфейсів забезпечує уніфіковану взаємодію між клієнтськими додатками та серверною частиною, що дозволяє виконувати CRUD-операції, інтегрувати аналітичні модулі, документообіг та інші внутрішні сервіси закладу. REST API також сприяє масштабованості системи та полегшує її подальше розширення відповідно до потреб установи.

Оскільки облік персоналу передбачає роботу з конфіденційними даними співробітників, критично важливо впровадити надійні механізми автентифікації, авторизації та контролю доступу. Spring Security дозволяє захищати систему від поширених кіберзагроз, налаштовувати ролі користувачів, забезпечувати шифрування чутливої інформації та вести аудит дій користувачів, що підвищує прозорість процесів і забезпечує відповідність законодавчим вимогам щодо захисту персональних даних.

Розроблена система підтримує комплексне управління кадровою інформацією: ведення електронних особових карток, контроль кадрових документів, моніторинг змін у структурі персоналу, управління відпустками, контрактами та атестаціями, а також автоматизоване формування звітів і аналітичних даних. Вбудовані аналітичні модулі дозволяють прогнозувати кадрові потреби, оцінювати навантаження на співробітників, оптимізувати розподіл ресурсів та підтримувати прийняття обґрунтованих управлінських рішень.

Крім того, модульна архітектура системи дає змогу виділяти окремі компоненти для управління персоналом, документообігу, аналітики, авторизації та адміністративного контролю, що сприяє незалежному масштабуванню, інтеграції з іншими сервісами та використанню сучасних технологій контейнеризації і оркестрації, таких як Docker і Kubernetes. Це забезпечує високу гнучкість, адаптивність і готовність системи до подальшого розвитку, включаючи інтеграцію інтелектуальних аналітичних модулів, електронного документообігу та мобільних застосунків.

Таким чином, впровадження інформаційної системи управління кадровими процесами на базі Spring Framework дозволяє стандартизувати та автоматизувати облік персоналу, підвищити безпеку та точність даних, зменшити адміністративне навантаження та створити основу для комплексної цифрової трансформації освітніх установ.

Література

1. Walls C. Spring in Action. 6th ed. Shelter Island : Manning Publications, 2022. 520 p.

2. Spring Framework Documentation [Electronic resource]. Available at : https://spring.io/projects/spring-framework.

3. Spring Boot Reference Guide [Electronic resource]. Available at : https://docs.spring.io/spring-boot/docs/.

4. PostgreSQL Documentation [Electronic resource]. Available at : https://www.postgresql.org/docs/.

5. Fowler M. Patterns of Enterprise Application Architecture. Boston : Addison-Wesley, 2020. 533 p.

6. Richardson C. Microservices Patterns. Shelter Island : Manning Publications, 2019. 520 p.

7. ISO/IEC 27001:2022 Information security management systems - Requirements. Geneva : ISO, 2022. 35 p.

УДК 004:305

ГЕНДЕРНА РІВНІСТЬ У СВІТІ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ: ВИКЛИКИ ТА МОЖЛИВОСТІ

Олександр ТАНАСКОВ, Денис ІНКУЛЕЦЬ, Діана РАЙТА
Львівський державний університет безпеки життєдіяльності

Анотація. *У тезі розглянуто проблему гендерної нерівності в контексті розвитку інформаційних технологій. Показано, що цифрове середовище може як посилювати існуючі соціальні бар'єри, так і сприяти їх подоланню. Проаналізовано вплив STEM-освіти, алгоритмічних упереджень та цифрової безпеки на формування рівних можливостей. Окрему увагу приділено ролі етичного впровадження штучного інтелекту та розвитку цифрової грамотності. Зроблено висновок, що інформаційні технології є ключовим інструментом забезпечення гендерної рівності у сучасному суспільстві.*

Ключові слова: *гендерна рівність, інформаційні технології, штучний інтелект, алгоритмічні упередження, STEM-освіта, цифрова безпека.*

Annotation*. The thesis examines the issue of gender inequality in the context of the development of information technologies. It demonstrates that the digital environment can both reinforce existing social barriers and contribute to overcoming them. The influence of STEM education, algorithmic bias, and digital safety on equal opportunities is analyzed. Special attention is given to the ethical implementation of artificial intelligence and the development of digital literacy. It is concluded that information technologies play a key role in ensuring gender equality in modern society.*

Keywords: *gender equality, information technologies, artificial intelligence, algorithmic bias, STEM education, digital safety.*

Гендерна рівність залишається важливим фактором сталого розвитку суспільства, а сфера інформаційних технологій відіграє ключову роль у подоланні бар'єрів, що виникають унаслідок соціальних стереотипів та нерівного доступу до можливостей.

Незважаючи на швидке зростання цифрової економіки, жінки досі недостатньо представлені в IT-секторі, що зумовлено низкою соціальних, культурних та економічних чинників. Одними з найпоширеніших є гендерні стереотипи щодо «чоловічих» та «жіночих» професій, обмежений доступ до якісної технічної освіти, а також відсутність достатньої кількості рольових моделей, які б заохочували дівчат до вибору STEM-спеціальностей.

Економічний розрив у сфері інформаційних технологій проявляється у відмінностях рівня заробітної плати, нерівномірному представленні на керівних посадах та недостатній участі жінок у складних технічних напрямках, таких як розробка систем штучного інтелекту, кібербезпека чи інженерія даних. Зменшення цього розриву можливе за рахунок розвитку програм підтримки дівчат і жінок у технічних професіях, забезпечення рівних умов найму та створення інклюзивного корпоративного середовища, яке сприяє професійному зростанню незалежно від статі.

Важливим аспектом є вплив цифрових технологій на формування нових форм дискримінації. Алгоритмічні системи, зокрема моделі машинного

навчання, можуть відтворювати або навіть підсилювати гендерні упередження, якщо навчаються на нерепрезентативних чи історично упереджених даних. Приклади таких ризиків включають дискримінаційні рекомендаційні системи, алгоритми добору персоналу або системи оцінювання в онлайн-освіті. Тому розробка етичних підходів до створення інтелектуальних систем, впровадження алгоритмічного аудиту, контроль якості даних і забезпечення прозорості роботи моделей є стратегічними завданнями сучасної ІТ-спільноти.

Безпека цифрового середовища також має значний гендерний вимір. Жінки частіше стають жертвами кібербулінгу, переслідування в соціальних мережах, витоку приватних даних та інших форм онлайн-насильства. Це знижує рівень їхнього цифрового комфорту, стримує активну участь у публічному житті та формує додаткові бар'єри для професійного розвитку. Використання сучасних інструментів цифрової ідентифікації, технологій анонімізації, захищених каналів комунікації та автоматизованих систем модерації контенту сприяє створенню більш безпечного та інклюзивного онлайн-простору.

Окреме значення має розвиток цифрової грамотності та доступу до сучасних освітніх ресурсів. Освітні платформи, інтерактивні курси, симулятори та відкриті онлайн-системи дають змогу усунути бар'єри доступу до навчання, мотивувати дівчат до STEM, формувати цифрові навички та підвищувати конкурентоспроможність на ринку праці. Підтримка з боку держави, міжнародних організацій та ІТ-компаній є ключовою для створення середовища рівних можливостей.

Отже, інформаційні технології можуть виступати як фактором поглиблення гендерної нерівності, так і потужним інструментом її подолання. Етичне впровадження штучного інтелекту, розвиток інклюзивних корпоративних практик, зменшення цифрового розриву, розширення доступу до STEM-освіти та формування безпечного цифрового середовища — це основні кроки, необхідні для забезпечення гендерної рівності у сучасному цифровому суспільстві. Лише комплексний підхід, що об'єднує технологічні, освітні та соціальні рішення, здатен створити умови для рівного розвитку всіх учасників цифрової екосистеми.

Література

1. Смотр О.О. Використання інструментарію інформаційних технологій для підвищення мотивації студента до навчання у форматі змішаної освіти / О. Смотр, М. Рашкевич, Р. Головатий, Х. Мечус // Інформаційно-комунікаційні технології в сучасній освіті: досвід, проблеми, перспективи : Збірник наукових праць. Випуск 6. / За ред. М. С. Коваля, Н. Г. Ничкало. – Львів : ЛДУ БЖД, 2021. – С.214-217.

2. European Institute for Gender Equality. Gender Equality and Digitalisation in the European Union. Luxembourg: Publications Office of the European Union, 2020.

3. UNESCO. *Cracking the Code: Girls' and Women's Education in STEM*. Paris: UNESCO Publishing, 2017.

UDC 004.932

MATHEMATICAL AND COMPUTER MODELING OF PDF RENDERING IN WIDE-FORMAT PRINTING SYSTEMS BASED ON ADOBE PDF PRINT ENGINE

Roman TYNDYK
Lviv Polytechnic National University

Анотація. *Проведено дослідження математичного і комп'ютерного моделювання процесу рендерингу PDF у цифрових RIP-системах широкоформатного струменевого друку з використанням Adobe PDF Print Engine. Розкрито особливості обробки прозоростей, Device N-каналів і кольорових перетворень. Розроблено критерії оптимальності та наведено порівняльний аналіз основних рендеринг модулів таких як APPE з Ghostscript, Harlequin та CPSI.*

Ключові слова: *APPE, ONYX, PDF rendering, DeviceN, rasterization.*

Abstract. *A study of mathematical and computer modeling of the PDF rendering process in digital RIP systems for wide-format inkjet printing using Adobe PDF Print Engine was conducted. The features of transparency processing, DeviceN channels, and color conversions were revealed. Optimality criteria were developed and a comparative analysis of the main rendering modules such as APPE with Ghost script, Harlequin, and CPSI was presented.*

Keywords: *APPE, ONYX, PDF rendering, DeviceN, rasterization.*

In large-format printing systems, the accuracy of PDF file rendering determines the quality of interpretation of transparencies, overlay effects, multichannel DeviceN objects, and complex graphic structures. Traditional PostScript-oriented engines perform forced flattening, which causes the loss of correct layer interaction. In contrast, Adobe PDF Print Engine (APPE) implements direct modeling of the PDF structure, which ensures accurate mathematical reproduction of the composition model.

APPE is based on the Adobe Common Rendering Model, which describes a page as an ordered set of graphic objects, each of which retains its color space and transparency parameters [1]. The composition of transparent elements is performed without flattening, by calculating the total contribution of objects to the pixel value. Mathematically, the result at the coordinate (x,y) is described by equation (1):

$$I(x,y) = \sum_{i=1}^{n} C_i(x,y)\ \mathrm{A}_i(x,y) \qquad (1)$$

Here, $C_i(x,y)$ - is the color of the object in the source space (RGB, CMYK, or DeviceN), and $\mathrm{A}_i(x,y)$ -is the local transparency according to the Porter–Duff model. One of the advantages of APPE is that it preserves DeviceN

channels until the final rasterization, which eliminates errors inherent in Ghost script or CPSI, which usually convert them to CMYK at early stages [2].

ONYX systems use a step-by-step PDF processing model. First, objects are syntactically analyzed, after which they form a Display List — an internal representation of the page that reproduces the PDF structure without simplifications. At the color conversion stage, the ICC mapping function is applied (2):

$$C_{out} = f_{ICC}(C_{in}, P_{src}, P_{dst}), \quad (2)$$

where P_{src} and P_{dst} – are the source and destination profiles. This mapping ensures color consistency regardless of the type of source data. This provides *predictable color rendering*; *common logic for RGB/CMYK/DeviceN*; *avoidance of color shifts during conversion*. Final rasterization in ONYX is implemented using the tile method. Let the page be divided into *m* regions T_k; then the set of rasters is described as (3):

$$R = \bigcup_{k=1}^{m} T_k \quad (3)$$

Where R is the set of raster data for the page, and m is the number of tiles. This approach allows you to process large-format canvases without overloading the random access memory. In the final phase, the raster is converted into the printer's physical color space (*CMYK, CMYK+LcLm, CMYK+OGV*, or other extended configurations), preserving DeviceN until the final DOT pattern is generated. Thus, the dithering method provides a balance between color accuracy, memory efficiency, and performance, which is critical for high-quality large-format printing.

In the context of large-format printing, it is important to consider the differences between the main rendering engines. Ghostscript processes PDF in the context of a PostScript engine and performs forced flattening of transparencies, which causes loss of gradient smoothness and DeviceN inaccuracies. CPSI, the predecessor to APPE, is limited by partial support for PDF and the lack of full transparency groups. Harlequin demonstrates high speed and correct DeviceN processing, but has a different PDF execution philosophy than Adobe, which can lead to deviations in complex effects. The summary is presented in Table 1:

Table 1 – Comparative characteristics of render engines

Characteristics	*Type of render engines*			
	APPE	*Ghostscript*	*CPSI*	*Harlequin*
Transparency	Native	Flattening	Partial	Native
DeviceN	Complete	Partial	No	Complete
Color accuracy	High	Low	Average	High
Productivity	Average	High	Low	Very high
PDF/X support	Complete	Partial	Partial	Complete

The analysis shows that APPE provides the most accurate reproduction of complex PDF structures thanks to native support for transparencies and DeviceN. The mathematical rendering model, which combines multi-layer composition, ICC conversion, and tile rasterization, can be used for further computer simulation of printing processes, optimization of RIP pipelines, and prediction of possible color deviations in large-format production.

References

1. Tyndyk R. S. CIELAB color space as a basic model for prepress processes in image preparation. 91st International Scientific Conference of Young Scientists, Postgraduates, and Students "Scientific Achievements of Youth - Solving the Problems of Human Nutrition in the 21st Century" NUHT, Kyiv, April 7–11, 2025, p. 402.

2. Tyndyk R. S. Development of a model to effectively minimize the negative impact of large-format solvent printing. Ekologia i racjonalne zarządzanie przyrodą: edukacja, nauka i praktyka. Vol 2, 2023. P. 211-214. DOI:10.58246/MFDS3545

УДК 004.9

ІНФОРМАЦІЙНА СИСТЕМА УПРАВЛІННЯ БІБЛІОТЕЧНИМИ РЕСУРСАМИ У ЗАКЛАДІ ВИЩОЇ ОСВІТИ

Юлія ТИХА, Марта ТРУШ, Юлія НАЗАР
Львівський державний університет безпеки життєдіяльності

Розглянуто розробку інтелектуальної інформаційної системи управління бібліотечними ресурсами у ЗВО. Представлено функціональну архітектуру, механізми автоматизації та переваги впровадження. Показано можливості оптимізації бібліотечних процесів та підвищення якості обслуговування користувачів.

Ключові слова: *інформаційна система, автоматизація, бібліотечні ресурси, база даних, управління даними.*

The paper explores the development of an intelligent information system for managing library resources in a higher education institution. The system's architecture, automation mechanisms, and implementation benefits are presented. The solution improves resource accessibility and enhances user service efficiency.

Keywords: *information system, automation, library resources, database, data management.*

Стрімке зростання обсягу інформаційних ресурсів у закладах вищої освіти та посилення вимог до оперативного доступу до знань роблять традиційні бібліотечні процеси малоефективними. Сучасні бібліотеки стикаються з необхідністю обліку великої кількості електронних та друкованих видань, а

ручне керування фондами часто призводить до помилок, втрат інформації та затримок у видачі матеріалів. У цьому контексті цифрові системи управління бібліотечними ресурсами стають невід'ємною складовою освітнього середовища, забезпечуючи не лише оперативний пошук літератури та автоматизований облік примірників, але й бронювання, видачу та повернення книг, формування історії користування та адміністрування акаунтів користувачів.

Впровадження сучасної інформаційної системи дозволяє персоналізувати роботу з користувачами, надаючи студентам та викладачам індивідуальні акаунти з доступом до розширених функцій. Користувачі отримують можливість переглядати каталог у режимі реального часу, переглядати детальні картки видань із наявними рецензіями, залишати власні оцінки та коментарі, а також подавати заявки на бронювання та отримання літератури. Викладачі, окрім стандартного функціоналу, можуть подавати пропозиції щодо закупівлі нових видань, формувати списки рекомендованої літератури для груп студентів та планувати навчальні курси з урахуванням доступних ресурсів.

Особливу увагу приділено безпеці та контролю доступу: система реалізує розподіл ролей – «Адміністратор», «Бібліотекар», «Викладач» та «Студент». Це забезпечує високий рівень захисту даних та контроль над операціями користувачів. Адміністратор керує користувачами, їхніми правами доступу та структурою даних, що дозволяє централізовано управляти інформаційними потоками. Бібліотекар контролює наявність і стан примірників, обробляє заявки, змінює статуси видань та керує фондами. Студенти та викладачі отримують інтуїтивно зрозумілий інтерфейс для пошуку та замовлення ресурсів, що підвищує ефективність навчального процесу.

Запровадження цифрової системи зменшує адміністративне навантаження на персонал бібліотеки, мінімізує людський фактор і скорочує час обслуговування користувачів. Одночасно система забезпечує прозорість обліку та можливість формувати детальні статистичні дані. Аналітичні модулі дозволяють прогнозувати попит на літературу, планувати закупівлі, оптимізувати роботу бібліотеки та підтримувати стратегічне управління фондами. Особливо важливо, що система зберігає історію дій користувачів і операцій з примірниками, що створює умови для повного контролю і аналітики.

Технологічно система базується на клієнт-серверній архітектурі, що дозволяє масштабувати її відповідно до потреб закладу освіти. Використання мови програмування Java та реляційної СУБД MySQL забезпечує високу продуктивність, надійність та інтеграцію з іншими освітніми платформами. Архітектура передбачає модульність, що дозволяє додавати нові функції, такі як рекомендаційні алгоритми, мобільний доступ, інтеграцію з електронними журналами та освітніми ресурсами.

Перспективи подальшого розвитку системи включають впровадження мобільних додатків для дистанційного доступу, покращення алгоритмів рекомендаційного сервісу на основі аналізу історії користування, а також роз-

ширення аналітичних інструментів для підтримки управлінських рішень. Цифровізація бібліотечних процесів не лише підвищує ефективність роботи персоналу та доступність ресурсів, але й сприяє формуванню сучасного інтелектуального освітнього середовища, підвищенню інформаційної грамотності студентів та розвитку інноваційних підходів до навчання.

Таким чином, створена інформаційна система управління бібліотечними ресурсами є важливим кроком у цифровій трансформації бібліотек закладів вищої освіти, забезпечує оптимізацію процесів, інтеграцію з освітніми сервісами та сприяє формуванню ефективного, зручного та безпечного доступу до знань для всіх учасників навчального процесу.

Література

1. Бабенко, Л. М. Інформаційні системи та технології. Київ: Центр учбової літератури, 2020.

2. Коваленко, О. В. Сучасні бібліотечні інформаційні системи: теорія і практика. Харків: ХДАК, 2019.

3. Грінченко, С. С., Тюріна, Н. М. Автоматизація бібліотечних процесів у закладах освіти. Київ: Ліра-К, 2021.

4. Silberschatz, A., Korth, H., Sudarshan S. Database System Concepts. 7th ed. McGraw-Hill, 2020.

5. Sommerville, I. Software Engineering. 10th ed. Pearson, 2019.

6. Pressman, R. S., Maxim, B. R. Software Engineering: A Practitioner’s Approach. 9th ed. McGraw-Hill, 2020.

7. Connolly, T., Begg, C. Database Systems: A Practical Approach to Design, Implementation and Management. 6th ed. Pearson, 2015.

8. Литвин, В. В. Проєктування інформаційних систем. Львів: Новий Світ, 2018.

9. ISO 16439:2014. Methods and Procedures for Assessing the Impact of Libraries. International Organization for Standardization, 2014.

10. MySQL Documentation. MySQL 8.0 Reference Manual. Oracle, 2024.

11. Oracle. Java Platform, Standard Edition Documentation. Oracle, 2024.

УДК 004.8:004.932.4

РОЗРОБКА ВИСОКОДЕТАЛІЗОВАНОЇ 3D-МОДЕЛІ ПРОТЕЗУ НИЖНЬОЇ КІНЦІВКИ ДЛЯ ВИКОРИСТАННЯ В МЕДИЧНИХ ТА ОСВІТНІХ ВІЗУАЛІЗАЦІЯХ

Олена ТОВТ, Наталія ЖЕЗЛО-ХЛЕВНА
Львівський державний університет безпеки життєдіяльності, Львів

Анотація. *Розробка високодеталізованої 3D-моделі протезу нижньої кінцівки є актуальним напрямом у сфері медичних технологій, біомеханіки та освітніх симуляцій, оскільки сучасні протезні рішення потребують точного цифрового відтворення для навчання, аналізу та клінічної комунікації. Створення цифрових моделей забезпечує можливість демонстрації внутрішньої структури протеза, принципів роботи механізмів, а також оптимізації дизайну та адаптації під потреби пацієнтів.*

Ключові слова: 3D-моделювання, протезування, нижня кінцівка, біомеханіка, Blender, візуалізація, медичні симуляції.

Annotation. *The development of highly detailed 3D models of lower limb prostheses is a topical area in medical technology, biomechanics, and educational simulations, as modern prosthetic solutions require accurate digital reproduction for training, analysis, and clinical communication. The creation of digital models makes it possible to demonstrate the internal structure of the prosthesis, the principles of operation of the mechanisms, as well as to optimize the design and adapt it to the needs of patients.*

Keywords: 3D modeling, prosthetics, lower limb, biomechanics, Blender, visualization, medical simulations.

Сучасні освітні програми медичних та безпекоорієнтованих спеціальностей активно впроваджують цифрові технології для пояснення будови та принципів роботи протезних конструкцій. Традиційні методи презентації, такі як схеми та фото, не забезпечують достатнього ступеня деталізації, особливо коли йдеться про складні механічні вузли або матеріали. Використання високополігональних 3D-моделей дозволяє детально візуалізувати внутрішню структуру протеза, демонструвати поведінку компонентів під навантаженням та створювати анімації руху.

Розроблена 3D-модель протезу стегна включає основні конструктивні елементи: приймальну гільзу з гільзовим адаптером, вакуумний клапан, дубль-адаптер, колінний вузол, тримальний модуль та штучну стопу (рисунок 1). Структура моделі створена у Blender із використанням методів полігонального моделювання та скульптингу, що забезпечило високу деталізацію поверхонь та механізмів. Для покращення реалістичності застосовано процедурні матеріали та текстури, що імітують карбон, силікон та металеві сплави.

Рисунок 1 – 3D-модель стегного модульного протеза

Особлива увага приділена оптимізації полігональної сітки, оскільки надмірна кількість полігонів ускладнює подальше використання моделі у VR/AR-середовищах та інтерактивних навчальних платформах. Було застосовано ретопологію, яка дозволила зберегти форму та деталізацію, водночас зменшивши вагу моделі без втрати якості візуалізації. Також передбачена можливість експорту в медичні симулятори та навчальні програми завдяки підтримці форматів FBX, OBJ та GLTF.

Створена модель може використовуватися в медичних лекціях, курсах ортопедії та протезування, 3D-симуляторах, а також у процесі взаємодії лікаря з пацієнтом для демонстрації роботи протеза. Це розширює розуміння біомеханічних принципів, покращує якість освіти та сприяє підготовці фахівців у сфері протезування.

Література

1. Smith, J., & Brown, L. *Advanced Prosthetics Design and Biomechanics.* – Springer, 2020.

2. Blender Foundation. *Blender Documentation.* – [Електронний ресурс]. – Режим доступу: https://docs.blender.org.

3. Helgeson, M. *3D Modeling for Medical Visualization.* – CRC Press, 2019.

4. Жезло-Хлевна Н., Хлевной О., Назар Ю., Борзов Ю. & Довбняк В. (2025). Евакуація осіб із модульними протезами нижніх кінцівок при пожежі: сучасний стан, проблеми та перспективи досліджень. Пожежна безпека, 46, 53-64. ttps://doi.org/https://doi.org/10.32447/20786662.46.2025.05

УДК 004.9:614.8

ВИКОРИСТАННЯ МЕРЕЖЕВИХ МОДЕЛЕЙ (OSMNX + NETWORKX) ДЛЯ АНАЛІЗУ ТРАНСПОРТНОЇ ДОСТУПНОСТІ МІСЦЬ ДИСЛОКАЦІЇ ДОБРОВІЛЬНИХ РЯТУВАЛЬНИХ ФОРМУВАНЬ

Анатолій ТРИГУБА[1], Лілія КОВАЛЬ[2]

[1] Львівський національний університет ветеринарної медицини та біотехнологій імені С. З. Ґжицького

[2] Львівський державний університет безпеки життєдіяльності

У роботі запропоновано використовувати мережеві моделі на основі інструментів OSMnx та NetworkX для оцінювання транспортної доступності потенційних місць розміщення добровільних рятувальних формувань у сільських громадах. Запропоновано підхід до аналізу дорожньої інфраструктури, визначення ізохрон реагування та формування критеріїв вибору оптимальних локацій.

The paper proposes using network models based on OSMnx and NetworkX tools to assess the transport accessibility of potential locations for volunteer rescue teams in rural communities. An approach to analyzing road infrastructure, determining response isochrones, and forming criteria for selecting optimal locations is proposed.

Ефективне створення добровільних рятувальних формувань у сільських громадах потребує обґрунтованого вибору місць їх дислокації [1]. У сільській місцевості дорожня мережа, як правило, має нерівномірну структуру, що зумовлює значні відмінності у часі прибуття рятувальників до населених пунктів. Це потребує використання моделей, здатних точно враховувати топологію транспортної мережі, обмеження щодо швидкостей руху та реальні маршрути, доступні для оперативного транспорту [2].

Одним із найбільш придатних інструментів для такої задачі є поєднання бібліотек OSMnx та NetworkX, які дозволяють автоматично завантажувати дорожні графи з OpenStreetMap, проводити очищення та структурування даних, а також виконувати обчислення найкоротших шляхів та побудову ізохрон. Нехай дорожня мережа подається у вигляді орієнтованого графа:

$$G(V,E), \tag{1}$$

де V – множина вузлів; E – множина ребер з атрибутами довжини та швидкісних обмежень.

Час пересування між двома вузлами визначається за формулою

$$t_{ij} = \frac{d_{ij}}{v_{ij}}, \tag{2}$$

де t_{ij} – час проходження ділянки; d_{ij} – довжина ділянки транспортної мережі; v_{ij} – швидкість руху рятувальних формувань на відповідній ділянці транспортної мережі.

Використання формули (2) дає змогу формувати матрицю часової доступності, на основі якої визначаються території, що знаходяться в межах нормативного часу реагування. Це дозволяє перетворити геометричну мережу на метричний граф, оптимальний для задач оперативного реагування. Загальний час прибуття рятувального формування до пункту призначення $\tau(s,k)$ задається як мінімальна сума ваг маршруту між вихідною точкою s та населеним пунктом k:

$$\tau(s,k) = \min_{p \in P_{s,k}} \sum_{(i,j) \in p} t_{ij}, \quad (3)$$

де $P_{s,k}$ – множина всіх можливих маршрутів.

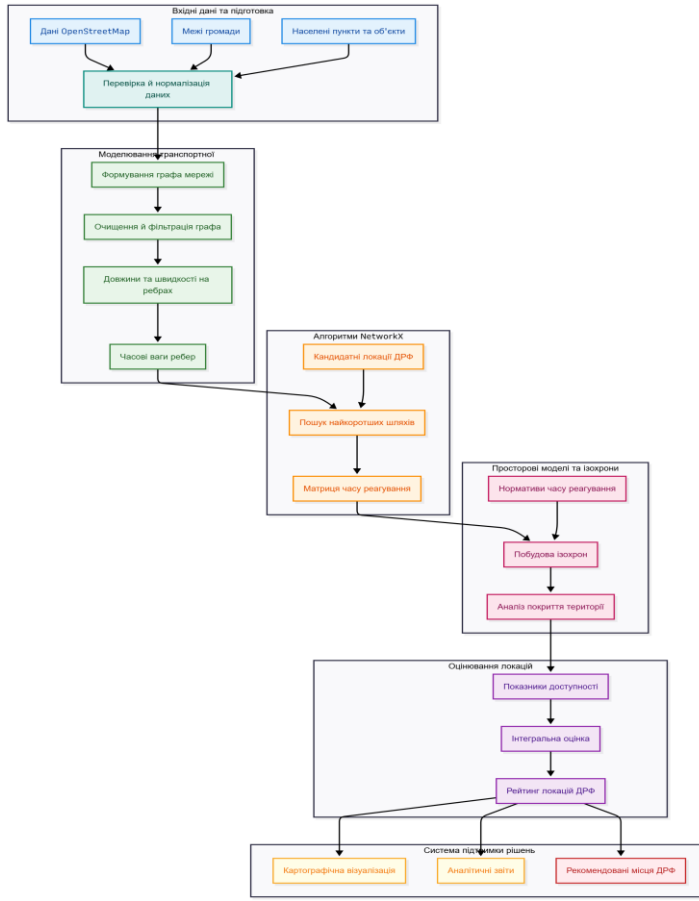

Рисунок 1 – Структурна схема моделі оцінювання транспортної доступності добровільних рятувальних формувань

Рівняння (3) реалізується через алгоритми Dijkstra або A*, що враховують реальну структуру мережі, транспортні обмеження і евристики.

Матриця часу реагування для громади позначається як:

$$T = [\tau(s,k)]_{S\times K}, \tag{4}$$

де S – набір потенційних локацій добровільного рятувального формування; K – множина населених пунктів.

Матриця (4) є основою для оцінювання доступності територій. Для кожної локації визначаються середній час реагування:

$$T_{\text{avg}} = \frac{1}{|K|}\sum_{k=1}^{|K|}\tau(s,k), \tag{5}$$

та максимальний час реагування

$$T_{\max} = \max_{k\in K}\tau(s,k), \tag{6}$$

Усе вище сказане дає змогу оцінити як загальну ефективність, так і найбільш уразливі зони громади. Частка території, охопленої в межах нормативного часу T_{norm}, визначається формулою:

$$P = \frac{|\{k \in K : \tau(s,k) \le T_{\text{norm}}\}|}{|K|}. \tag{7}$$

Інструментарій OSMnx дає змогу не лише завантажити дорожню мережу та виконати попередню обробку, але й побудувати ізохрони – зони, до яких рятувальне формування може дістатися протягом фіксованого часу. Ізохрони є ключовим елементом вибору локацій, адже вони відображають реальну геометрію досяжності, що неможливо отримати за допомогою евклідових відстаней.

На рисунку 1 подано узагальнену логічну структуру моделі оцінювання транспортної доступності місць дислокації добровільних рятувальних формувань, побудовану на основі мережевої інфраструктури та алгоритмів пошуку найкоротших шляхів.

Для кількісного оцінювання локації пропонується використати інтегральний критерій:

$$k = \alpha\cdot P - \beta\cdot T_{avg} - \gamma\cdot T_{max}, \tag{8}$$

де P – частка покриття; T_{avg} – середній час реагування на надзвичайні ситуації; T_{max} – максимальний час реагування на виклик серед усіх населених пунктів, які обслуговує добровільне рятувальне формування; α,β,γ – коефіцієнти, які задають ваги залежно від пріоритетів громади.

Отримані результати свідчать, що використання мережевих моделей на основі OSMnx і NetworkX дозволяє суттєво підвищити точність планування місць розташування добровільних рятувальних формувань. Поєднання дорожньої топології, даних про швидкісні режими та алгоритмів shortest path створює можливість моделювання різних сценаріїв реагування та обґрунтування управлінських рішень. Запропонована модель є універса-

льною і її можна адаптувати до процесів аналізу доступності медичних пунктів, пожежних депо чи пунктів гуманітарної допомоги.

Література

1. Tryhuba A., Ratushny R., Bashynsky O. and Shcherbachenko O. Identification of firefighting system configuration of rural settlements, Proceedings of the Fire and Enviromnental Safety Engineering. MATEC Web Conf. Volume 247 of FESE 2018. doi:10.1051/matecconf/201824700035

2. Tryhuba A., Ratushny R., Bashynsky O., Ptashnyk V. Development and Usage of a Computer Model of Evaluating the Scenarios of Projects for the Creation of Fire Fighting Systems of Rural Communities. Proceedings of the Xlth International Scientific and Practical Conference on Electronics and Information Technologies (ELIT 2019), Lviv, 2019, pp. 34-39. doi: 10.1109/ELIT.2019.8892320

УДК 005.8:620.9:681.3

ІНТЕЛЕКТУАЛЬНІ МЕХАНІЗМИ ЕНЕРГОМЕНЕДЖМЕНТУ В УПРАВЛІННІ СКЛАДНИМИ ЕНЕРГЕТИЧНИМИ ПРОЄКТАМИ

Анатолій ТРИГУБА[1], Олег АНДРУШКІВ[2],
Роман ОЛІЙНИК[2], Мар'ян КОЦИЛОВСЬКИЙ[1]
[1] Львівський національний університет ветеринарної медицини та біотехнологій імені С. З. Ґжицького
[2] Львівський державний університет безпеки життєдіяльності

У роботі розглянуто інтелектуальні механізми енергоменеджменту для підвищення ефективності управління складними енергетичними проєктами. Запропоновано моделі прогнозування, оцінювання ризиків та оптимізації енергетичних рішень із застосуванням цифрових технологій і методів штучного інтелекту.

The paper examines intelligent energy management mechanisms aimed at improving the efficiency of complex energy project management. Forecasting models, risk assessment methods, and optimization tools based on digital technologies and artificial intelligence are proposed.

В умовах трансформації енергетичного сектора особливої актуальності набуває науково-прикладна задача розроблення інтелектуальних механізмів енергоменеджменту, які дозволяють удосконалити управління складними енергетичними проєктами [1]. Реалізація таких проєктів відбувається в середовищі високої невизначеності, що зумовлена нестабільністю енергоринку, зростанням частки відновлюваних джерел, змінами у режимах споживання, а також впливом воєнних та надзвичайних чинників [2]. З огляду на це управління проєктами енергозабезпечення потребує інтеграції моделей прогнозування, оптимізаційних процедур і цифрових інструментів, здатних забезпечити системну підтримку прийняття рішень.

Основою інтелектуального енергоменеджменту є побудова математичної моделі енергетичної системи, що включає взаємопов'язані джерела, акумуляційні потужності та змінні профілі навантаження. У загальному вигляді динаміка енергобалансу визначається залежністю:

$$E(t) = P_г(t) - P_c(t) + P_a(t), \tag{1}$$

де $P_г(t)$ – виробництво (генерування) енергії різними джерелами; $P_c(t)$ – споживання енергії; $P_a(t)$ – надходження або відбір енергії з накопичувачів.

У разі формування оптимізаційної моделі обгрунтування конфігурації проєктів енергозабезпечення об'єктів, критерієм є мінімізація сукупних приведених витрат за весь життєвий цикл. Функцію мети можна подати у вигляді:

$$\min Z = \sum_{i=1}^{n} \left(C_i + O_i + R_i \right), \tag{2}$$

де C_i – капітальні витрати на впровадження підсистеми; O_i – операційні витрати; R_i – витрати на резервування та забезпечення стійкості.

Умови стійкого функціонування енергетичної системи доповнюються обмеженнями:

$$P_c(t) + P_a^+(t) \geq P_c(t) + P_a^-(t), \quad (3)$$

$$0 \leq SOC(t) \leq SOC_{\max}, \quad (4)$$

де $SOC(t)$ – рівень заряду акумуляторної системи.

Ефективність інтелектуальних механізмів енергоменеджменту значною мірою залежить від якості інформаційної підтримки. Важливою складовою є отримання достовірних даних щодо навантаження, погодних умов, технічного стану обладнання та прогнозних моделей [3]. Для опису структури даних доцільно використати узагальнену таблицю 1, що наведена нижче.

Таблиця 1 – Основні групи даних для енергоменеджменту складних енергетичних проєктів

Категорія даних	Опис	Джерело
Енергетичні показники	Профіль генерації, споживання, пікові навантаження	Лічильники, SCADA
Погодні параметри	Радіація, температура, швидкість вітру	Метеостанції, супутники
Технічні характеристики	Паспортні дані обладнання, параметри деградації	Виробник, технічні журнали
Показники ризику	Інтенсивність загроз, відмови, аварійність	Оперативні дані, аналітика

Системність управління складними енергетичними проєктами забезпечується впровадженням цифрових двійників, які дозволяють поєднувати фактичні дані з аналітичними моделями. Цифровий двійник формує віртуальну копію об’єкта, де відтворюється поведінка системи у реальному або наближеному до реального часі. На рисунку 1 наведено загальну концепцію цифрового двійника для енергетичної системи.

Рисунок 1 – Концептуальна схема цифрового двійника енергетичного об’єкта

У процесі функціонування цифровий двійник виконує прогнозування навантаження через методи машинного навчання. Узагальнена модель регресійного прогнозу може бути подана залежністю:

$$\bar{P}(t+1) = f\left(P(t), W(t), T(t), SOC(t)\right), \quad (5)$$

де $W(t)$ – вітрові показники; $T(t)$ – температура навколишнього середовища; $f(\cdot)$ функція, яка базується на основі нейронної мережі, градієнтного бустингу або гібридної моделі.

Управлінські рішення у складних енергетичних проєктах часто залежать від оптимального розподілу потужності між джерелами та накопичувачами. Для оцінки рішень використовується критерій стійкості, який можна описати через функцію ризику:

$$R = \sum_{j=1}^{m} p_j \cdot L_j, \quad (6)$$

де p_j – ймовірність події, L_j – втрати, що виникають у разі її настання. Цей критерій дозволяє визначити необхідний рівень резервування та підвищити стійкість системи до зовнішніх впливів.

У разі впровадження циркуляційних моделей управління системи енергозабезпечення переходять від ієрархічної до децентралізованої структури. Важливою особливістю такого підходу є залучення локальних енергетичних підсистем, які можуть функціонувати автономно або у складі мікромережі. Для опису структури такої підсистеми використано схему, подану на рисунку 2.

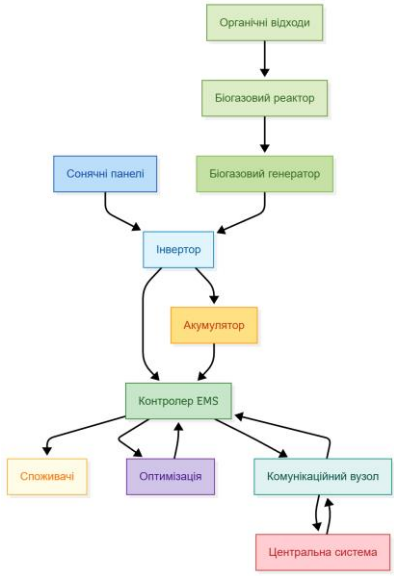

Рисунок 2 – Узагальнена структура децентралізованої енергетичної підсистеми з використанням органічних відходів

Важливою складовою інтелектуальних механізмів є аналітичні моделі оцінювання ефективності проєкту. Для цього застосовують показник інтегральної ефективності:

$$I = \alpha E_{ек} + \beta E_{ен} + \gamma E_{ст}, \quad (7)$$

де $E_{ек}$ – економічний ефект; $E_{ен}$ – енергетичний ефект; $E_{ст}$ – показник стійкості; α, β, γ – показники, що задають залежно пріоритети проєкту.

Таким чином, інтелектуальні механізми енергоменеджменту становлять сукупність математичних моделей, цифрових аналітичних інструментів та систем підтримки прийняття рішень, що дозволяють підвищити ефективність управління складними енергетичними проєктами. Їх застосування забезпечує можливість адаптивного планування, зменшення невизначеності та зростання стійкості енергетичних систем у сучасних умовах.

Література

1. Tryhuba, A., Hutsol, T., Čėsna, J., Tryhuba, I. Optimizing energy systems of livestock farms with computational intelligence for achieving energy autonomy. Scientific Reports, 2025, 15(1). DOI: https://doi.org/10.1038/s41598-025-92836-6

2. Tryhuba, A., Mudryk, K., Tryhuba, I., Kotsylovskyi, M. Models for sustainable management of livestock waste based on neural network architectures. Scientific Reports, 2025, 15(1). DOI: https://doi.org/10.1038/s41598-025-13150-9

3. Тригуба І.Л., Маланчук О.М., Татомир А.В., Коциловський М.П., Андрушків О.Я. Інформаційно-аналітична модель оцінення ресурсного потенціалу для реалізації проєктів енергозабезпечення домогосподарств. Міжнародна науково-практична конференція «Інформаційні системи та інноваційні технології управління проєктами і програмами» (Харків–Коблево, 15–20 верес. 2025 р.). Збірник праць. Харків: ХНУРЕ, 2025. С. 282-286.

УДК 005.8:614.2

ОСОБЛИВОСТІ ІНТЕЛЕКТУАЛЬНО-ЦІННІСНОГО УПРАВЛІННЯ ПРОЄКТАМИ РОЗВИТКУ МЕДИЧНОЇ ІНФРАСТРУКТУРИ

Анатолій ТРИГУБА[1], Роксолана ШОЛУДЬКО[2]
[1] Львівський національний університет ветеринарної медицини та біотехнологій імені С. З. Ґжицького
[2] Львівський державний університет безпеки життєдіяльності

У роботі представлено інтелектуально-ціннісну модель управління проєктами розвитку медичної інфраструктури громад. Запропоновано інтеграцію цифрових двійників, просторового аналізу та багатокритеріальної оцінки для формування обґрунтованих управлінських рішень щодо оптимізації мережі медичних закладів.

The paper presents an intellectual value model for managing community medical infrastructure development projects. It proposes the integration of digital twins, spatial analysis, and multi-criteria assessment to form informed management decisions on optimizing the network of medical facilities.

Теперішній розвиток медичної інфраструктури в умовах територіальної децентралізації та соціально-економічних викликів потребує нових підходів до планування й реалізації проєктів [1]. Інтелектуально-ціннісне управління передбачає поєднання технічних, соціальних і безпекових критеріїв, що визначають реальну важливість медичного об'єкта для громади. Традиційні підходи, орієнтовані переважно на кошторисну вартість та строки реалізації, виявляються недостатніми, адже вони не враховують пріоритетності послуг, логістичної доступності, стійкості інфраструктури та ризиків надзвичайних ситуацій [2]. Зазначений підхід базується на поєднанні цифрових технологій, алгоритмів штучного інтелекту та механізмів експертного оцінювання.

Особливим компонентом інтелектуально-ціннісної системи є бальна модель оцінювання проєктів, що інтегрує кілька ключових показників. Загальний індекс ефективності пропонується визначати за формулою:

$$I = w_1 A + w_2 S + w_3 R^{-1} + w_4 C \qquad (1)$$

де A – показник доступності медичних послуг; S – соціальна цінність, у тому числі значущість послуги для різних груп населення; R^{-1} – обернений показник ризику, що характеризує стійкість об'єкта; C – інфраструктурна та технічна готовність закладу; w_i – вагові коефіцієнти, визначені експертним методом або нечіткою логікою.

Ціннісні чинники формуються на основі експертного опитування, анкетування населення та аналізу локальних стратегій розвитку [3]. Соціальна

значущість медичних послуг має багатовимірну природу й охоплює такі аспекти, як вплив закладу на якість життя, безпековий потенціал, важливість для демографічно вразливих груп та відповідність стандартам МОЗ.

Оцінювання ризиків проводиться в інтеграції з цифровим двійником, що дає змогу врахувати можливі пікові навантаження, сезонні коливання та зміни в інфраструктурі громади. Модель дозволяє оцінити не лише ризик відмови системи, але й здатність медичного об'єкта забезпечувати безперервність послуг під час надзвичайних ситуацій.

Структура інтелектуально-ціннісної системи представлена на рисунку 1 у вигляді логічної взаємодії основних її модулів.

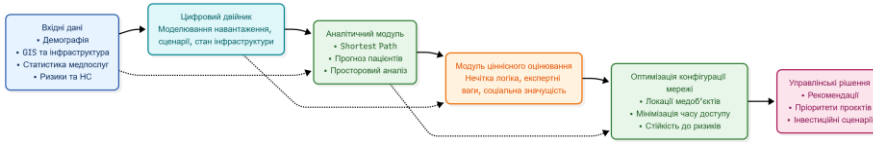

Рисунок 1 – Структурна схема інтелектуально-ціннісної системи управління проєктами розвитку медичної інфраструктури

Систематизація основних критеріїв, що визначають управлінські рішення щодо розвитку медичних об'єктів, подана в таблиці 1.

Таблиця 1 – Основні критерії оцінювання медичних інфраструктурних проєктів

Критерій	Зміст	Джерело даних
Доступність	Час прибуття пацієнтів	GIS, моделі shortest path
Соціальна цінність	Важливість послуги для громади	Експертні інтерв'ю
Ризики	Вразливість до НС та пікових навантажень	Цифровий двійник
Інфраструктурний стан	Технічна готовність закладу	Аудит, паспортизація

Показник доступності описує реальний час прибуття пацієнтів до медичного закладу. Використання даних GIS і алгоритмів shortest path. Соціальна цінність відображає важливість медичних послуг для населення, включаючи їх значущість для різних вікових та соціальних груп. Ризики визначають стійкість медичного закладу до пікових навантажень та можливих надзвичайних ситуацій. Інфраструктурний стан характеризує технічну готовність медичного об'єкта, включно з якістю будівель і технічного оснащення. Дані аудиту та паспортизації є ключовими для розуміння того, наскільки заклад може забезпечити стабільну роботу та витримувати додаткові навантаження.

Інтелектуально-ціннісна система управління забезпечує перехід від статичного планування до адаптивного розвитку медичних мереж. Її перевага полягає у здатності поєднувати об'єктивні просторові та статистичні показники з експертними оцінками цінностей, формуючи комплексне бачення розвитку інфраструктури. Завдяки цьому громади отримують інструмент, що дозволяє приймати обґрунтовані рішення, спрямовані на підвищення доступності, якості й безпеки медичних послуг.

Література

1. Tryhuba, A., Malanchuk, O., Tryhuba, I., Sholudko, R. & Seleznov, R. "A model for optimizing the portfolio of hospital district development projects based on a genetic algorithm". IEEE 19th International Conference on Computer Sciences and Information Technologies (CSIT-2024). Lviv, Ukraine. IEEE; 2024. p. 1–4. DOI: https://doi.org/10.1109/CSIT65290.2024.10982562.

2. Tryhuba, A., Malanchuk, O., Tryhuba, I. & Marmulyak, A. "Decision support system for initiating projects of medical and social development in regions". Proceedings of the 5th International Workshop on IT Project Management (ITPM 2024). Bratislava, Slovakia. May 22, 2024. p. 204–218. URL: https://ceur-ws.org/Vol-3709/paper17.pdf.

3. Malanchuk, O., Tryhuba, A., Tryhuba, I., Sholudko, R. & Pankiv, O. "A neural network model-based decision support system for time management in pediatric diabetes care projects". IEEE 18th International Conference on Computer Sciences and Information Technologies (CSIT-2023). Lviv, Ukraine. IEEE; 2023. p. 1–4. DOI: https://doi.org/10.1109/CSIT61576.2023.10324014.

УДК 004.9:628.4

ІНТЕЛЕКТУАЛЬНА ЕКОСИСТЕМА УПРАВЛІННЯ ОРГАНІЧНИМИ ВІДХОДАМИ

Інна ТРИГУБА[1], Назарій КОВАЛЬ[2], Ігор ФІРМАН[2], Володимир ФАМУЛЯК[1]

[1] Львівський національний університет ветеринарної медицини та біотехнологій імені С. З. Ґжицького

[2] Львівський державний університет безпеки життєдіяльності

У роботі обґрунтовано інтелектуальну екосистему управління органічними відходами, що поєднує методи прогнозування ризиків, цифровий моніторинг та моделі оптимізації циркуляційних потоків. Запропоновано структурну модель екосистеми та аналітичні залежності для оцінювання потенціалу відходів.

The paper proposes an intelligent ecosystem for organic waste management integrating risk prediction models, digital monitoring and optimization tools. A structural architecture and analytical models for assessing waste potential are presented.

Формування інноваційних підходів до управління органічними відходами стає основним напрямом екологічної політики громад. Зростання обсягів побутових, харчових і агровиробничих відходів збільшує навантаження на інфраструктуру та підвищує ризики забруднення ґрунтів, води й повітря, а також ускладнює санітарно-епідеміологічну ситуацію. Традиційні моделі утилізації не забезпечують необхідної адаптивності та не дозволяють ефективно реалізувати енергетичний і біотехнологічний потенціал органічних відходів. Тому виникає потреба у створенні інтелектуальної екосистеми, яка інтегрує штучний інтелект, цифровий моніторинг, прогнозування екологічних ризиків та оптимізацію циркуляційних потоків ресурсів. *Інтелектуальна екосистема управління органічними відходами* – це інтегрований цифровий комплекс, що об'єднує моделі штучного інтелекту, інформаційні системи, сенсорні дані та управлінські сервіси з метою оптимізації процесів збору, переробки, логістики та прогнозування екологічних ризиків у циркуляційній системі органічних відходів на рівні громади чи регіону (рис. 1).

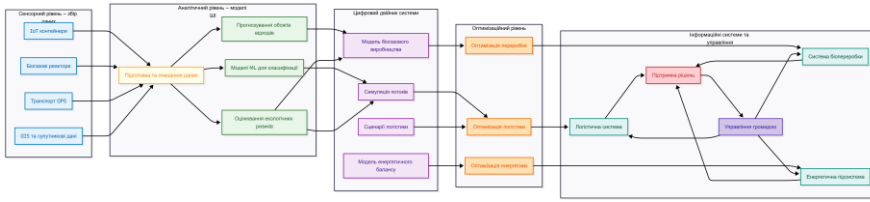

Рисунок 1 – Інтелектуальна екосистема управління органічними відходами

Основу екосистеми формує багаторівнева архітектура, у межах якої кожен рівень виконує специфічні функції. На первинному рівні відбувається збір даних за допомогою сенсорних мереж, які встановлюються на контейнерах збору органічних відходів, у біогазових реакторах, на майданчиках сортування та у транспортних засобах, що здійснюють логістичні операції. Сенсори об'єднані в єдину інформаційну підсистему через LoRaWAN, NB-IoT або MQTT та забезпечують можливість дистанційного відстеження стану об'єктів у режимі реального часу.

Другий рівень екосистеми представлений аналітичними та математичними моделями оцінювання екологічних ризиків. Однією з основних задач є прогнозування ймовірності настання негативних подій, таких як перевищення концентрації шкідливих речовин, утворення токсичних сполук у процесах анаеробного бродіння або порушення санітарних параметрів зберігання відходів. Для цього використовується модель інтегрального ризику, яка може бути визначена залежністю:

$$R = P(E) \cdot S(E), \tag{1}$$

де R – рівень ризику; $P(E)$ – ймовірність настання екологічної події E; $S(E)$ – обсяги її потенційних наслідків.

У межах екосистеми величина $P(E)$ визначається за допомогою алгоритмів машинного навчання, зокрема методів градієнтного бустингу, GCN-моделей та рекурентних мереж для обробки часових рядів. Значення $S(E)$ формується на основі нормованих показників забруднення та експертних оцінок.

Третій рівень інтелектуальної екосистеми представлений модулем цифрового двійника. Цей модуль забезпечує симуляцію руху органічних відходів, сценарії логістики їх транспортування, зміни параметрів біогазового виробництва, варіанти енергетичного використання та вплив управлінських рішень на рівень ризиків. Цифровий двійник дозволяє моделювати процеси аеро- та анаеробної стабілізації відходів, а також розраховувати енергетичний потенціал на основі формули:

$$E = m \cdot q \cdot k, \tag{2}$$

де m – маса органічних відходів; q – теплотворна здатність; k – коефіцієнт ефективності перетворення.

Залежно від характеристик субстрату та технологічного циклу цей показник дозволяє визначати оптимальні режими роботи біореакторів і баланс енергії в локальних мікромережах.

Четвертий рівень екосистеми включає оптимізаційний модуль, побудований на методах багатокритеріальної оптимізації. Він формує оптимальні траєкторії руху транспортних засобів, плани переробки та енергетичного використання органічних ресурсів. Процедура оптимізації включає цільову функцію:

$$F = w_1 C + w_2 T + w_3 R, \quad (3)$$

де C – витрати на логістику; T – тривалість переробки; R – інтегральний рівень ризику, w_i – вагові коефіцієнти.

Розв'язання оптимізаційної задачі здійснюється із застосуванням методів еволюційних алгоритмів, зокрема генетичних стратегій та мурашиних алгоритмів.

Сукупність розглянутих компонентів створює інтелектуальну екосистему, здатну адаптуватися до змін зовнішнього середовища, враховувати екологічні ризики та забезпечувати ефективне використання потенціалу органічних відходів. Такий підхід формує підґрунтя для сталого розвитку громад, підвищення енергетичної автономності та зменшення негативного впливу на довкілля.

Література

1. Tryhuba I., Tryhuba A., Hutsol T., Szufa S., Glowacki S., Andrushkiv O., Padyuka R., Faichuk O., Slavina N. European Green Deal: Substantiation of the Rational Configuration of the Bioenergy Production System from Organic Waste. Energies. 2024. Vol. 17, No. 17. Article 4513. DOI: https://doi.org/10.3390/en17174513

2. Tryhuba I., Tryhuba A., Hutsol T., Lopushniak V., Cieszewska A., Andrushkiv O., Barabasz W., Pikulicka A., Kowalczyk Z., Vasyuk V. European Green Deal: Justification of the Relationships between the Functional Indicators of Bioenergy Production Systems Using Organic Residential Waste Based on the Analysis of the State of Theory and Practice. Energies. 2024. Vol. 17, No. 6. Article 1461. DOI: https://doi.org/10.3390/en17061461

УДК 004.42

АВТОМАТИЗОВАНА СИСТЕМА ПЛАНУВАННЯ ТА РОЗПОДІЛУ СЛУЖБОВИХ ЧЕРГУВАНЬ (НАРЯДІВ)

Назарій ФЕДЕЦЬ, Юлія НАЗАР
Львівський державний університет безпеки життєдіяльності

У роботі представлено автоматизовану систему планування та розподілу службових чергувань (нарядів). Розроблене рішення автоматизовує процес, підвищує ефективність організації служби, мінімізує вплив людського фактора та забезпечує рівномірний розподіл навантаження на курсантів. Система реалізована як fullstack-рішення з використанням Java та JavaFX.

***Ключові слова**: алгоритм, службове чергування (наряд), JavaFX, інтерфейс.*

The paper presents an automated system for planning and distributing duty shifts (assignments). The developed solution automates the process, increases the efficiency of service organization, minimizes human influence, and ensures an even distribution of workload among cadets. The system is implemented as a full-stack solution using Java and JavaFX.

***Keywords:** algorithm, duty shift (assignment), JavaFX, interface.*

Сучасна практика організації несення служби, що базується на ручному плануванні та розподілі чергувань серед особового складу, є застарілим та неефективним підходом. До основних проблем належать вплив людського фактора та імовірність виникнення помилок при формуванні графіків, що призводить до неефективності службової діяльності. Крім того, традиційний підхід ускладнює забезпечення об'єктивного та рівномірного розподілу нарядів, що є вкрай важливо для забезпечення хорошого мікроклімату у колективі.

Актуальним завданням є створення автоматизованої системи, яка забезпечить рівномірний розподіл чергувань відповідно до встановлених вимог і норм.

Саме тому метою роботи є створення програмного рішення, яке автоматизує процес розподілу чергувань серед особового складу, з урахуванням усіх службових норм, та надасть користувачам інтуїтивно зрозумілий графічний інтерфейс.

Розробка програмного рішення здійснена на базі мови програмування Java. Для забезпечення кросплатформного та функціонального графічного інтерфейсу користувача використано бібліотеку JavaFX. Архітектура проекту ґрунтується на принципах об'єктно-орієнтованого програмування (ООП), що забезпечує модульність, розширюваність та гнучкість системи.

Візуальна частина розроблена у середовищі Scene Builder з використанням FXML. Інтерфейс оформлений у сучасному стилі за допомогою CSS.

Система розподілу чергувань реалізована з урахуванням ключових ролей користувачів: Адміністратора та Особового складу (Користувача), кожна з яких має відповідний функціонал.

Адміністративний модуль підтримує два ключові режими роботи для управління графіком чергувань, зокрема це – автоматичний режим (розподіл нарядів здійснюється системою автоматично на основі реалізованого алгоритму) та ручний (адміністратор може вносити прямі корективи до сформованого графіку, включаючи призначення, видалення або заміну чергувань).

Алгоритм розподілу чергувань полягає в рівномірному розподілі навантаження між особовим складом з урахуванням усіх норм. Кожний користувач має лічильник кількості відслужених чергувань. При формуванні нового графіка система надає перевагу тим, у кого найменший показник, забезпечуючи тим самим справедливий розподіл. Алгоритм враховує обмеження щодо кількості чергувань на добу та повторних призначень на одну дату.

На рисунку 1 зображений функціонал адміністратора для розподілу нарядів в автоматичному режимі. Для того, щоб його викликати достатньо натиснути кнопку «Розподілити наряди».

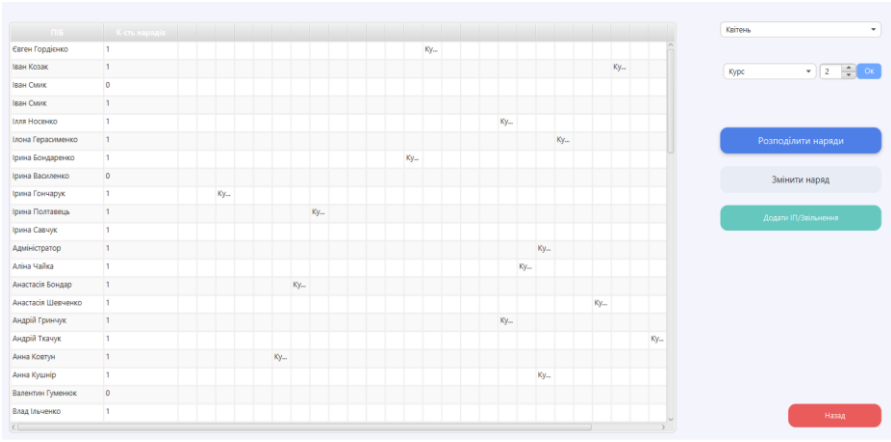

Рисунок 1 – Автоматичний режим розподілу чергувань

Кнопка «Змінити наряд» направляє адміністратора у ручний режим, де він зможе добавити ті, чи інші зміни. Приклад роботи ручного режиму зображений на рисунку 2.

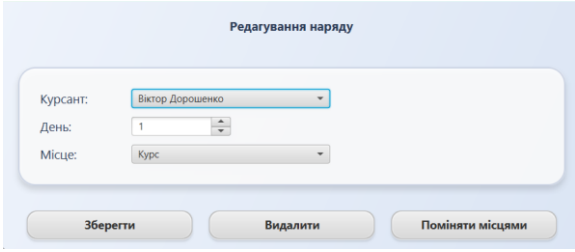

Рисунок 2 – Ручний режим розподілу чергувань

Інтерфейс користувача забезпечує особовому складу можливість переглядати графік чергувань (Рисунок 3), а також подавати заявки на зміну чи заміну наряду, які надалі підлягають на розгляд та затвердження адміністратору системи (Рисунок 4).

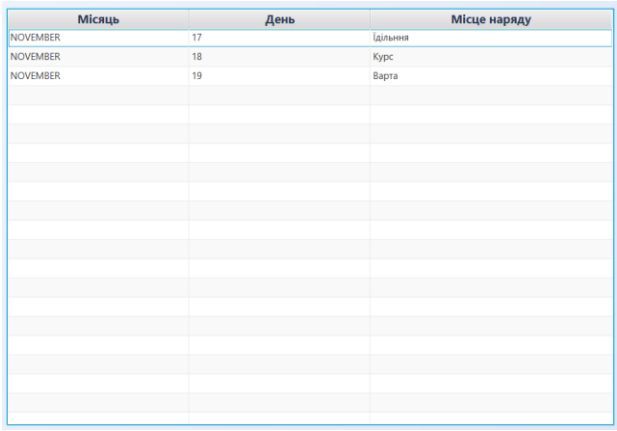

Рисунок 3 – Інтерфейс користувача

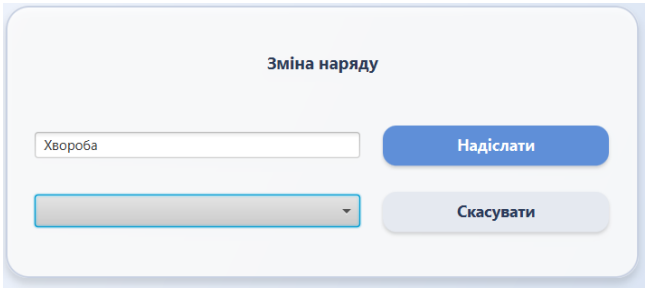

Рисунок 4 – Заявка на зміну чергування

Таким чином, розроблена система автоматичного розподілу нарядів забезпечує справедливе та рівномірне планування чергувань, усуває людський фактор і підвищує ефективність організації служби. Використання алгоритму для розподілу нарядів та JavaFX дозволило створити сучасний, зручний і функціональний інтерфейс, що підтримує як автоматичний, так і ручний режими роботи. Запропоноване рішення може бути впроваджене в практичну діяльність підрозділів для оптимізації розподілу навантаження та покращення управлінських процесів.

Література:

1. Основи програмування (мовою Java) : курс лекцій / Придатко О., Хлевной О., Бурак Н. – Львів : ЛДУ БЖД, 2019. – 180 с.

2. Придатко О. В., Бурак Н. Є., Дзень В. Є., Кунинець М. С. Адаптивна інформаційно-довідкова система "UniBell" як складова частина проєкту "Smart-університет". Науковий вісник НЛТУ України. 2020, т. 30, № 5. С. 113–121.

3. Head First Java / Kathy Sierra, Bert Bates. – «O'REILLY», 2012. – 678 с.

4. Kordunova Y., Prydatko O., Smotr O., Golovatyi R. Expert Decision Support System Modeling in Lifecycle Management of Specialized Software. Lecture Notes on Data Engineering and Communications Technologies, Springer, Switzerland. Vol. 149, 2022, pp. 367-383, https://doi.org/10.1007/978-3-031-16203-9_22

ВИЯВЛЕННЯ ВИСОКОРИЗИКОВИХ ПОВЕДІНКОВИХ ПРОФІЛІВ ЗА ДАНИМИ ЗІ СКРІНШОТІВ ВСТАНОВЛЕНИХ ЗАСТОСУНКІВ

Тарас ФЕДИНИШИН, Ольга ПАРТИКА
Національний університет «Львівська політехніка»

Abstract*. This study analyzes installed mobile applications from 477 screenshots provided by 100 users to identify behavioral patterns relevant to digital forensics. Clustering, risk-oriented app analysis, and persona profiling reveal two distinct user groups, including one with elevated digital risk. Results demonstrate the value of app-ecosystem patterns for forensic assessment.*

Keywords*: mobile forensics; behavioral profiling; installed applications; user clustering; digital risk assessment; smartphone analysis; app ecosystem; risk indicators; forensic intelligence; persona modeling.*

Анотація*. У дослідженні проаналізовано 477 скріншотів встановлених застосунків 100 користувачів з метою виявлення поведінкових моделей. Групування, оцінка ризикових застосунків та формування поведінкових профілів показали наявність двох відмінних груп, одна з яких має підвищений цифровий ризик.*

Ключові слова*: мобільна криміналістика; встановлені застосунки; поведінкове профілювання; групування користувачів; цифровий ризи; екосистема застосунків; ризикові категорії; поведінкові профілі.*

Сучасні мобільні пристрої формують унікальний цифровий слід користувача, який може бути використаний для криміналістичного аналізу поведінкових моделей [1] та виявлення потенційно ризикових осіб [2]. Набори встановлених застосунків відображають [3] інтереси, звички, рівень цифрової культури та навіть ставлення користувача до конфіденційності чи фінансових інструментів [4]. У цьому дослідженні проаналізовано 477 скріншотів, зібраних від 100 анонімних студентів, що містять списки встановлених мобільних застосунків. На основі цих даних сформовано структурований датасет, який дозволив застосувати методи кластеризації, ентропійного аналізу, оцінки ризикових застосунків та побудови поведінкових профілів. Дослідження спрямоване на розробку підходу до криміналістичного аналізу образів мобільних пристроїв через виявлення патернів використання застосунків, co-occurrence-зв'язків і формування "persona profiles". Отримані результати демонструють можливість використання екосистеми встановлених застосунків як джерела цифрових поведінкових індикаторів для подальших завдань кіберфорензіки та оцінки потенційно небезпечних користувачів.

Метою дослідження є розроблення та апробація підходу до криміналістичного аналізу мобільних пристроїв на основі структурованої інформації про встановлені застосунки, що дозволяє ідентифікувати поведінкові патерни користувачів та виявляти потенційно ризикові профілі.

Для досягнення поставленої мети визначено такі завдання дослідження:

1. Зібрати та сформувати анонімний датасет, що містить скріншоти списків застосунків і перетворити його у структуровану таблицю «користувач – застосунок – категорія».
2. Виконати кластерний аналіз користувачів за пропорціями категорій застосунків для виявлення природних поведінкових груп.
3. Виділити групи високоризикових застосунків (VPN, cryptocurrency, dev-tools, secure messaging) та інтегрувати їх у єдиний поведінковий risk score.
4. Сформувати persona profiles кожного кластера для криміналістичної інтерпретації виявлених поведінкових моделей.

У межах роботи здійснено збирання 477 анонімних скріншотів зі списками встановлених застосунків від 100 користувачів. Зображення були перетворені у структурований датасет формату «користувач – застосунок – категорія». На основі цих даних виконано кілька етапів аналізу. По-перше, проведено кластеризацію користувачів за пропорціями категорій застосунків для виявлення природних поведінкових груп. По-друге, сформовано типологію застосунків через аналіз співзустрічей (bigrams) для визначення характерних патернів використання. По-третє, обчислено ентропію Шеннона для оцінки різноманіття застосунків кожного користувача. Додатково виділено групи високоризикових застосунків (VPN, криптогаманці, dev-tools, secure-messaging) та розраховано інтегральний поведінковий risk score. На завершальному етапі побудовано persona profiles для кожного кластера з метою криміналістичної інтерпретації отриманих поведінкових моделей.

У дослідженні сформовано структурований набір даних із 477 скріншотів, де всі мобільні застосунки класифіковано за категоріями. Аналіз із використанням методів групування виявив дві чіткі поведінкові групи користувачів: першу — з переважанням соціальних мереж, месенджерів і мультимедійних сервісів, та другу — з підвищеною часткою засобів обходу обмежень, криптовалютних застосунків і технічних інструментів. На основі ризикових категорій розраховано інтегральний показник поведінкового ризику, який суттєво відрізняється між двома групами та підтверджує існування користувачів із підвищеним цифровим ризиком. Для кожної групи сформовано типові поведінкові портрети, які спрощують криміналістичну інтерпретацію та дають змогу проводити первинне виявлення потенційно ризикових або аномальних користувачів.

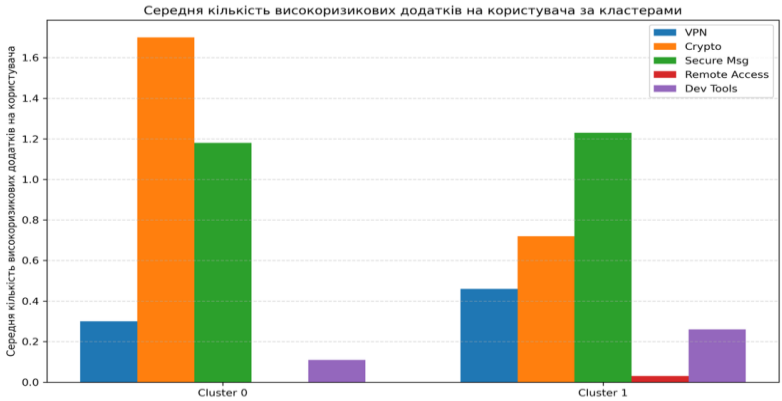

Рисунок 1 – Інтегральний показник поведінкового ризику.

Проведений аналіз встановлених мобільних застосунків показав, що структура використаних сервісів може слугувати інформативним джерелом для криміналістичного оцінювання поведінки користувачів. Отримані результати продемонстрували наявність двох відмінних груп користувачів, серед яких одна характеризується підвищеною концентрацією ризикових застосунків. Розрахований показник поведінкового ризику та сформовані поведінкові портрети підтверджують можливість застосування такого підходу для ідентифікації потенційно небезпечних або аномальних профілів. Запропонована методика може бути використана як допоміжний інструмент у цифровій криміналістиці та подальших дослідженнях, спрямованих на виявлення прихованих поведінкових ознак за даними мобільних пристроїв.

Література

1. Dudhe, P., & Gupta, S. R. (2023). Data Behavioral Pattern Analysis and Noise Classification in Mobile Forensic . International Journal of Intelligent Systems and Applications in Engineering, 12(4s), 223–227. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/3785

2. K. Barmpatsalou, T. Cruz, E. Monteiro and P. Simoes, "Mobile Forensic Data Analysis: Suspicious Pattern Detection in Mobile Evidence," in IEEE Access, vol. 6, pp. 59705-59727, 2018, doi: 10.1109/ACCESS.2018.2875068

3. Okmi M, Por LY, Ang TF, Al-Hussein W, Ku CS. A Systematic Review of Mobile Phone Data in Crime Applications: A Coherent Taxonomy Based on Data Types and Analysis Perspectives, Challenges, and Future Research Directions. Sensors (Basel). 2023 Apr 28;23(9):4350. doi: 10.3390/s23094350. PMID: 37177554; PMCID: PMC10181620.

4. Hongkyun Kwon, Sangjin Lee, Doowon Jeong, User profiling via application usage pattern on digital devices for digital forensics, Expert Systems with Applications, Volume 168, 2021, 114488, ISSN 0957-4174, https://doi.org/10.1016/j.eswa.2020.114488.

УДК: 556.166:004.9:528.94

ГЕОІНФОРМАЦІЙНЕ МОДЕЛЮВАННЯ ЗОН ЗАТОПЛЕННЯ У СИСТЕМІ ARCGIS: НА ПРИКЛАДІ РУЙНУВАННЯ ГІДРОТЕХНІЧНИХ СПОРУД В УМОВАХ ВОЄННИХ ЗАГРОЗ

Вікторія ФІЛІППОВА, Андрій ГАВРИСЬ
Львівський державний університет безпеки життєдіяльності

Анотація. У роботі розглянуто можливості застосування геоінформаційних систем, зокрема програмного забезпечення ArcGIS, для моделювання затоплених територій у разі аварій чи навмисного руйнування гідротехнічних споруд. Особлива увага приділена українському контексту, у якому геоінформаційні технології відіграють критично важливу роль через зростання ризиків, пов'язаних із військовими діями та загрозами для критичної інфраструктури.

Ключові слова: затоплення, гідротехнічні споруди, ArcGIS, цивільний захист.

Геоінформаційні системи (ГІ) відіграють значну роль у сучасному аналізі ризиків як природного та техногенного характеру. У контексті України, особливо в умовах воєнних загроз, значущість цього інструментарію зростає експоненційно, оскільки цілеспрямовані обстріли та атаки на критичну інфраструктуру часто призводять до її руйнування та виникнення масштабних катастроф. Одним із найбільш поширених та комплексних програмних рішень у цій сфері є програмний комплекс ArcGIS – система, призначена для збирання, управління, аналізу, моделювання та візуалізації просторових даних. Завдяки своїй архітектурі, ArcGIS дозволяє трансформувати географічну інформацію в ефективний інструмент підтримки управлінських рішень, що є критично важливим для цивільного захисту, екологічного моніторингу та планування реагування на надзвичайні ситуації. Фундаментальна перевага системи полягає у здатності працювати з великими обсягами гетерогенних просторових даних, включаючи цифрові моделі рельєфу (ЦМР), супутникові знімки, векторні шари інфраструктури та мережі гідрологічних об'єктів, об'єднуючи їх у єдиному аналітичному просторі. Застосування інструментів ArcGIS дає змогу створювати прогнозні моделі можливого затоплення, оцінювати наслідки руйнування інженерних споруд, визначати зони потенційної небезпеки та розробляти детальні сценарії реагування. Для України, де гідротехнічні об'єкти є стратегічними для енергетичної, водної та зрошувальної систем, це питання набуває особливої актуальності [1].

Теракт, що призвів до руйнування греблі Каховської ГЕС засвідчив, що атаки на такі споруди мають потенціал генерувати масштабні техногенні лиха, тому що, об'єм води, що неконтрольовано вивільнився з Кахов-

ського водосховища, призвів до затоплення сотень квадратних кілометрів території, знищення соціальної та критичної інфраструктури, матеріальні збитки, людські жертви та спричинив довготривалі екологічні та соціальні наслідки. Збитки, завдані Україні руйнуванням, за оцінками Уряду України та ООН, сягнули щонайменше 14 мільярдів доларів США. Серед катастрофічних наслідків було зафіксовано деградацію до 75% рослинного покриву, забруднення акваторії на площі 6800 км², аграрну кризу, втрату систем зрошення, що до цього забезпечували полив 426,8 тисяч гектарів сільськогосподарських угідь на Херсонщині. Також було знищено місця нересту риб, і на відновлення популяцій знадобиться до 10 років. Ці події є наочною демонстрацією необхідності розробки та постійного оновлення моделей можливих сценаріїв затоплення для системи цивільного захисту та органів державної влади [2].

Методологічна основа моделювання затоплення у середовищі ArcGIS ґрунтується на використанні цифрової моделі рельєфу. ЦМР дозволяє з високою точністю симулювати шляхи та динаміку поширення водних мас у разі прориву гідротехнічної споруди. На основі цих моделей, із застосуванням інструментів гідрологічного аналізу, стає можливим оцінити глибину та швидкість руху води, ідентифікувати низинні ділянки, які будуть затоплені першочергово, а також встановити території потенційного довготривалого підтоплення. Ключовими етапами цього процесу є аналіз напрямку стоку, генерація моделей руху води, розрахунок зон перенакопичення та створення полігонів затоплення, які залежать від заданого рівня прориву. При моделюванні сценарію прориву, як це було виконано на прикладі Каховської ГЕС, необхідно враховувати висоту хвилі, характеристики річкового русла, ухил місцевості та об’єм водосховища. У результаті формується геопросторова модель, яка візуалізує поширення затоплення протягом перших годин після руйнування, охоплюючи насамперед заплавні території. На такій карті чітко відображаються межі, в яких вода затримуватиметься протягом тривалого часу.

Практична цінність таких геопросторових моделей полягає не лише у створенні статичних карт затоплення, а й у прогнозуванні подальших, вторинних наслідків катастрофи. Мова йде про ймовірне руйнування дорожнього покриття, підтоплення сховищ небезпечних речовин, втрату водопостачання, деградацію земель та знищення природних екосистем. ArcGIS дозволяє інтегрувати отримані результати з іншими важливими картографічними шарами, такими як населені пункти, транспортна інфраструктура, об’єкти соціального значення та системи енергозабезпечення, що перетворює карту на динамічний інструмент кризового управління. Ця модель дає змогу точно визначити населені пункти, що потребують негайної евакуації, та оцінити можливість доступу аварійно-рятувальних служб до найбільш уражених територій. Для органів державної влади ця інфор-

мація є необхідною при формуванні планів реагування, визначенні зон евакуації та розробленні інженерних рішень для захисту територій і управління відновлювальними процесами після катастрофи [3].

В українських реаліях, використання ArcGIS забезпечує можливість створення національної бази даних щодо ризиків гідродинамічних аварій, проведення комплексної оцінки стійкості гідротехнічних споруд та впровадження більш інтегрованих систем просторового моніторингу. Окрім моделювання проривів дамб, ГІС-технології можуть ефективно застосовуватися для аналізу паводків, прогнозування підтоплень, оптимізації використання водних ресурсів та оцінки впливу кліматичних змін на водний баланс. Приклад Каховської ГЕС однозначно демонструє, що відсутність попереднього, детального моделювання значно ускладнює та сповільнює дії рятувальних служб, тоді як наявність актуальних карт затоплення дозволяє значно підвищити оперативну готовність регіональних органів влади та підрозділів цивільного захисту. Програмний комплекс ArcGIS дає змогу перетворити географічні дані на інструмент стратегічної безпеки, адже моделювання зон затоплення є не просто технічним завданням, а ключовим компонентом сучасної державної політики безпеки. Враховуючи виклики, що постали перед Україною, впровадження та використання ГІС-технологій у сфері управління ризиками та планування реагування на надзвичайні ситуації має стати державним стандартом, оскільки, застосування цих технологій сприяє не лише зменшенню техногенних втрат, але й підвищує шанси на порятунок населення та матеріальних та культурних цінностей завдяки швидкому та обґрунтованому прийняттю рішень.

Література

1. Стародуб, Ю. П., Гаврись, А. П., Ковальчук, В. М., Рогуля, А. О., & Філіппова, В. (2022). Досягнення стабільного розвитку територій шляхом реалізації проєкту визначення зон паводкового затоплення в Україні. Том 6 № 1 (2022): Збірник наукових праць ЧІПБ імені Героїв Чорнобиля НУЦЗ України «Надзвичайні ситуації: попередження та ліквідація» DOI: https://doi.org/10.31731/2524.2636.2022.6.1.103-114.

2. Пічура В. І., Потравка Л. О., Білошкуренко О. С. «Дослідження наслідків руйнації Каховської дамби та осушення водосховища для населення України». Науковий журнал «Водні біоресурси та аквакультура» 1(17)/2025. DOI https://doi.org/10.32782/wba.2025.1.20.

3. Havrys, A., Veselivsky, R., Pekarska, O., Liubovetskyi, O., Filippova, V., 2025. Support System For Management Decision-Making By Heads Of Hydrological Emergency Situations Liquidation Using Geo-Information Technologies. Municipal economy of cities 1, 416-427. https://doi.org/10.33042/2522-1809-2025-1-189-416-427.

УДК 614.841

СУЧАСНІ МЕТОДИ ГЕЙМІФІКАЦІЇ ДЛЯ ПІДГОТОВКИ ПОЖЕЖНИХ-РЯТУВАЛЬНИКІВ

Анастасія ФРИС, Володимир-Петро ПАРХОМЕНКО
Львівський державний університет безпеки життєдіяльності

Анотація. *Підготовка пожежних-рятувальників є критично важливою для ефективного реагування особового складу ОРС ЦЗ на пожежі, аварії та катастрофи, але традиційні методи обмежені вартістю, ризиками для здоров'я, логістикою та недостатньою реалістичністю, що ускладнює навчання в умовах сьогодення. В умовах технологічного процесу гейміфікація підготовки пожежних-рятувальників може осучаснити класні заняття в системі службової підготовки, та замінити деякі практичні відпрацювання. Метою даної роботи є висвітлення можливості використання віртуальних тренувальних комплексів для осучаснення та гейміфікації в підготовці особового складу пожежно-рятувальних підрозділів ДСНС України. Описано вітчизняний (СИМ-3) та можливості і переваги закордонного тренувального комплексу (FLAIM Trainer) для включення їх у систему службової підготовки пожежно-рятувальних підрозділів ДСНС України. Гейміфіковані віртуальні тренувальні комплекси (зокрема, СИМ-3 та FLAIM Trainer) є ключовим інструментом для модернізації та осучаснення класних занять в системі службової підготовки ДСНС України, оскільки дозволяють знизити ризики і вартість навчання.*

Ключові слова: *гейміфікація, тренажери віртуальної реальності, підготовка пожежних-рятувальних, віртуальна реальність (VR), службова підготовка, гасіння пожеж, непридатне для дихання середовище.*

Abstract. *Training fire and rescue personnel is critical for the effective response of civil protection personnel to fires, accidents, and disasters, but traditional methods are limited by cost, health risks, logistics, and insufficient realism, which complicates training in today's environment. In the context of technological processes, gamification of firefighter and rescue worker training can modernize classroom training in the professional training system and replace some practical exercises. The purpose of this work is to highlight the possibility of using virtual training complexes for modernization and gamification in the training of personnel of the fire and rescue units of the State Emergency Service of Ukraine. The domestic (SIM-3) and foreign (FLAIM Trainer) training complexes are described, along with their capabilities and advantages for inclusion in the professional training system of the fire and rescue units of the State Emergency Service of Ukraine. Gamified virtual training complexes (in particular, SIM-3 and FLAIM Trainer) are a key tool for modernizing and updating classroom training in the professional training system of the State Emergency Service of Ukraine, as they reduce the risks and cost of training.*

Keywords: *gamification, virtual reality simulators, fire and rescue training, virtual reality (VR), professional training, firefighting, unbreathable environment.*

Підготовка пожежних-рятувальників є критично важливою для забезпечення ефективного реагування на надзвичайні ситуації, такі як пожежі, аварії та природні катастрофи. Традиційні методи навчання, що базуються на теоретичних лекціях, практичних вправах на полігонах та симуляціях з використанням реального обладнання, часто стикаються з обме-

женнями: високою вартістю, ризиком для здоров'я учасників, логістичними труднощами та недостатньою реалістичністю сценаріїв. Підготовка особового складу відіграє ключову роль для ефективності підрозділів під час проведення оперативних дій на пожежі. Метою даної роботи є висвітлення сучасних тренувальних комплексів для осучаснення і гейміфікації підготовки особового складу пожежно-рятувальних підрозділів ДСНС України.

Гейміфікація, як метод інтеграції ігрових елементів (таких як бали, рівні, нагороди та змагання) у неігрові процеси, демонструє значний потенціал для покращення підготовки пожежних-рятувальників. Сучасні віртуальні реальності (VR) та інші тренажери відіграють ключову роль у гейміфікації при підготовці пожежних-рятувальників, де може бути включеною у систему службової підготовки особового складу оперативно-рятувальної служби цивільного захисту.

Цікавим та інноваційним з вітчизняних тренажерів є VR-симулятор СИМ-3, призначений для відпрацювання навичок з ліквідації пожеж різних класів необхідним типом вогнегасника. “Апаратно-програмний комплекс для навчання та закріплення навичок поводження з вогнегасником”. Корисна модель належить до тренажерів для гасіння пожежі за допомогою вогнегасників, і може бути використана в навчальному процесі навчання з пожежної безпеки для набуття практичного досвіду пожежогасіння вогнегасниками у віртуальному середовищі, а також для перевірки набутих навичок користування вогнегасниками. Перевагою даного тренажеру є можливість його застосовування без дорогого і громіздкого екрану, тільки використовуючи ноутбук або планшет і VR окуляри.

Прикладом використання закордонних тренувальних комплексів в Україні є тренувальний комплекс FLAIM Trainer. Система моделює реалістичні надзвичайні ситуації, такі як пожежі в промислових об'єктах, на транспорті чи в закритих приміщеннях, комплектується: VR-шоломом, симулятором пожежного рукава зі стволом, захисного одягу (жилету) з можливістю відтворення дії теплового випромінювання під час ліквідації та апарату автономного дихання стисненим повітрям з відкритим контуром. Використання повної комплектації даного тренувального комплексу сприяє формуванню м'язової пам'яті та навичок прийняття рішень під час ліквідації пожеж чи надзвичайних ситуацій на відкритому просторі та у непридатному для диханні середовищі (НДС). FLAIM Trainer забезпечує відтворення понад 150 різних сценаріїв за 28 умов. Квазі-експериментальні дослідження, проведені з 22 пожежниками в Португальській національній школі пожежної служби, демонструють високу прийнятність та ефективність системи, з підвищенням рівня занурення, зменшенням стресу та покращенням когнітивних реакцій порівняно з традиційними методами, а також підтвердженням як доповнення до реальних тренувань особового складу пожежно-рятувальних підрозділів.

Рисунок – 1 Зовнішній вигляд VR-тренажерів
а) СИМ-3, б) FLAIM Trainer

Для майбутніх досліджень перспективним напрямком є оцінка ефективності даних тренувальних комплексів під час навчання особового складу пожежно-рятувальних підрозділів різних медико-вікових груп особового складу пожежних-рятувальних підрозділів та здобувачів освіти закладів освіти із специфічними умовами навчання, які належить до сфери управління центрального органу виконавчої влади, що реалізує державну політику у сфері цивільного захисту.

Література

1. Лущ В.І., Великий Я.Б., Пархоменко В.-П.О. Створення полігону для підготовки газодимозахисників до проведення аварійно-рятувальних робіт в обмеженому просторі на горизонтальних ділянках. *Пожежна безпека: зб. наук. праць.* Львів: ЛДУ БЖД, 2020. №36. С. 59-65. URL: https://doi.org/10.32447/20786662.36.2020.06

2. Лазаренко О.В., Пархоменко В.-П.О., Мухін В.В. Особливості використання пожежного тепловізора в умовах проведення пошуково-рятувальних робіт. *Пожежна безпека: зб. наук. праць*. Львів: ЛДУ БЖД, 2022. №41. С. 87-93. URL: https://doi.org/10.32447/20786662.41.2022.10

3. Пархоменко В.-П.О., Лазаренко О.В., Сукач Р.Ю. Аналіз обладнання для гасіння електромобілів та розробка рекомендацій з їх гасіння. *Пожежна безпека: зб. наук. праць*. Львів: ЛДУ БЖД, 2023. №42. С. 74-84. URL: https://doi.org/10.32447/20786662.42.2023.09

4. Про затвердження Порядку організації службової підготовки осіб рядового і начальницького складу служби цивільного захисту: наказ Міністерства внутрішніх справ України від 15.06.2017 року №511. Офіційний вісник України. 2017. №59. С. 135. URL: https://zakon.rada.gov.ua/laws/show/z0835-17#Text

5. STEM Class [електронний ресурс]. URL: https://stemclass.com.ua/catalog/kabinet-bezpeki/mobilni-simulyatori/simulyator-pozhezhnoi-bezpeki-elektrichna-duhovka

6. Підвищення професійних умінь під час практичних занять на віртуальному симуляторі FLAIM Trainer. Львівський державний університет безпеки життєдіяльності. 2024. [електронний ресурс]. URL: https://ldubgd.edu.ua/node/8852

УДК 004.8:004.56

МЕТОДИ ПІДГОТОВКИ КОНТЕКСТУ ДЛЯ АНАЛІЗУ ВРАЗЛИВОСТЕЙ LLM

Роман ЦАПКОВАТИЙ, Тетяна ЛАВРИК
Сумський державний університет

Анотація. *Проаналізовано і систематизовано методи підготовки контексту для LLM у задачах аналізу безпеки програмного забезпечення. Ефективність LLM у виявленні та валідації вразливостей критично залежить від наданого контексту. Розглянуто методи, що базуються на синтаксичному розширенні, аналізі потоків даних (DFA) та семантичному "зрізанні" коду (program slicing), з метою визначення оптимальних стратегій підготовки даних.*

Ключові слова: *великі мовні моделі, статичний аналіз безпеки, підготовка контексту, аналіз вразливостей, аналіз потоків даних, семантичне зрізання коду, інженерія промптів, зменшення хибних спрацювань, гібридні системи захисту.*

Abstract. *This paper analyzes and systematizes context preparation methods for Large Language Models in software security analysis tasks. The efficacy of LLMs in vulnerability detection and validation is critically dependent on the provided context. Methods based on syntactic extension, Data Flow Analysis (DFA), and semantic program slicing are examined to determine optimal data preparation strategies.*

Keywords: *Large Language Models, LLM, Static Application Security Testing, SAST, context preparation, vulnerability analysis, Data Flow Analysis, DFA, semantic program slicing, prompt engineering, false positives reduction, hybrid security systems.*

Інтеграція великих мовних моделей у процеси аналізу безпеки ПЗ відкриває нові горизонти, особливо у вирішенні задачі валідації результатів статичного аналізу (SAST). Як показують недавні дослідження, гібридні підходи, що поєднують SAST та LLM, можуть суттєво підвищити точність виявлення вразливостей [1]. Проте LLM не працюють у вакуумі. На відміну від традиційного аналізатора, LLM отримує на вхід лише послідовність токенів, і ефективність аналізу залежить від того, наскільки коректно цей "контекст" репрезентує програмну логіку. Проста передача фрагмента коду, на який вказав SAST, є недостатньою, оскільки ігнорує джерела даних та шляхи їх поширення. Таким чином, задача ефективної підготовки контексту стає центральною для побудови дієвих гібридних систем аналізу.

Основний виклик при використанні LLM для аналізу коду полягає у двох обмеженнях:

1. **Технічне обмеження (Розмір вікна)** – сучасні LLM мають обмежений обсяг вхідного контексту (наприклад, від 8K до 128K токенів), чого недостатньо для аналізу цілих проєктів;

2. **Семантичне обмеження** – LLM потребує вказівок, які саме частини коду є релевантними для аналізу, оскільки модель не може автоматично "здогадатися" про зв'язки між різними файлами.

Для вирішення цих проблем, методи підготовки контексту можна класифікувати за зростанням рівню їхньої складності.

- Найпростіший метод – **Синтаксичне Розширення** (напр., включення N рядків до/після вразливості або тіла всієї функції). Він простий у реалізації, але майже гарантовано пропускає міжпроцедурні взаємодії.
- Більш просунутий підхід – **Аналіз Потоків Даних** (Data-Flow Analysis, DFA), що фокусується на відстеженні "забруднених" даних. Для валідації SAST-попередження, контекст для LLM повинен містити джерело (Source), точку входу (Sink) та інформацію про санітизацію на шляху між ними.
- Найбільш точним методом є **Семантичне "Зрізання" Коду** (Program Slicing), що полягає у виділенні мінімальної підмножини коду ("зрізу"), яка впливає на поведінку програми у певній точці [2]. Використання зворотного зрізу (Backward Slicing) від "sink" дозволяє зібрати всі інструкції, що вплинули на значення даних, забезпечуючи LLM найбільш повним та релевантним контекстом.

Окрім коду, підготовка контексту включає Інженерію Промптів (Prompt Engineering). Ефективний промпт повинен містити роль ("Ти – експерт з кібербезпеки..."), завдання ("Проаналізуй код..."), сам код (отриманий методом DFA або "зрізання") та конкретизацію ("Зверни увагу на змінну username..."). Використання методологій "Ланцюжка Думок" (Chain-of-Thought, CoT) [3] також допомагає моделі структурувати свій аналіз, що підвищує точність.

Ефективний процес підготовки контексту для гібридної системи (SAST+LLM) можна візуалізувати як конвеєр, що автоматизує збір та агрегацію даних. Наведена діаграма (Рис. 1) ілюструє цей процес.

Рисунок 1 – Діаграма процесу формування контексту для LLM-валідації

Незважаючи на переваги просунутих методів, залишається низка викликів. Автоматизація семантичного "зрізання" коду для великих проєктів є нетривіальною задачею, а оптимізований контекст все ще може перевищувати ліміти вікна LLM. Майбутні дослідження будуть зосереджені на розробці моделі взаємодії компонентів гібридної системи, яка б реалізовувала адаптивне "зрізання" коду, та алгоритмів агрегації результатів.

Ефективність LLM у задачах аналізу вразливостей визначається не лише самою моделлю, але й методами підготовки вхідних даних. Перехід від наївних синтаксичних підходів до семантично обґрунтованих методів, таких як аналіз потоків даних та "зрізання" коду, є необхідною умовою для побудови точних та надійних гібридних систем безпеки.

Література

1. H. Pearce, R. Goel, P. Godefroid, and R. Majumdar, "IRIS: LLM-Assisted Static Analysis for Detecting Security Vulnerabilities," arXiv preprint arXiv:2402.19418, 2024.

2. X. Zhang, T. Zhang, Y. Wu, C. Xu, and H. Chen, "SEVUL: A static analysis-based vulnerability detection tool using code slicing and graph attention networks," in Proc. 2023 6th Int. Conf. Inf. Sci. Syst., 2023, pp. 574-580.

3. J. Wei et al., "Chain-of-thought prompting elicits reasoning in large language models," arXiv preprint arXiv:2201.11903, 2022.

УДК 004.9

ПРАКТИЧНЕ ЗАСТОСУВАННЯ ПРОГРАМНОГО СЕРЕДОВИЩА NI MULTISIM ДЛЯ ДОСЛІДЖЕННЯ СХЕМОТЕХНІКИ ОПЕРАЦІЙНИХ ПІДСИЛЮВАЧІВ

Євген ЦІТКОВСЬКИЙ, Юрій БОРЗОВ
Львівський державний університет безпеки життєдіяльності

Анотація.*Розглянуто функціональні можливості САПР NI Multisim для дослідження електронних кіл. На прикладі схеми інвертуючого підсилювача продемонстровано процес моделювання: від створення принципової схеми до аналізу сигналів за допомогою віртуального осцилографа. Підтверджено ефективність використання віртуальних приладів для верифікації теоретичних розрахунків.*

Ключові слова: NI Multisim, моделювання, схемотехніка, операційний підсилювач, віртуальні прилади.

Abstract.*The functional capabilities of NI Multisim CAD for electronic circuit research are considered. Using the example of an inverting amplifier circuit, the simulation process is demonstrated: from creating a schematic to signal analysis using a virtual oscilloscope. The efficiency of using virtual instruments for verifying theoretical calculations is confirmed.*

Key words: NI Multisim, simulation, circuitry, operational amplifier, virtual instruments.

Сучасний рівень розвитку комп'ютерної техніки дозволяє значно спростити процес вивчення та проектування електронних пристроїв. Використання систем автоматизованого проектування (САПР), зокрема програмного середовища NI Multisim, є актуальним у навчальному процесі, оскільки дозволяє проводити складні експерименти без необхідності використання реальної елементної бази, уникаючи ризику пошкодження обладнання. Головною метою роботи є демонстрація можливостей Multisim для побудови схем та аналізу принципів їх роботи.

Як об'єкт дослідження обрано схему інвертуючого ввімкнення операційного підсилювача (ОП). Згідно з теоретичними відомостями, таке ввімкнення дозволяє отримати вихідний сигнал, що знаходиться у протифазі до вхідного, а коефіцієнт підсилення визначається співвідношенням опорів зворотного зв'язку.

Процес моделювання у Multisim розпочинається з розміщення компонентів на робочому полі. На рис. 1 представлено зібрану схему, де використано віртуальну модель ОП, резистори R1 та R2, що утворюють коло зворотного зв'язку. Перевагою програми є наявність великої бібліотеки компонентів та інтуїтивно зрозумілий інтерфейс, що дозволяє швидко змінювати номінали та конфігурацію схеми.

Важливою особливістю Multisim є наявність віртуальних вимірювальних приладів, які повністю імітують роботу реальних пристроїв. Для генерації вхідного сигналу використано функціональний генератор (Function Generator).

Аналіз роботи схеми проводиться за допомогою двоканального осцилографа. Використання цього інструменту в Multisim дозволяє одночасно спостерігати вхідний (Channel A) та вихідний (Channel B) сигнали. Результат моделювання наведено на рис. 2.

Отримана осцилограма наочно демонструє ключові можливості програми для аналізу схем:

1. **Візуалізація підсилення:** амплітуда вихідного сигналу (помаранчева крива) значно перевищує амплітуду вхідного (червона крива), що підтверджує коректність роботи розрахованого каскаду.

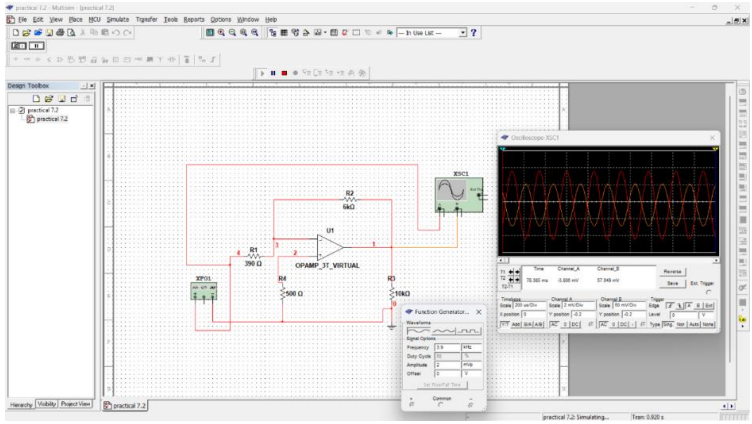

Рисунок 1 – Моделювання інвертуючого підсилювача в середовищі NI Multisim

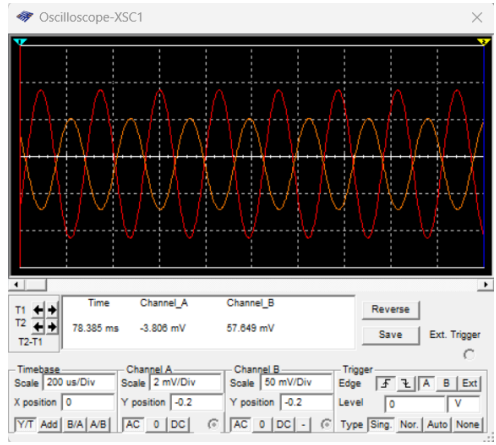

Рисунок 2 – Осцилограма вхідного та вихідного сигналів

2. **Аналіз фазових співвідношень:** за допомогою курсорних вимірювань та графічного відображення чітко видно зсув фаз на 180 градусів. Коли вхідний сигнал має позитивну напівхвилю, вихідний сигнал набуває негативного значення, що повністю узгоджується з теорією інвертуючого підсилювача.

3. **Точні вимірювання:** інформаційна панель осцилографа (див. рис. 2) дозволяє миттєво отримувати цифрові значення напруги та часових інтервалів (T2-T1), що значно пришвидшує обробку результатів експерименту.

Висновок. Програмне середовище NI Multisim є дуже корисним інструментом для схемотехнічного моделювання. Воно дозволяє не лише проектувати схеми, але й проводити глибокий аналіз їх роботи за допомогою віртуальних приладів. Використання Multisim дає змогу наочно перевірити теоретичні закономірності, такі як інверсія фази та коефіцієнт підсилення, роблячи процес дослідження електронних кіл інтерактивним, безпечним та наочним.

Література

1. Комп'ютерна схемотехніка: лабораторний практикум для студентів напряму підготовки 122 «Комп'ютерні науки» / уклад.: Ю.О. Борзов, О.О. Смотр. – Львів, 2019. – 67 с.

2. Гончаренко Б.М., Коновалов К.В. Електроніка та мікросхемотехніка: Навч. посіб. – К.: НУХТ, 2006. – 565 с.

3. Юрченко М.М., Сенько Л.І., Ясінський В.В. Аналогові та імпульсні пристрої. Т.2. – Харків: Фоліо, 2002. – 510 с.

УДК 004.8:004.62

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ БАЗОВОГО АНАЛІЗУ ДАНИХ

Євген ЦІТКОВСЬКИЙ, Юлія НАЗАР
Львівський державний університет безпеки життєдіяльності

Розглянуто потенціал застосування інструментів штучного інтелекту для базового аналізу даних. Висвітлено переваги автоматизації обробки інформації, виявлення прихованих закономірностей та візуалізації результатів. Окреслено перспективи використання мовних моделей та спеціалізованих алгоритмів для підвищення ефективності прийняття рішень.

Ключові слова: штучний інтелект, аналіз даних, автоматизація, машинне навчання, Python, статистика.

The potential of using artificial intelligence tools for basic data analysis is considered. The advantages of automating information processing, identifying hidden patterns, and visualizing results are highlighted. The prospects for using language models and specialized algorithms to improve decision-making efficiency are outlined.

Keywords: artificial intelligence, data analysis, automation, machine learning, Python, statistics.

Сучасний етап розвитку інформаційних технологій характеризується стрімким зростанням обсягів даних, що генеруються у різних сферах людської діяльності — від державного управління та цивільного захисту до бізнесу та науки. Ефективна обробка цих масивів інформації стає критично важливою умовою для прийняття обґрунтованих рішень. У цьому контексті використання штучного інтелекту (ШІ) для аналізу даних перестає бути прерогативою виключно вузькоспеціалізованих наукових центрів і стає доступним інструментом для вирішення повсякденних завдань.

Традиційні методи ручної обробки даних часто виявляються недостатньо ефективними при роботі з багатовимірними наборами даних. Людський фактор збільшує ймовірність помилок, а час, витрачений на попередню обробку інформації, часто перевищує час, відведений на її інтерпретацію. Штучний інтелект пропонує альтернативний підхід, який дозволяє автоматизувати рутинні процеси.

Основним напрямом застосування ШІ у простому аналізі даних є використання мови програмування Python та бібліотек машинного навчання, таких як Scikit-learn. Ці інструменти дозволяють навіть при базових навичках реалізовувати алгоритми прогнозування. Зокрема, на рисунку 1 представлено приклад застосування алгоритму лінійної регресії для прогнозування обсягу умовних інцидентів, що базується на даних попередніх років. Слід зазначити, що для побудови моделі було задіяно вибірку тесто-

вих даних, а подальше підвищення точності прогнозування вимагає істотного збільшення обсягу емпіричної бази.

```python
import numpy as np
import pandas as pd
from sklearn.linear_model import LinearRegression

# Створення набору даних: рік та кількість інцидентів
data = {
    'Year': [2019, 2020, 2021, 2022, 2023],
    'Incidents': [150, 165, 160, 180, 195]
}
df = pd.DataFrame(data)

# Підготовка даних (X - ознаки, y - цільове значення)
X = df[['Year']]
y = df['Incidents']

# Ініціалізація та навчання моделі лінійної регресії
model = LinearRegression()
model.fit(X, y)

# Прогноз на 2025 рік
future_year = np.array([[2025]])
prediction = model.predict(future_year)

print(f"Прогноз кількості інцидентів на 2025 рік: {prediction[0]:.0f}")
```

```
Прогноз кількості інцидентів на 2025 рік: 212
```

Рисунок 1 – Приклад застосування алгоритму лінійної регресії для прогнозування обсягу умовних інцидентів

Наведений код демонструє, як за допомогою кількох рядків можна створити модель, що знаходить залежність між часовим проміжком та кількістю подій. У реальних умовах служби цивільного захисту такі моделі дозволяють аналізувати значно складніші нелінійні залежності, враховуючи погодні умови (температуру, вологість, силу вітру), час доби, густоту забудови та наявність джерел протипожежного водопостачання.

Окремої уваги заслуговує використання великих мовних моделей (LLM) для інтерпретації таких даних. Сучасні генеративні моделі (наприклад, на базі архітектури GPT) здатні виступати не лише як інструмент написання коду, але і як «інтелектуальний асистент» аналітика. Вони можуть обробляти неструктуровані текстові дані, такі як описи оперативних зведень або рапорти чергових змін, виокремлюючи з них ключові сутності та тенденції. Користувач отримує можливість завантажити «сирі» дані та сформулювати запит природною мовою, наприклад: «Проаналізуй причини загорянь у житловому секторі за останній квартал та вияви аномалії». Це суттєво знижує поріг входження в аналітику даних, дозволяючи фахівцям без глибокої математичної підготовки отримувати якісні інсайти.

Втім, широке впровадження ШІ у сферу безпеки супроводжується суттєвими викликами. Ключовою проблемою є феномен «чорної скриньки» (black box), коли логіка прийняття рішення нейронною мережею залишається непрозорою для користувача. У сфері цивільного захисту, де ціна помилки вимірюється людськими життями та матеріальними збитками, сліпа довіра алгоритму є неприпустимою. Саме тому при аналізі критично важливих даних необхідно дотримуватися принципу «Human-in-the-loop» (людина в контурі управління), забезпечуючи верифікацію машинних прогнозів традиційними методами статистики та експертною оцінкою. Необхідно розвивати напрямок «пояснюваного штучного інтелекту» (Explainable AI, XAI), який дозволяє інтерпретувати фактори, що вплинули на результат роботи моделі.

Підсумовуючи, можна стверджувати, що інтеграція інструментів штучного інтелекту та скриптових мов програмування у процеси аналізу даних є закономірним етапом цифрової трансформації служби цивільного захисту. Для майбутніх фахівців, які навчаються у Львівському державному університеті безпеки життєдіяльності, опанування цими технологіями стає необхідною фаховою компетенцією. Це дозволяє перейти від парадигми реактивного реагування на надзвичайні ситуації до проактивного прогнозування ризиків та превентивного управління ресурсами на основі даних.

Література

1. Рак Ю. П., Меньшикова О. В. Моделювання небезпек складних технічних систем : монографія. Львів : ЛДУБЖД, 2018. 220 с.

2. Мюллер А., Гвідо С. Вступ до машинного навчання з Python. Київ : Фабула, 2019. 390 с.

3. Шопський О., Хлевной О. (2025). Метод прогнозування кількості пожеж в житловому секторі на основі алгоритмів машинного навчання. Вісник Львівського державного університету безпеки життєдіяльності, 31, 80-90. https://doi.org/https://doi.org/10.32447/20784643.31.2025.09

4. Зачко О. Б., Іванюта С. П. Управління ризиками у сфері цивільного захисту на основі інтелектуальних систем. *Проблеми надзвичайних ситуацій*. 2021. № 1(33). С. 12–24.

5. Burak, N., Khlevnoi, O., Zhezlo-Khlevna, N., Raita, D., Dotsenko, O. (2025). Determination of Fire Evacuation Parameters in Higher Education Institutions with Inclusive Groups Using Machine Learning Methods. In: Babichev, S., Lytvynenko, V. (eds) Lecture Notes in Data Engineering, Computational Intelligence, and Decision-Making, Volume 2. ISDMCI 2024. Lecture Notes on Data Engineering and Communications Technologies, vol 244. Springer, Cham. https://doi.org/10.1007/978-3-031-88483-2_14

6. McKinney W. Python for Data Analysis: Data Wrangling with Pandas, NumPy, and IPython. 3rd ed. O'Reilly Media, 2022. 560 p.

УДК 004.942:655

МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ ТЕХНОЛОГІЧНИХ ПАРАМЕТРІВ ФЛЕКСОДРУКУ НА ПІДПРИЄМСТВІ «ПАКОТЕК»

Камелія ЧІНКУЕ
Інститут поліграфії та медійних технологій НУ «Львівська політехніка»

***Анотація**. Виконано дослідження флексографічного друку на виробництві упаковки. Виявлено недоліки у процесі встановлення робочих параметрів. Розроблено модель для передбачення результатів друку на основі швидкості, температури і тиску з метою покращення виробничих показників.*
***Ключові слова:** флексодрук, математична модель, технологічні параметри, оптимізація виробництва.*

***Abstract.** A study of flexographic printing in packaging production was performed. Deficiencies in the process of setting operating parameters were identified. A model was developed to predict printing results based on speed, temperature and pressure to improve production performance.*
***Keywords:** flexographic printing, mathematical model, technological parameters, production optimization.*

Проблематика підтримання стабільних показників якості продукції під час роботи флексографічного обладнання залишається невирішеною для багатьох виробників упаковки. Компанія «ПАКОТЕК», чиї виробничі потужності орієнтовані на випуск упаковки для різних промислових секторів [1], має труднощі зі значними втратами сировини під час переходу між різними типами замовлень. Виробничі дані свідчать про втрату 8-12% матеріалів лише на етапі підготовки устаткування до роботи, що негативно позначається на економічних показниках.

Головна причина таких втрат полягає у відсутності систематизованого методу встановлення робочих режимів друкування. Визначення швидкості роботи машини, температурного режиму для висихання барвника і рівня тиску циліндра виконується персоналом емпіричним шляхом. Результатом стає необхідність проведення численних тестових циклів – від трьох до п'яти - що подовжує підготовчий період і створює додаткові обсяги непридатної продукції.

Детальне вивчення виробничого циклу показало, що регулювання окремих параметрів відбувається без врахування їхнього взаємного впливу. Зокрема, збільшення швидкості роботи потребує адекватних змін температурного режиму і коригування зусилля притискання, проте ці залежності не зафіксовані у виробничій документації. Крім того, брак систематизованої інформації про ефективні поєднання налаштувань для конкретних ма-

теріалів унеможливлює швидке відновлення оптимальних режимів при повторному виконанні аналогічних робіт.

Вирішення описаної проблеми можливе через створення математичного апарату, який визначає зв'язок між якістю результату і ключовими виробничими факторами. Підхід ґрунтується на статистичному опрацюванні виробничої інформації і враховує комплексний вплив швидкості V (м/хв), температури T (°C), тиску P (Н/см²) і властивостей субстрату M:

$$Q = f(V, T, P, M), \quad (1)$$

де Q – узагальнений критерій якості, який охоплює насиченість кольору, різкість зображення і однорідність покриття.

Окремо для поліетиленових, поліпропіленових і багатошарових матеріалів встановлюються індивідуальні параметри моделі через аналіз попередніх виробничих циклів. Такий підхід враховує специфічну реакцію кожного типу основи на зміну робочих умов, для поліетиленової плівки залежність якості друку від швидкості та температури сушіння (рис. 1) показує, що оптимальний діапазон роботи знаходиться при температурі 55°C і швидкості 60-75 м/хв, що забезпечує якість понад 95%.

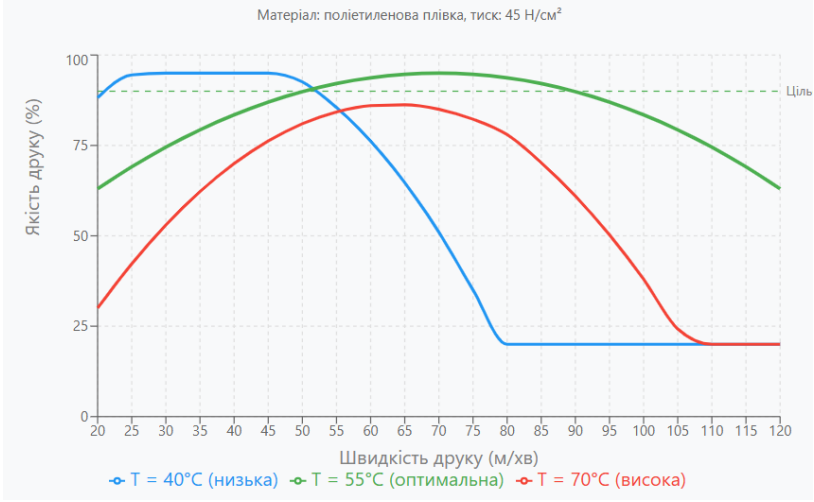

Рисунок 1 – Інтерактивний графік залежності якості друку

Реалізація моделі передбачає розробку програмного засобу для операторів устаткування. Працівник задає характеристики матеріалу і необхідний рівень якості, система обчислює відповідні значення швидкості,

температури і тиску. Очікується скорочення кількості тестових циклів з 3-5 до одного, що зменшить втрати матеріалів до 2-3% і прискорить підготовчий етап на 40-50%.

Застосування моделі формує основу для систематизації виробничого досвіду. Фіксація параметрів і результатів кожного циклу збагачує інформаційну базу, підвищуючи достовірність розрахунків для наступних завдань. Доцільним є подальше включення моделі у систему автоматичного керування для динамічного коригування режимів роботи.

Висновок. Використання математичного апарату для визначення оптимальних режимів флексографічного друку дає можливість знизити обсяги непридатної продукції і підвищити ефективність виробничого процесу. Реалізація описаного підходу на виробництві «ПАКОТЕК» забезпечить зменшення втрат сировини, скорочення підготовчого періоду і досягнення стабільних показників якості.

Література

1. Офіційний сайт компанії «ПАКОТЕК». URL: https://packotek.com.ua (дата звернення: 15.11.2025).

2. Бараускєне О., Чепурна К., Вихристюк О. Відтворення пантонів при виготовленні етикеткової продукції флексографічним друком. Технологія і техніка друкарства. 2021. № 3(73). С. 31–41.

УДК 004.8-378

DATA SCIENCE AND ARTIFICIAL INTELLIGENCE SYSTEMS IN THE MODERN WORLD

Dmytro SHARHUT
Lviv Polytechnic National University

Ця теза досліджує взаємозв'язок між наукою про дані (Data Science) та системами штучного інтелекту, наголошуючи на якості даних, аналітичному моделюванні та сучасних архітектурах ШІ. Вона висвітлює проблеми прозорості моделей, етичні аспекти та інтеграцію методів Data Science у інтелектуальні системи для підвищення надійності, масштабованості та практичної застосовності в сучасному світі.

Наука про дані, Штучний інтелект, Машинне навчання, Архітектури ШІ, Якість даних, Аналітичне моделювання, Прозорість моделей, Етичний ШІ, Інтелектуальні системи, Масштабованість.

This thesis examines the relationship between Data Science and Artificial Intelligence, emphasizing data quality, analytical modelling, and modern AI architectures. It highlights challenges of model transparency, ethical considerations, and the integration of Data Science methods into intelligent systems to improve reliability, scalability, and practical applicability in the modern world.

Data Science, Artificial Intelligence, Machine Learning, AI Architectures, Data Quality, Analytical Modelling, Model Transparency, Ethical AI, Intelligent Systems, Scalability.

Artificial intelligence (AI) systems and Data Science have become fundamental drivers of technological progress, shaping the modern digital ecosystem and redefining approaches to information processing, decision-making, and automation. AI focuses on developing computational models capable of performing tasks traditionally associated with human intelligence such as classification, prediction, planning, reasoning, and natural language processing while Data Science forms the analytical core that enables these systems to learn from empirical data [2]. The interaction between these fields creates a comprehensive methodological framework integrating statistics, machine learning, optimization, and advanced computational techniques.

The purpose of this research is to examine the conceptual and methodological connections between Data Science and AI, emphasizing the role of data-centric approaches, model interpretability, and the practical implementation of intelligent systems in real-world environments. Special consideration is given to the lifecycle of AI solutions, which typically includes data acquisition, preprocessing, feature extraction, model development, evaluation, deployment, and continuous monitoring. Each stage requires

rigorous methodological support to ensure the accuracy, reliability, and reproducibility of analytical results [1].

A significant challenge for modern AI systems lies in ensuring high-quality datasets, as noise, bias, incompleteness, and unbalanced structures may distort model behavior. Data Science tools including statistical diagnostics, exploratory data analysis, dimensionality reduction, and anomaly detection help mitigate these limitations and strengthen the stability of machine learning pipelines 111. Additionally, contemporary AI models, particularly deep neural networks, require large-scale heterogeneous datasets and powerful computational resources, which explains the growing role of data engineering and distributed architectures.

The rapid development of neural architectures such as transformers, diffusion models, and graph neural networks has substantially expanded the applicability of AI across scientific, industrial, and public domains. These advanced models demonstrate exceptional performance in natural language understanding, computer vision, decision support, robotics, and multimodal processing . However, increased model complexity raises critical questions about interpretability, fairness, algorithmic transparency, and ethical considerations. Responsible AI principles require explainability mechanisms, rigorous validation procedures, and adherence to international standards concerning data protection and accountability [3].

In this context, Data Science serves as a unifying discipline that bridges theoretical advancements in AI with their practical integration into operational systems. It ensures systematic analysis, objective evaluation of model performance, risk assessment, and optimization of computational workflows. Combining AI methodologies with Data Science techniques provides a powerful foundation for developing intelligent, adaptive, and scalable systems capable of addressing complex tasks in manufacturing, healthcare, finance, cybersecurity, transport, and smart infrastructure [4].

References

1. Bishop, C. Pattern Recognition and Machine Learning. Springer, 2006.
2. Provost, F., Fawcett, T. Data Science for Business. O'Reilly Media, 2013.
3. Russell, S., Norvig, P. Artificial Intelligence: A Modern Approach. Pearson, 2021.
4. Chollet, F. Deep Learning with Python. Manning Publications, 2021.

УДК 004.75:004.42

РОЗРОБКА МІКРОСЕРВІСНОЇ АРХІТЕКТУРИ ДЛЯ ВЕБОРІЄНТОВАНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ

Михайло ШЕВЦІВ, Юрій КОЛЕСНИК, Роман ПАДЮКА

Львівський національний університет ветеринарної медицини та біотехнологій імені С.З. Гжицького

Анотація. *У роботі представлено підхід до проєктування мікросервісної архітектури веборієнтованої інформаційної системи із використанням сучасного Java-стеку. Розглянуто механізми маршрутизації, виявлення сервісів, централізованої конфігурації, балансування навантаження, відмовостійкості, трасування та асинхронної взаємодії.*

Ключові слова: *мікросервіси, Spring Cloud, Eureka, балансування навантаження, RabbitMQ.*

Abstract. *The paper presents an approach to designing a microservice architecture for a web-oriented information system using a modern Java technology stack. The study examines routing, service discovery, centralized configuration, load balancing, resilience, distributed tracing, and asynchronous communication.*

Keywords: *microservices, Spring Cloud, Eureka, load balancing, RabbitMQ.*

Сучасні веборієнтовані програмні системи функціонують в умовах високих вимог до надійності, гнучкості та адаптивності, що робить проблему вибору ефективної архітектури однією з ключових у проєктуванні. Монолітні підходи, які традиційно застосовувались у розробленні складних інформаційних систем, дедалі частіше проявляють обмеження, пов’язані з неможливістю швидкого масштабування, складністю оновлення компонентів та низькою стійкістю до збоїв. Тому мікросервісна архітектура стає одним з найбільш перспективних рішень для систем, орієнтованих на високу інтенсивність обробки запитів і динамічний розвиток.

У межах розробленої системи використано Java-орієнтований стек з інструментами Spring Cloud Gateway, Netflix Eureka, Spring Cloud Config, Ribbon, механізмом автоматичного вимикача, Zipkin/Sleuth та RabbitMQ. Кожен з цих компонентів виконує важливу роль у функціонуванні архітектури: шлюз маршрутизує запити, служба виявлення сервісів забезпечує динамічність системи, конфігураційний сервер – узгодженість параметрів, а брокер повідомлень – асинхронну комунікацію.

Першочерговим елементом у системі є API Gateway, який формує єдину точку доступу для всіх клієнтів і приховує внутрішню структуру мікросервісів. Spring Cloud Gateway реалізує неблокуючу модель обробки

запитів, що дозволяє досягати високої пропускної здатності та гарантувати стабільність роботи навіть при пікових навантаженнях. Застосування фільтрів, правил маршрутизації й механізмів автентифікації дозволяє централізовано забезпечувати безпеку і контроль трафіку.

Другим важливим елементом є система виявлення сервісів, реалізована за допомогою Netflix Eureka. Вона дозволяє автоматично реєструвати сервіси, оновлювати інформацію про їх стан та забезпечувати їх пошук у режимі реального часу. Це усуває необхідність ручного налаштування IP-адрес і дає змогу динамічно масштабувати систему шляхом додавання або вилучення екземплярів сервісів.

Централізоване керування конфігурацією забезпечується Spring Cloud Config, що дає можливість зберігати конфігураційні файли в репозиторії Git та поширювати їх між усіма сервісами. Такий підхід підвищує узгодженість архітектури, спрощує підтримку, дозволяє швидко змінювати параметри системи та застосовувати однакові конфігурації для різних середовищ розгортання.

Важливим аспектом забезпечення стабільності роботи є механізм балансування навантаження. Ribbon реалізує клієнтське балансування, що дозволяє застосунку самостійно обирати екземпляр сервісу для обробки запиту. Це сприяє рівномірному використанню ресурсів та знижує ризик перевантаження окремих компонентів системи.

Додаткове підвищення стійкості забезпечується механізмом автоматичного вимикача (circuit breaker), який запобігає каскадним відмовам у разі виходу з ладу одного з сервісів. У разі частих тайм-аутів або помилок він ізолює проблемний сервіс і дозволяє системі підтримувати працездатність без повного припинення робочих процесів.

Важливий елемент контролю над системою забезпечують Zipkin і Spring Cloud Sleuth, які виконують роль інструментів для розподіленого трасування. Їх використання дає змогу відстежувати проходження запитів між сервісами, аналізувати час виконання операцій і виявляти «вузькі місця» в архітектурі.

Асинхронна взаємодія сервісів реалізується за допомогою RabbitMQ, який гарантує ефективний обмін повідомленнями, зменшує затримки у роботі і дозволяє реалізувати подієво-орієнтовану модель комунікації.

Узагальнена архітектура розробленої системи представлена на рисунку 1, де наведено зв’язки між основними мікросервісними компонентами та їхня взаємодія.

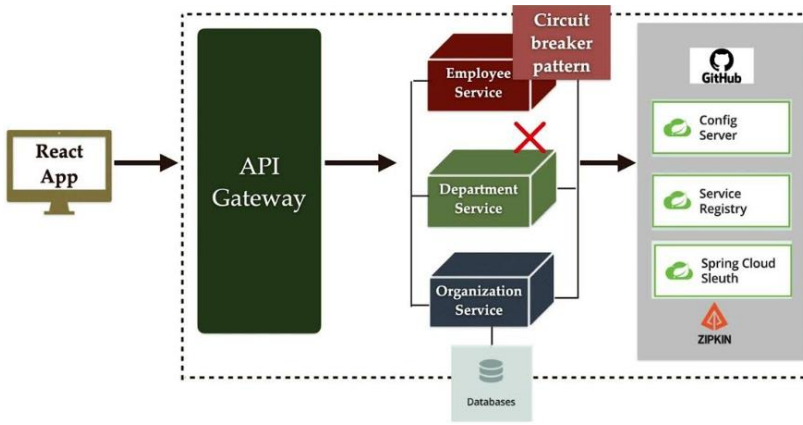

Рисунок 1 – Загальна архітектура мікросервісної системи

Запропонована архітектура демонструє високу гнучкість, здатність до масштабування та стійкість до помилок, що робить її перспективною для побудови розподілених веборієнтованих систем із високими вимогами до продуктивності. Використання сучасного стеку Spring Cloud забезпечує узгоджену роботу всіх компонентів і спрощує подальшу підтримку та розвиток системи.

УДК 004.3

РЕАЛІЗАЦІЯ БЕЗДРОТОВОГО ПРОТОКОЛУ ЗВ'ЯЗКУ (PS2 CONTROLLER) ДЛЯ ВІДДАЛЕНОГО КЕРУВАННЯ РОБОТИЗОВАНИМ КОМПЛЕКСОМ

Андрій ШМИГЕЛЬСЬКИЙ, Ігор МАЛЕЦЬ
Львівський державний університет безпеки життєдіяльності, м. Львів

Анотація. *Розглянуто реалізацію системи бездротового керування роботизованою рукою на базі крокових двигунів та контролера PS2. Описано архітектуру взаємодії компонентів та алгоритм перетворення сигналів джойстика у керуючі імпульси STEP/DIR. Обґрунтовано ефективність поєднання точного позиціонування приводів із ергономікою геймпада для створення бюджетного та функціонального маніпулятора.*

Ключові слова: *робототехніка, PS2 контролер, крокові двигуни, бездротове керування, мікроконтролер.*

Abstract. *The implementation of a wireless control system for a robotic arm based on stepper motors and a PS2 controller is examined. The component interaction architecture and the algorithm for converting joystick signals into STEP/DIR control pulses are described. The effectiveness of combining precise actuator positioning with gamepad ergonomics to create a low-cost and functional manipulator is substantiated.*

Keywords: *robotics, PS2 controller, stepper motors, wireless control, microcontroller.*

Роботизовані руки широко застосовуються у промисловості, медицині та наукових дослідженнях. Точне позиціонування є критично важливим для багатьох із цих застосувань, тому крокові двигуни часто є кращим вибором. Вони забезпечують високий крутний момент на низьких швидкостях і можливість роботи у відкритому циклі без необхідності використання зворотного зв'язку (енкодерів).

Для забезпечення мобільності та зручності оператора, бездротовий пульт керування є необхідним. Контролер PS2, завдяки своїй ергономіці, наявності великої кількості кнопок та двох аналогових джойстиків, є популярним та недорогим рішенням для створення таких інтерфейсів.

Архітектура системи складається з трьох основних блоків:

1.Передавач (контролер PS2): Надсилає команди оператора.

2.Бездротовий приймач PS2 та Мікроконтролер: Приймає дані, обробляє їх та перетворює на команди для двигунів.

3.Силова частина (драйвери крокових двигунів та крокові двигуни): Виконує команди руху.

Бездротовий зв'язок між контролером PS2 та приймачем зазвичай здійснюється на частоті 2.4 ГГц. Приймач PS2 підключається до мікрокон-

тролера через стандартний послідовний синхронний інтерфейс, який за функціональністю нагадує SPI (Serial Peripheral Interface). Для роботи з протоколом часто використовують спеціалізовану Arduino-бібліотеку - PS2X Library, яка спрощує отримання даних про стан кнопок та положення аналогових джойстиків.

Крокові двигуни керуються за допомогою спеціальних драйверів (наприклад, A4988 або DRV8825), які отримують сигнали STEP - для генерації кроків та DIR – для визначення напрямку від мікроконтролера.

Перетворення даних розпочинається з читання джойстика, де мікроконтролер отримує аналогове значення положення джойстика в діапазоні від 0 до 255. Наступний крок — визначення швидкості та напрямку руху, де значення від 117 до 137 інтерпретується як зупинка. Значення джойстика в діапазоні від 0 до 116 або від 138 до 255 визначають відповідний напрямок, а їхня віддаленість від діапазону зупинки встановлює бажану швидкість руху. Для фактичного керування швидкістю крокового двигуна мікроконтролер здійснює генерацію імпульсів на піні STEP. Частота цих імпульсів повинна бути пропорційною заданій оператором швидкості.

Цифрові кнопки можуть бути використані для керування допоміжними функціями, такими як захоплення або точні покрокові рухи.

Реалізація бездротового керування роботизованою рукою на крокових двигунах за допомогою контролера PS2 є ефективним та економічно вигідним рішенням. Поєднання точного керування, яке забезпечують крокові двигуни, та інтуїтивного інтерфейсу PS2 дозволяє створити функціональну та зручну для використання роботизовану систему.

Література

1. Arduino PS2X Library Documentation [Electronic resource] // GitHub. – Access mode: https://github.com/madsci1016/Arduino-PS2X.

2. Wireless Mobile Robotic Arm Controlled by PS2 Joystick Based on Microcontroller [Electronic resource] // ResearchGate. – Access mode: https://www.researchgate.net/publication/320584696.

3. Baichtal J. Arduino for Arduinians: 70 Projects for the Experienced Programmer. New York: Que Publishing, 2013. 350 p.

УДК 004.9

ГЕОІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ОЦІНКИ ТА ОПТИМІЗАЦІЇ ТЕРИТОРІАЛЬНОГО ПОКРИТТЯ ПОЖЕЖНО-РЯТУВАЛЬНИМИ ПІДРОЗДІЛАМИ ДЕРЖАВНОЇ СЛУЖБИ УКРАЇНИ З НАДЗВИЧАЙНИХ СИТУАЦІЙ: МЕТОДИКА ПРОСТОРОВО-ЧАСОВОГО АНАЛІЗУ ТА ВИЯВЛЕННЯ ЗОН РИЗИКУ

Орест ШОПСЬКИЙ, Ігор ФІРМАН, Ростислав ГРИНИК
Львівський державний університет безпеки життєдіяльності

Анотація: У дослідженні представлено методику просторово-часової оцінки доступності пожежно-рятувальних підрозділів із використанням QGIS та мережевого аналізу на основі даних OpenStreetMap. Отримані результати дають змогу визначати території з підвищеним часом реагування та обґрунтовувати розміщення додаткових пожежних команд.

Ключові слова: ГІС; просторово-часовий аналіз; пожежно-рятувальні підрозділи; час реагування; мережевий аналіз; територіальне покриття.

Abstract: The study introduces a GIS-based method for spatio-temporal assessment of fire and rescue unit accessibility using QGIS and network analysis derived from OpenStreetMap data. The results support identifying areas with increased response times and provide an evidence-based foundation for optimizing the placement of supplementary fire units.

Key words: GIS; spatio-temporal analysis; fire and rescue units; response time; network analysis; territorial coverage.

Ефективність ліквідації надзвичайних ситуацій значною мірою залежить від часу прибуття підрозділів ДСНС України, який визначається їхнім територіальним розміщенням. Оптимізацію дислокації державних та добровільних пожежно-рятувальних підрозділів доцільно обґрунтовувати із застосуванням геоінформаційних систем (ГІС), що дозволяють проводити просторово-часовий аналіз та виявляти території з підвищеним часом реагування.

Розроблений на основі ГІС алгоритм мережевого моделювання дає змогу оцінювати доступність найближчих сил і засобів реагування та обґрунтовувати управлінські рішення щодо підвищення рівня пожежної безпеки. У Львівському державному університеті безпеки життєдіяльності створено методики просторового аналізу, які дозволяють ідентифікувати території, де час прибуття перших пожежно-рятувальних підрозділів

перевищує критичні 20–30 хвилин. Для оцінки часу прибуття найближчих сил реагування на потенційне місце надзвичайної ситуації розроблено та апробовано спеціалізований алгоритм з використанням геоінформаційних систем та допоміжних скриптів.

На територію дослідження наноситься регулярна сітка точок із кроком 500 м (рис. 1), після чого з неї відбираються лише точки, що входять до меж вибраних територіальних громад (рис. 2).

Рисунок 1 – Сітка точок із кроком 500 м

Рисунок 2 – Точки що належать до полігона

Після підготовки сітки точок виконується розрахунок найкоротших маршрутів від кожного аварійно-рятувального підрозділу ДСНС до всіх точок сітки. Для цього використовується мережевий аналіз (Network analysis) на основі актуальної дорожньої мережі OpenStreetMap з урахуванням диференційованих середніх швидкостей руху спеціальної пожежної техніки відповідно до ДСТУ 8767:2018 (таблиця 1).

Таблиця 1 – Гранична швидкість руху пожежного автомобіля

Групи населених пунктів за чисельністю населення, тис. чол.							
малі				середні	великі	крупні	найкрупніші
До 5	Від 5 до 10	Від 10 до 20	Від 20 до 50	Від 50 до 100	Від 100 до 250	Від 250 до 800	Понад 800
Гранична швидкість руху пожежного автомобіля, км/год							
31,0	32,0	33,0	35,0	35,0	35,0	39,0	26,0
Примітка. Якщо район виїзду охоплює населені пункти, які належать до різних груп, для розрахунків приймають середню швидкість від граничних швидкостей руху для цих населених пунктів.							

Для кожної точки сітки визначається найменший час доїзду серед усіх доступних підрозділів (мінімальний час прибуття першого підрозділу).

Отримані значення часу доїзду записуються в атрибутивну таблицю точкового шару та візуалізуються за допомогою категорізованої символіки (рис. 3):

- ≤ 20 хвилин – зелений колір (прийнятний рівень захисту);
- 20–30 хвилин – жовтий колір (обмежений рівень захисту);
- >30 хвилин – червоний колір (критично не захищена територія).

Рисунок 3 – Відображення точкового шару

Така градація відповідає сучасним нормативним вимогам щодо часу реагування на пожежі та інші надзвичайні ситуації, а також дозволяє чітко виявляти так звані «білі плями» — території з незадовільним рівнем пожежно-рятувального покриття.

Проведений ГІС-аналіз часу доїзду пожежно-рятувальних підрозділів на території досліджуваної громади чітко виявив зони з часом реагування понад 30 хвилин, які потребують негайного створення місцевих або добровільних пожежних команд. Запропоноване рішення є реалізованим у QGIS і рекомендується для впровадження в органах місцевого самоврядування та ДСНС України.

Література

1. Martyn Ye. Software for Shelter's Fire Safety and Comfort Levels Evaluation /Martyn Ye., Smotr O., Burak N., Prydatko O., Malets I. //Communications in Computer and Information Science, Springer, Cham. – Vol. 1158, 2020. pp. 457-469 https://doi.org/10.1007/978-3-030-61656-4_31

2. Шопський, О., & Малець, І. (2025). Класифікація та просторовий аналіз пожеж у системі оперативно-диспетчерського управління. Системні технології, 3(158), 140. https://doi.org/10.34185/1562-9945-3-158-2025-14

3. Prydatko, V. V., Chalyy, D. O., Prydatko, O. V., & Kobko, V. A. (2023). Аналітичний огляд методів та параметрів оптимізації зон обслуговування рятувальних підрозділів. Fire Safety, 43, 123–136. https://doi.org/10.32447/20786662.43.2023.14

4. Пугач, С. О., Кайдик, О. Л., Терлецький, Т. В., Угрин, Д. І., & Вісин, О. О. (2025). ГІС-інструменти для аналізу та моделювання надзвичайних ситуацій (на прикладі пожеж у Волинській області). Computer-integrated technologies: education, science, production, (60), 466–475. https://doi.org/10.36910/6775-2524-0560-2025-60-49

5. Kustov, M., Sobol, O., & Fedoryaka, O. (2021). Територіальне розміщення пожежних підрозділів різної функціональної спроможності. Problems of Emergency Situations, (33), 181–192. https://doi.org/10.52363/2524-0226-2021-33-14

Пожежно-рятувальні частини. Вимоги до дислокації та району виїзду, комплектування пожежними автомобілями та проектування. (2018).

УДК 004:37

ЄДИНЕ ЦИФРОВЕ ОСВІТНЄ СЕРЕДОВИЩЕ УНІВЕРСИТЕТУ НА ОСНОВІ MOODLE ТА MICROSOFT 365: ТЕОРЕТИЧНІ ЗАСАДИ ТА ПРАКТИЧНА МОДЕЛЬ ВПРОВАДЖЕННЯ

Богдан ШУВАР
Львівський національний університет ветеринарної медицини та біотехнологій імені С.З. Ґжицького

Анотація. У статті розглянуто теоретичні засади та практичну модель формування єдиного цифрового освітнього середовища університету на основі системи Moodle та хмарних сервісів Microsoft 365. Наголошено на перевагах моделі «один логін» для доступу до навчальних ресурсів, сервісів комунікації й внутрішніх адміністративних послуг.

Ключові слова: інформаційні технології, Moodle, Microsoft 365, Teams, єдине освітнє середовище, цифрова трансформація, SSO.

Abstract. The paper presents theoretical foundations and a practical model of a unified digital learning environment based on Moodle and Microsoft 365 in a university. Special attention is paid to the "single sign-on" approach, enabling access to educational resources, communication tools and internal administrative services through one institutional account.

Keywords: information technologies, Moodle, Microsoft 365, Teams, unified learning environment, digital transformation, SSO.

Сучасний етап розвитку суспільства характеризується переходом до цифрової економіки, що зумовлює необхідність цифрової трансформації освіти [1; 2]. Заклади вищої освіти мають не лише використовувати окремі інформаційні технології (ІТ), а й вибудовувати цілісну цифрову екосистему, яка підтримує навчальний процес, наукову діяльність та управління [3]. Актуальним стає проєктування цілісних моделей цифрового середовища на базі поєднання LMS та хмарних сервісів.

Інформаційні технології в освіті доцільно розглядати в кількох взаємопов'язаних площинах: як засіб організації доступу до навчального контенту, як інструмент взаємодії між учасниками освітнього процесу; як механізм збору, аналізу та використання освітніх даних для прийняття управлінських рішень [1; 3]. В основі результативного впровадження ІТ лежить сформована цифрова компетентність викладачів і студентів, яка включає вміння добирати, поєднувати та педагогічно обґрунтовано застосовувати цифрові інструменти [1].

Ключовим елементом цифрового освітнього середовища виступають платформи управління навчанням (LMS). Використання Moodle як «ядра» електронного навчання забезпечує структуровану подачу навчальних ма-

теріалів, підтримку різних форматів оцінювання, гнучкі засоби зворотного зв'язку та аналітику успішності [3; 5]. Moodle дозволяє проєктувати курси з урахуванням результатів навчання, застосовувати різні моделі змішаного навчання, підтримувати роботу великих потоків студентів та формувати електронні журнали [3; 5].

Комплекс хмарних сервісів Microsoft 365 (Exchange Online, Teams, OneDrive, SharePoint, Forms, Power Automate, Power BI тощо) створює єдине корпоративне середовище для комунікації, спільної роботи та управління освітніми й адміністративними процесами [4; 6]. Інтеграція Moodle з Microsoft 365 дає змогу реалізувати модель єдиного входу (Single Sign-On, SSO): студент чи викладач використовує один обліковий запис університету для доступу до Moodle, Microsoft Teams, внутрішніх електронних заявок до відділів, корпоративних порталів підрозділів, а за потреби - й до зовнішніх сервісів, зокрема наукометричних баз і профілів, пов'язаних з інституційною поштою [5;6;7].

Сервіс Microsoft Teams виступає «фронт-ендом» комунікації: підтримує проведення онлайн-занять, консультацій, захистів кваліфікаційних робіт, групову роботу студентів, інтегрується з календарем і каналами курсів [4; 6]. Для викладача це означає можливість швидко організувати відеозустріч безпосередньо з курсу Moodle, а для студента — доступ до навчальних матеріалів, завдань та записів занять з єдиного інтерфейсу.

З точки зору адміністрації університету сервіси Microsoft 365 дають низку стратегічних переваг. По-перше, хмарна модель зменшує навантаження на локальну інфраструктуру та забезпечує високу доступність сервісів (пошта, календар, документообіг, комунікація) для всіх підрозділів університету [4; 6]. По-друге, зв'язка SharePoint + Teams використовується для побудови електронного документообігу та корпоративних порталів кафедр, деканатів, відділів, де зберігаються положення, накази, методичні матеріали. По-третє, інструменти затверджень (Approvals у Teams) і Power Automate дозволяють формалізувати процедури погодження заяв, графіків, наказів, договорів, внутрішніх електронних заявок до різних служб університету, перевівши їх у прозорий та відслідковуваний цифровий формат [6; 7].

Додатковою перевагою є наявність єдиного сховища файлів (OneDrive та бібліотеки документів SharePoint), що спрощує спільну роботу над навчальними матеріалами, робочими програмами дисциплін, звітами кафедр, а також усуває дублювання та розпорошеність документів по різних локальних носіях [4]. Використання Power BI відкриває можливості для побудови інформаційних панелей (дашбордів) для керівництва університету, де в інтегрованому вигляді відображаються показники контингенту, успішності, завантаженості викладачів, використання електронних ресурсів тощо [6; 7].

Разом із тим, упровадження інформаційних технологій супроводжується низкою проблем. Серед них – нерівний доступ до цифрових ресурсів

і якісного інтернет-з'єднання, недостатній рівень цифрової культури частини викладачів, фрагментарність використання різних платформ без єдиної стратегії розвитку [2; 3]. Додатковими викликами є інформаційна безпека, захист персональних даних та забезпечення академічної доброчесності в умовах дистанційного оцінювання [2; 4].

Організаційною передумовою успішної цифрової трансформації є наявність узгодженої стратегії розвитку інформаційно-освітнього середовища університету [3]. Така стратегія має визначати пріоритетні напрями розвитку (цифровізація навчального процесу на базі Moodle, впровадження Microsoft 365 як платформи комунікації та документообігу, розвиток відкритих онлайн-курсів), відповідальні підрозділи, механізми фінансування й систему моніторингу ефективності [3; 4]. Важливою складовою є системне підвищення кваліфікації науково-педагогічних працівників щодо використання LMS, хмарних сервісів і моделей SSO [1; 3; 5].

Таким чином, інформаційні технології в освіті, зокрема поєднання Moodle та хмарних сервісів Microsoft 365 в єдиному цифровому середовищі, виступають не лише технічним інструментом, а й чинником зміни освітньої парадигми - від передачі знань до організації активної, дослідницько-орієнтованої та персоналізованої діяльності студентів [2-4]. Практична модель «один логін - багато сервісів» демонструє, що успіх цифрової трансформації закладу вищої освіти залежить від поєднання технологічних рішень із продуманою освітньою політикою, розвитком цифрових компетентностей учасників освітнього процесу та послідовною підтримкою керівництва університету [1; 3; 4; 6].

Література

1. European Commission. DigCompEdu: European Framework for the Digital Competence of Educators : educational framework. Luxembourg : Publications Office of the European Union, 2017.

2. UNESCO. Guidance on Open Educational Resources and ICT in Education. Paris : UNESCO, 2020.

3. Морзе Н. В., Кочубей Н. В. Цифрова трансформація університетської освіти : монографія. Київ, 2021.

4. Співаковський О. В. Інформаційні технології в освіті: теорія, практика, перспективи : монографія. Херсон : [б. в.], 2019.

5. Moodle Docs. Managing a Moodle-based learning environment. URL : https://learn.microsoft.com (дата звернення: 22.11.2025).

6. Microsoft. Microsoft 365 for Education: Teams, SharePoint, OneDrive and security in educational institutions. URL : https://learn.microsoft.com (дата звернення: 22.11.2025).

7. Microsoft. Microsoft Power Platform in Education: Approvals and workflow automation for universities. URL : https://learn.microsoft.com (дата звернення: 22.11.2025).

УДК 004:056

ІНФОРМАЦІЙНА БЕЗПЕКА В УМОВАХ ГІБРИДНОЇ ВІЙНИ: РИЗИКИ, ЗАГРОЗИ ТА УПРАВЛІНСЬКІ РІШЕННЯ

Богдан ШУВАР
Львівський національний університет ветеринарної медицини та біотехнологій імені С.З. Ґжицького

Анотація. У статті досліджуються особливості інформаційної безпеки в умовах гібридної війни. Проаналізовано ключові ризики та загрози, пов'язані з дезінформацією і кібератаками, окреслено ризик-орієнтований підхід до управління та запропоновано управлінські рішення для державних інституцій і закладів освіти.
Ключові слова: інформаційна безпека; гібридна війна; дезінформація; кіберзагрози; управління ризиками; медіаграмотність.

Annotation. The article examines information security in the context of hybrid warfare. It analyzes key risks and threats related to disinformation and cyber attacks, outlines a risk-based approach to information security management and proposes managerial decisions for public institutions and higher education establishments.
Keywords: information security; hybrid warfare; disinformation; cyber threats; risk management; media literacy.

Гібридна війна як форма сучасних збройних конфліктів характеризується поєднанням традиційних військових дій із політичним, економічним, кібернетичним та інформаційно-психологічним впливом. У такій конфігурації інформаційна сфера перестає бути лише середовищем обміну даними й перетворюється на ключовий простір боротьби за сприйняття реальності, легітимність рішень та рівень довіри до державних інститутів. Інформаційна безпека в умовах гібридної війни набуває стратегічного значення, оскільки визначає здатність суспільства зберігати стійкість перед маніпуляціями, дезінформаційними кампаніями та цілеспрямованим руйнуванням інформаційної інфраструктури.

Специфіка гібридної війни полягає в тому, що інформаційні, медійні та кібернетичні операції розгортаються як до початку відкритих бойових дій, так і паралельно з ними та після їх активної фази. Масовані кампанії дезінформації, створення альтернативних наративів, дискредитація політичного та військового керівництва, підрив довіри до союзників і міжнародних організацій — усе це формується як цілісна система впливу, в якій інформація використовується як інструмент зброї. Особливу роль відіграють неправдиві або маніпулятивні «вкиди» у засобах масової інформації та соціальних мережах, які подаються під виглядом «ексклюзивних даних», «аналітики» чи «думки експертів».

Ризики для інформаційної безпеки в умовах гібридної війни доцільно розглядати у взаємозв'язку технічних, організаційних та соціальних чинників. До технічних ризиків належать кібератаки на інформаційні системи органів влади, закладів освіти, об'єктів критичної інфраструктури, зокрема злами вебсайтів, компрометація облікових записів адміністраторів, виведення з ладу серверів чи систем управління. Організаційні ризики пов'язані з відсутністю або формальністю політик інформаційної безпеки, нечітким розподілом відповідальності за комунікації, фрагментарністю внутрішніх регламентів перевірки інформації. Соціальні ризики, своєю чергою, проявляються у низькому рівні медіаграмотності, схильності до емоційного сприйняття новин, готовності користувачів без критичного аналізу поширювати неперевірені повідомлення.

Загрози, що випливають із таких ризиків, мають багатовимірний характер. На рівні державного управління вони можуть призводити до дестабілізації суспільно-політичної ситуації шляхом поширення чуток про «капітуляцію», «втрату територій», «зраду союзників», а також до підриву легітимності прийнятих рішень. Для сектору безпеки й оборони помилкові або навмисно спотворені повідомлення здатні створювати хибні очікування, деморалізувати особовий склад, впливати на громадську підтримку оборонних зусиль. В освітньому та науковому середовищі дезінформація може використовуватися для дискредитації університетів, маніпулювання думкою студентської молоді, поширення антинаукових, конспірологічних чи радикальних наративів.

Управління інформаційною безпекою в таких умовах доцільно будувати на основі ризик-орієнтованого підходу, який передбачає системну ідентифікацію, оцінювання та обробку ризиків у відповідності до міжнародних стандартів, зокрема ISO/IEC 27001 та ISO/IEC 27005. На першому етапі важливо визначити перелік ключових інформаційних активів: офіційні вебпортали, сторінки в соціальних мережах, системи електронного документообігу, освітні платформи, бази персональних даних тощо. Наступним кроком є виявлення можливих загроз для кожного активу, включаючи як кібератаки, так і інформаційні впливи — захоплення каналу комунікації, створення фейкових «дзеркал» сайту, розсилку повідомлень від імені організації.

Оцінювання ризиків передбачає встановлення ймовірності реалізації кожної загрози та масштабу її потенційних наслідків. Управлінські рішення в сфері інформаційної безпеки мають комплексний характер і охоплюють політики, процеси, структури та технології. На рівні політик доцільно розробити й затвердити чіткі документи, що визначають статус офіційних каналів, правила публікації інформації, вимоги до верифікації даних, порядок реагування на інформаційні інциденти.

У процесному вимірі важливо впровадити стандартизовані процедури моніторингу інформаційного простору, виявлення та аналізу ворожих наративів, а також регулярного інформування керівництва про поточну ситуацію. Ефективність управлінських рішень значною мірою залежить від здатності організації не лише реагувати на окремі інциденти, а й виявляти довгострокові тенденції та адаптовувати свою комунікаційну стратегію.

Важливим складником управлінських рішень є розвиток людського потенціалу. Підготовка персоналу і користувачів до дій в умовах гібридної війни включає навчання основам медіаграмотності, критичного мислення, цифрової гігієни, а також ознайомлення з типовими сценаріями інформаційних атак. Для закладів вищої освіти це означає інтеграцію відповідних тем у навчальні плани, залучення студентів до дослідження й аналізу дезінформаційних кампаній, створення навчальних лабораторій і симуляцій, які дозволяють відпрацьовувати практичні навички виявлення й нейтралізації інформаційних загроз.

Узагальнюючи, можна стверджувати, що інформаційна безпека в умовах гібридної війни є не лише технічною чи комунікаційною проблемою, а системним управлінським викликом. Ефективні рішення у цій сфері повинні базуватися на ризик-орієнтованому підході, поєднанні політик, процесів, структур і технологій, а також на довгострокових інвестиціях у розвиток медіаграмотності та стійкості суспільства. Досвід держав і організацій, що зіткнулися з масштабними інформаційними атаками, зокрема України, створює підґрунтя для формування нових моделей управління інформаційною безпекою, релевантних як у воєнний, так і в повоєнний періоди.

Література

1. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems – Requirements. Geneva : International Organization for Standardization, 2022.

2. ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection – Guidance on managing information security risks. - Geneva : International Organization for Standardization, 2022.

3. Про основні засади забезпечення кібербезпеки України : Закон України від 05 жовтня 2017 р. № 2163-VIII // Відомості Верховної Ради України. 2017. № 45. Ст. 403.

4. Hybrid Threats and Information Warfare : analytical reports / NATO Strategic Communications Centre of Excellence. Riga, 2020.

5. Міжнародні фактчекінгові проєкти щодо дезінформації в умовах гібридної війни [Електронний ресурс]: EUvsDisinfo, StopFake. - Режим доступу : https://euvsdisinfo.eu (дата звернення: 22.11.2025).

Секція 2
КІБЕРБЕЗПЕКА

УДК 004.056.60

WHY IS CYBERSECURITY VERY IMPORTANT FOR ARCHITECTURE FIRMS, AND HOW CAN IT BE IMPROVED WITH AI IN NOWADAYS

Yelyzaveta BODNAR
Lviv Polytechnic National University

Анотація. *У наші дні архітектурні проєкти, інформаційні моделі будівель (BIM) та проєктні плани є надзвичайно цінними. Через це архітектурні фірми часто стають мішенню кібератак, щоб їхні дані та файли могли бути викрадені для корпоративного шпигунства, для зниження ціни на тендерах або для копіювання дизайнів. Фірми працюють з конфіденційною інформацією клієнтів, планами ділянок та внутрішніми схемами будівель. Порушення призводить до порушення законів про конфіденційність (таких як GDPR, CCPA) та руйнує довіру клієнтів. Кіберзлочинці можуть зашифрувати файли, що зберігаються в хмарі, утримуючи їх як заручників, доки не буде сплачено викуп. Для великої фірми з обмеженими термінами це може бути катастрофою, повністю зупиняючи роботу. Публічний витік даних може непоправно зашкодити репутації фірми, ускладнюючи залучення нових клієнтів та призводячи до втрати старих. Крім викупу, фірми стикаються з витратами на відновлення даних, юридичні збори, регуляторні штрафи та втрачений бізнес.*

Ключові слова: *ШІ, Кібербезпека, залучення ШІ до захисту архітектурних проєктів, атаки на „Єдине сховище даних.”*

Abstract: *In our days architectural designs, Building Information Models(BIM), and project plans are extremely valuable,because of that Architecture Firms are often targeted by cyberattacks so their data and files can be stolen for corporate espionage, to underbid projects, or to replicate designs.Firms handle sensitive client information, site plans, and internal building layouts. A breach violates privacy laws (like GDPR, CCPA) and destroys client trust.Cybercriminals can encrypt cloud-stored files, holding them hostage until a ransom is paid. For a big firm on a tight deadline, this can be catastrophic, halting work completely.A public data breach can irreparably damage a firm's reputation, making it difficult to win new clients and lose old ones.Beyond ransoms, firms face costs for data recovery, legal fees, regulatory fines, and lost business.*

Keywords: *AI, Cybersecurity, AI involvement in architectural project security, Attacks on the "Common Data Environment" (CDE).*

Nobody is secured from cyberattacks,for example an Architectural firm in Maryland was hacked and tricked into sending its insurance premium to a hacker and had a loss of more than 500.000$.So we understand that Architectural firms must educate their employees, clients, and vendors about these risks and take the appropriate actions to protect their information.Whenever we open a unknown file,click an unknown link,and fail to have a security patch on device everyone can be in risk.Company have to ensure all devices connected to work network are up to date with the latest security software because often cyber criminals target the companies with old or out of date software.We know that many Architecture firms utilizes public cloud data centers but forget to ensure

the devices with tools and procedures in place to monitor possible threats and isolate data from others in data clouds.

If the cyberattack happened,for company this is a critical situation that requires a swift, structured, and calm response.Company must identify the type of attack,isolate and prevent attack from spreading by unpluging network cables or disable Wi-Fi,call the Cyber Insurance Provider,this is one of the most important steps,they will have a pre-approved list of forensic investigators, legal counsel, and public relations firms who specialize in data breaches,do not pay ransom,explain what happened to clients,employees,partners in simple terms.

The best way to improvise cybersecurity nowadays is AI,it is revolutionizing cybersecurity for architecture firms by moving from a reactive to a proactive and predictive security posture.AI also enhance threat detection and response, automating repetitive tasks, and creating more adaptive defenses. It uses machine learning to analyze vast amounts of data to identify anomalies, block malicious activity in real time, and automate tasks like vulnerability scanning and security alert prioritization, which helps reduce human error and frees up security teams,because AI process and analyze data at a speed and scale far beyond human capabilities, leading to more accurate and efficient security analysis. For example phishing remains one of the biggest cybersecurity threats facing businesses across all industries,and AI can quickly and easily identify signs of phishing, such as email spoofing, forged senders, and misspelled domain names.

Based on all of the above, we can assume that artificial intelligence will become an integral part of cyber security, which will simplify the work of architectural firms,allowing companies to focus more on working with clients without wasting energy on protecting the data that will be protected by AI.

Література

1. Cybersecurity Framework. URL: https://www.nist.gov/cyberframework

2. Securiyi by Design-An Architect’s Guide to Managing Cyber Threats-Resource-AIA Trust/ URL: https://theaiatrust.com/resource/architects-guide-cyber-threats/

3. BIM and Intellectual Property-BIM and Intellectual Property. URL: https://wp.architecture.com.au/bim/wp-content/uploads/sites/40/2014/08/L1-BIM-and-Intellectual-Property.pdf

4. A Guide To Cybersecurity For Architecture Firms- initial.it. URL: https://initialit.net/cybersecurity-for-architecture-firms/

5. 5 Steps to Implement AI-Based Threat Intelligence in Construction-Abnormal. URL: https://abnormal.ai/blog/threat-intelligence-in-construction.

6. Artifical Intelligente (AI) in Cebersecurity: The Future of Threat Defense- Fortinet. URL: https://www.fortinet.com/resources/cyberglossary/artificial-intelligence-in-cybersecurity

7. Reasons AEC Firms Are Prime Targets for Cyberattacks — and How to Fight Back- ATG USA. URL: https://atgusa.com/5-reasons-aec-firms-are-prime-targets-for-cyberattacks-and-how-to-fight-back/

УДК 004.056:004.415

АВТОНОМНЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ДЛЯ БЕЗПЕЧНОГО ЗБЕРІГАННЯ КОНФІДЕНЦІЙНИХ ДАНИХ

Віктор БОНК[1] Ростислав ТКАЧУК[1,2], Валентина ЯЩУК[1]
1. Львівський державний університет безпеки життєдіяльності
2. Національний університет «Львівська політехніка»

Анотація. *У роботі розглянуто програмне забезпечення для безпечного локального зберігання конфіденційної інформації. Наведено обґрунтування вибору мови програмування Python та середовища розробки PyCharm. Для захисту інформації запропоновано використання симетричне шифрування ChaCha20-Poly1305 із генерацією ключа за допомогою PBKDF2-HMAC-SHA256 і випадкової солі, що гарантує конфіденційність та автентифікацію даних. Запропоноване рішення забезпечує надійне, зручне та автономне зберігання персональних даних, сумісне з сучасними стандартами безпеки та нормативними вимогами.*

Ключові слова: *кіберзахист, конфіденційна інформація, локальне сховище, шифрування, Python, модульна архітектура.*

Abstract*. The paper considers software for secure local storage of confidential information. The rationale for choosing the Python programming language and the PyCharm development environment is presented. To protect information, it is proposed to use symmetric encryption ChaCha20-Poly1305 with key generation using PBKDF2-HMAC-SHA256 and a random salt, which guarantees data confidentiality and authentication. The proposed solution provides reliable, convenient and autonomous storage of personal data, compatible with modern security standards and regulatory requirements.*

Keywords: *cyber security, confidential information, local storage, encryption, Python, modular architecture.*

У сучасному цифровому середовищі стрімке зростання обсягів персональних даних і численних онлайн-сервісів підсилює ризики витоку, підробки та несанкціонованого доступу до інформації, що підтверджується численними масштабними інцидентами в державному та корпоративному секторі. Більшість користувачів не мають достатніх технічних знань для самостійного захисту даних, а стандартні інструменти часто зберігають інформацію у відкритому або слабко зашифрованому вигляді та не враховують захист вкладень. У цьому контексті особливо актуальною стає потреба в автономному програмному забезпеченні для локального зберігання конфіденційних відомостей без використання хмарних сервісів, яке забезпечує повноцінне шифрування, простоту використання та відповідність вимогам GDPR, українського законодавства та міжнародних стандартів NIST. Такий підхід дозволяє мінімізувати ризики втрати чи компрометації даних і підвищує рівень довіри користувачів до цифрових технологій [1].

Для створення програмного забезпечення безпечного зберігання конфіденційної інформації необхідне середовище, що забезпечує зручне написання коду, налагодження, керування залежностями та підтримку су-

часних бібліотек. Проведений аналіз засвідчив, що PyCharm є оптимальним інструментом для розробки Python-застосунків завдяки інтелектуальному автозавершенню, потужному налагоджувачу, інтеграції з Git, зручному управлінню віртуальними середовищами та повній сумісності з криптографічними бібліотеками й фреймворками для створення GUI [2].

Альтернативні рішення — Visual Studio Code, Visual Studio, Sublime Text і Jupyter Notebook — мають окремі переваги, однак або потребують значного додаткового налаштування, або не підтримують повноцінний цикл розробки десктопних застосунків. З огляду на комплексність інструментів, офіційну підтримку та зручність роботи з екосистемою Python, PyCharm було обрано як основне середовище розробки.

Python було обрано як оптимальне рішення завдяки поєднанню високої гнучкості, швидкості розробки, широкої підтримки GUI-фреймворків і наявності надійних криптографічних бібліотек. Використані інструменти Python забезпечили реалізацію всіх необхідних компонентів системи: криптографічного захисту, обробки файлів, зберігання структурованих даних і побудови графічного інтерфейсу [3].

Таким чином, екосистема Python надала збалансоване середовище для створення сучасного, захищеного та кросплатформного застосунку, забезпечивши оптимальне співвідношення продуктивності, функціональності та рівня безпеки.

Розроблене програмне забезпечення побудоване за модульною архітектурою, що забезпечує чіткий розподіл функціональних обов'язків, підвищує масштабованість та спрощує супровід системи. Структура складається з чотирьох основних підсистем: ядра, моделей даних, сервісних компонентів і графічного інтерфейсу.

Ядро (core) реалізує основні операції зі сховищем, включно з генерацією криптографічних ключів на основі PBKDF2-HMAC-SHA256 та шифруванням даних за алгоритмом ChaCha20-Poly1305. Сховище представлено єдиним зашифрованим файлом, що містить параметри криптографічної сесії та зашифрований вміст.

Моделі даних (models) описують типи записів (акаунти, картки, документи, нотатки), які уніфіковано представлені через базовий клас та можуть містити вкладені файли у форматі base64.

Сервісні модулі (services) забезпечують керування записами, обробку вкладень, тимчасове копіювання конфіденційних даних у буфер обміну та контроль неактивності користувача.

Графічний інтерфейс (gui) включає вікна аутентифікації, основне робоче середовище, панелі перегляду та діалоги налаштувань, забезпечуючи доступність функцій у зрозумілому інтерактивному форматі.

Розроблена система використовує повне симетричне шифрування всього сховища, зберігаючи всі конфіденційні дані в одному файлі без жодної інформації у відкритому вигляді. Для шифрування застосовано алго-

ритм ChaCha20-Poly1305, який забезпечує як конфіденційність, так і автентифікацію даних.

Ключ генерується шляхом перетворення майстер-пароля через PBKDF2-HMAC-SHA256 із використанням випадкової солі. Структура файлу включає salt, nonce та ciphertext, що гарантує коректність і безпеку відновлення даних.

Процедури шифрування й розшифрування складаються з послідовних етапів: серіалізації та десеріалізації структури сховища, генерації криптографічних параметрів, шифрування/дешифрування та формування підсумкового файлу. Усі помилки автентифікації блокують доступ до даних, унеможливлюючи їх читання при спотворенні вмісту або введенні неправильного пароля.

Система підтримує додавання вкладених файлів до будь-якого запису. Вкладення зберігається у вигляді текстового представлення (base64), що забезпечує сумісність із JSON-структурою та коректність подальшого шифрування.

Процес включає вибір користувачем файлу, перевірку його параметрів, кодування в base64, включення вкладення до моделі запису та повторне шифрування всього сховища. Тимчасові файли створюються лише на час перегляду та видаляються по завершенні сеансу. Обмеження на розмір вкладення забезпечують ефективність шифрування та швидкість роботи системи.

Запропоноване рішення забезпечує захищене збереження особистих записів і вкладень на основі сучасних криптографічних алгоритмів, поєднуючи зручність використання, гнучкість налаштувань і високий рівень надійності, що робить його придатним для особистих і професійних потреб.

Література

1. Моравський В., Ткачук Р. Л., Колос Н. М. Криптологія: сучасні тенденції та перспективи. Інформаційна безпека та інформаційні технології : зб. тез доповідей VI Всеукраїнської науково-практичної конференції молодих учених, студентів і курсантів. (Львів, 30 листопада 2023 р.). Львів : ЛДУБЖД, 2023. С. 130–133.

2. Балацька В.С., Ткачук Р.Л., Маслова Н.О. Еволюція КСЗІ та інтеграція блокчейн-технологій у кіберзахисті державних інформаційних систем України. Кібербезпека: освіта, наука, техніка. Спеціальний випуск : електронне фахове наукове видання Київ, 2025. № 2 (30). С. 316–332. DOI: https://doi.org/10.28925/2663-4023.2025.30.975

3. Казмірчук Є. Ткачук Р. Л. Тестування безпеки програмного коду. Інформаційна безпека та інформаційні технології : зб. тез доповідей V Всеукраїнської науково-практичної конференції молодих учених, студентів і курсантів. (Львів, 26 листопада 2021 р.). Львів : ЛДУБЖД, 2021. С. 43–45.

УДК 004.056.53:004.7

МЕТОДИ ЗАБЕЗПЕЧЕННЯ ЗАХИЩЕНОГО ВІДДАЛЕНОГО ДОСТУПУ ДО IOT-ІНФРАСТРУКТУРИ SOHO З ВИКОРИСТАННЯМ ПРИНЦИПІВ ZERO TRUST

Назарій БУРАК, Богдан ДМИТРУК,
Іван ДМИТРУК, Артем ГЕРАСИМЧУК
Львівський державний університет безпеки життєдіяльності

Анотація. *У роботі досліджено проблему вразливості IoT-пристроїв у домашніх мережах (SOHO) та запропоновано архітектуру захищеного віддаленого доступу, що базується на принципах «нульової довіри» (Zero Trust). З використанням середовища симуляції Cisco Packet Tracer розроблено та протестовано трирівневу систему захисту, яка включає ізоляцію на рівні хоста, мінімізацію поверхні атаки через Port Forwarding та захист бездротового сегмента. Результати тестування підтвердили ефективність запропонованого підходу проти зовнішніх загроз та компрометації внутрішніх пристроїв.*

Ключові слова: *інтернет речей (IoT), SOHO, Zero Trust, інформаційна безпека, Cisco Packet Tracer, ESP32, фаєрвол.*

Abstract. *The paper investigates the vulnerability of IoT devices in Small Office/Home Office (SOHO) networks and proposes a secure remote access architecture based on Zero Trust principles. Using the Cisco Packet Tracer simulation environment, a three-level protection system was developed and tested, incorporating host-level isolation, attack surface reduction via Port Forwarding, and wireless segment protection. Test results confirmed the effectiveness of the proposed approach against external threats and internal device compromise.*

Keywords: *Internet of Things (IoT), SOHO, Zero Trust, information security, Cisco Packet Tracer, ESP32, firewall.*

Стрімке поширення пристроїв Інтернету речей (IoT) у домашніх мережах (SOHO — Small Office/Home Office) створює нові вектори загроз. Бюджетні IoT-пристрої (наприклад, на базі ESP32) часто мають обмежені можливості шифрування та вразливі прошивки. Класичний захист на рівні периметра (роутера) є недостатнім, оскільки компрометація одного пристрою в "плоскій" мережі ставить під загрозу критичні сервери.

Метою роботи є розробка архітектури захищеного віддаленого доступу до домашнього сервера та IoT-пристроїв, що базується на принципах "нульової довіри" (Zero Trust). Для моделювання мережі використано середовище Cisco Packet Tracer. Топологія мережі включає: сегмент глобальної мережі (WAN) з імітацією зовнішнього клієнта ("Hacker/Remote User") та локальний сегмент (LAN) з сервером керування, клієнтськими пристроями та IoT-контролером (SBC/ESP32).

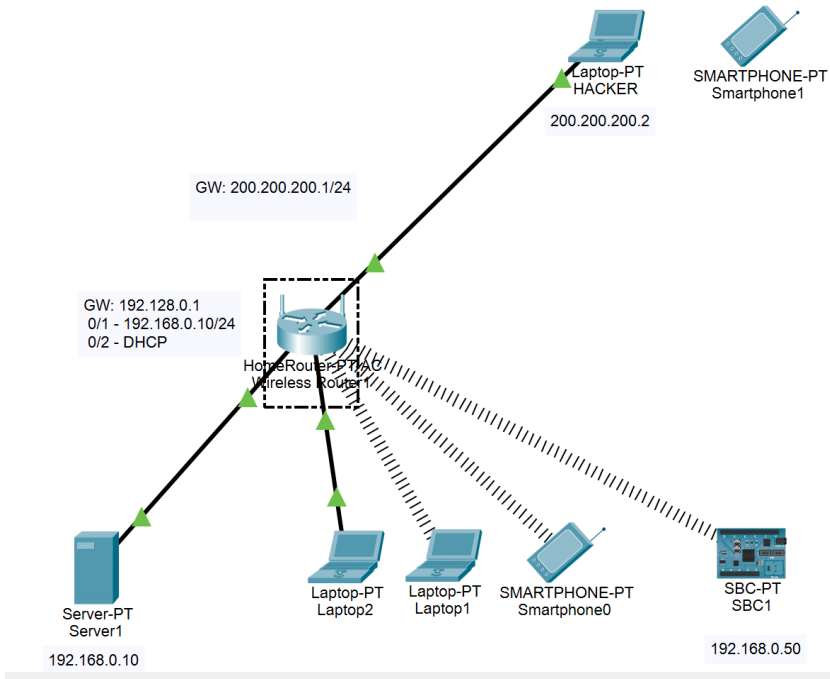

Рисунок 1 – Топологія мережі в середовищі Cisco Packet Tracer з виділеним WAN та LAN сегментами.

В ході дослідження реалізовано трирівневу систему захисту:

Захист бездротового середовища. Використано стандарт WPA2-PSK (AES) у поєднанні з приховуванням ідентифікатора мережі (Hidden SSID). Це ускладнює пасивний моніторинг ефіру та автоматизовані атаки на підбір паролів.

Мінімізація поверхні атаки (Attack Surface Reduction). На межовому маршрутизаторі налаштовано статичну трансляцію адрес (NAT/Port Forwarding) виключно для порту TCP/80. Це забезпечує доступність веб-інтерфейсу керування ззовні, залишаючи IoT-контролери та внутрішні сервіси (SMB, FTP) невидимими для зовнішнього сканування.

Реалізація Zero Trust на рівні хоста. Оскільки бюджетні маршрутизатори не підтримують VLAN, ізоляцію реалізовано на рівні сервера. Налаштовано Host-based Firewall з політикою "White-list": дозволено лише вхідний трафік HTTP та ICMP.

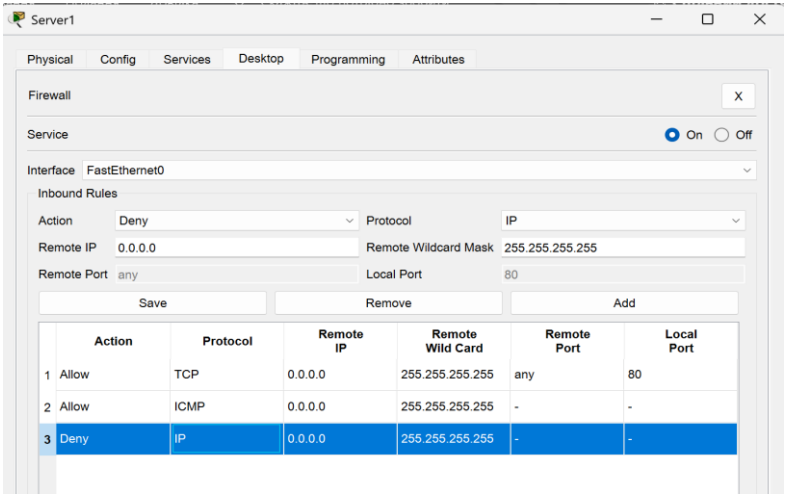

Рисунок 2 – Конфігурація Host-based Firewall на сервері керування (політика білого списку)

- **Сценарій легітимного доступу:** Зовнішній клієнт успішно отримує доступ до веб-панелі керування через публічну IP-адресу.
- **Сценарій внутрішньої загрози (Insider Threat):** Спроба скомпрометованого внутрішнього пристрою (ноутбука в тій же підмережі) отримати доступ до файлової системи сервера через протокол FTP була автоматично заблокована фаєрволом, незважаючи на відсутність мережевої сегментації.
- **Ізоляція IoT:** Контролер ESP32 недоступний з глобальної мережі, керування ним здійснюється виключно через захищений сервер-посередник.

Висновки. Запропонована архітектура дозволяє забезпечити високий рівень безпеки в мережах SOHO без використання дорогого корпоративного обладнання. Перенесення логіки захисту з периметра мережі на кінцеві точки (Server Endpoint) дозволяє ефективно протидіяти атакам навіть у випадку проникнення зловмисника всередину локальної мережі.

Література

1. **What is Zero Trust?** *Cloudflare Learning Center*. URL: https://www.cloudflare.com/learning/security/glossary/what-is-zero-trust/

2. **Building an Efficient Small Office/Home Office (SOHO) Network.** *Cisco Learning Network*. URL: https://learningnetwork.cisco.com/s/question/0D56e0000EBteL5CQJ/ building-an-efficient-small-officehome-office-soho-network

3. **From Smartphones to Smart Homes: Extending Mobile Security to IoT Devices.** *ESET Blog*. URL: https://www.eset.com/za/about/newsroom/press-releases-za/blog/from-smartphones-to-smart-homes-extending-mobile-security-to-iot-devices/

УДК 004.056.5

INTEGRATING THREAT MODELING AS CODE INTO GITOPS WORKFLOWS WITH AI SUPPORT IN DEVSECOPS PIPELINES

Oleksandr VAKHULA
Lviv Polytechnic National University

Abstract. *This thesis proposes a framework for embedding Threat Modeling as Code (TMaaC) into GitOps-based DevSecOps pipelines with AI-assisted analysis. Threat models are captured in machine-readable, version-controlled formats and processed by LLM-based agents to generate threats and mitigations automatically. We detail the system architecture, including how AI agents consume and update threat-model artifacts, and how GitOps pipelines enforce continuous validation. Our contributions include a methodology that formalizes threat modeling into an automated DevSecOps workflow.*

Keywords: *threat modeling as code, GitOps, DevSecOps, AI agents, security automation.*

Анотація. *У тезі запропоновано систему інтеграції моделювання загроз у вигляді коду (TMaaC) з GitOps-воркфлоу та AI-підтримкою у DevSecOps. Формалізовані моделі загроз (у YAML/JSON) версіонуються і автоматично аналізуються за допомогою AI-агентів. Описано архітектуру системи, взаємодію AI з артефактами моделі загроз та роль GitOps-пайплайнів у безперервному забезпеченні безпеки.*

Ключові слова: *моделювання загроз як код, GitOps, DevSecOps, штучний інтелект, автоматизація безпеки.*

1. Introduction. Security initiatives must shift left to catch design-level flaws early in development. Traditional threat modeling is performed manually (workshops, DFDs, STRIDE analysis) and often disconnected from automated pipelines. Threat modeling should occur “from the very early stages” of design, but remains a complex, expert-driven task . Manual approaches are costly and error-prone. Integrating threat modeling into DevSecOps addresses this gap. By treating threat models as code (TMaaC) - using structured, versioned formats – we enable continuous, automated analysis.

2. Methodology. The proposed system integrates Threat Modeling as code into a GitOps-style CI/CD pipeline. Design artifacts (architecture diagrams, OpenAPI specs, IaC templates) reside in a Git repository. On each commit or pull request, a CI process invokes an AI-based Threat Modeling Engine. This may include LLM-powered agents or parsers (e.g. Threagile or custom LLM chain) that analyze the code and specifications to generate or update a structured threat model (in YAML/JSON). The threat model describes assets, trust boundaries, data flows, and identified threats. The AI agent augments the model by proposing new threats and mitigations, leveraging contextual knowledge and

threat libraries. All TMaaC artifacts are stored back in Git, enabling version control and code review of threat analysis.

Meanwhile, the GitOps pipeline (using tools like ArgoCD, Flux or Jenkins) continuously reconciles both application infrastructure and the TMaaC repository with the desired state. GitOps agents compare the live environment against the Git-stored specifications. If the AI agent has updated the threat model (for example by discovering a new vulnerability pattern), the pipeline can automatically trigger downstream tasks: it may apply policy-as-code rules (e.g. OPA/Gatekeeper policies derived from the model) or generate compliance tickets if critical threats lack controls. The pipeline enforces checks: for instance, a build may fail if the TMaaC analysis flags an unmitigated high-severity threat. Additionally, the pipeline can feed the threat model into Controls Mapping modules: generating firewall/WAF rules, Sigma alerts for SIEM, or Jira issues linking threats to countermeasures.

In this way, AI agents interact with threat artifacts throughout the flow. On code changes, AI agents parse updated diagrams or code and refresh the TMaaC document, then create Git commits or PRs for peer review. Conversely, existing threat model entries guide the deployment: the pipeline can align infrastructure changes with the TMaaC definitions. For example, if the TMaaC YAML indicates a database containing PII is exposed, the pipeline might enforce encryption policies or network controls as specified in code. Overall, the GitOps pipeline provides the automation backbone: it treats threat models as first-class inputs, ensuring that any change to the system (code or TMaaC) triggers a reproducible, auditable build and deployment sequence. This creates a continuous feedback loop where security analysis (via AI and TMaaC) is part of the normal Git-based workflow.

3. Comparison with traditional Threat modeling. This thesis core contribution is demonstrating how TMaaC transforms threat analysis into a reproducible, automatable discipline, contrasting sharply with traditional methods. In conventional threat modeling, teams manually construct diagrams and checklists, often in an ad-hoc way. Such models are typically not version-controlled or integrated with CI/CD, making them hard to update or reuse. By contrast, TMaaC formalizes the model: threats, assets, and controls are encoded in machine-readable form. This formalization enables automated reasoning and precise verification . For example, formal threat specifications can be fed to tools that automatically verify if the current configuration violates any defined security property.Integration into automated workflows is another key advantage. TMaaC pipelines can automatically generate mitigation checks and policy rules, linking security directly to code commits. Traditional threat modeling usually happens in isolation, without CI/CD enforcement. With TMaaC, threat analysis is continuous and “shifted left”: builds can break if security rules from the model aren’t satisfied. This tightly couples design intent and implementation. As one

source emphasizes, embedding threat modeling into DevSecOps provides a tactical advantage for proactive defense . By codifying security knowledge (often using policy-as-code and AI), our approach embeds security gates into GitOps operations, whereas manual methods lack such automation.

4. Conclusion. We have presented an approach to integrate Threat Modeling as Code into GitOps-based DevSecOps pipelines. By treating threat models as formal, version-controlled artifacts and augmenting them with AI-driven analysis, our methodology makes threat modeling iterative, automated, and reproducible. The expanded methodology section described a pipeline architecture where AI agents generate and refine threat-model code, while GitOps ensures continuous validation and deployment of security controls. The scientific evaluation highlighted TMaaC's benefits in enabling formalized, repeatable security analysis versus traditional manual techniques. In future work, we will prototype this architecture and evaluate its effectiveness on real-world case studies. Embedding TMaaC into automated workflows promises to significantly improve secure design practices and resilience of deployed systems.

Література

1. O. Vakhula, I. Opirskyy, O. Mykhaylova. "Research on Security Challenges in Cloud Environments and Solutions based on the 'Security-as-Code' Approach." In Proc. of CPITS 2023-II, CEUR Workshop Proc. Vol-3550, pp. 55–69, 2023.

2. O. Vakhula, I. Opirskyy. "Research on Security as Code Approach for Cloud-Native Applications based on Kubernetes Cluster." In Proc. of CSDP 2024, CEUR Workshop Proc. Vol-3800, pp. 58–69, 2024.

3. OWASP Foundation, "Threat Modeling Manifesto," 2024. [4] GitHub Actions Documentation, "Workflow Automation for DevSecOps," 2025.

УДК 004.056

АНАЛІЗ КОМПЛЕКСНОГО ПІДХОДУ ДО ЗАБЕЗПЕЧЕННЯ ЦІЛІСНОСТІ ТА БЕЗПЕКИ РОЗГОРТАННЯ ХМАРНИХ КОНТЕЙНЕРИЗОВАНИХ ЗАСТОСУНКІВ

Володимир ГАВРИЛЯК, Юрій КУЛИК, Богдан СКОРИНОВИЧ
Національний університет «Львівська політехніка»

Анотація. *В даній роботі досліджено проблематику захисту ланцюга постачання контейнеризованих застосунків. Обґрунтовано доцільність застосування стратегії "Shift-Left" для нівелювання ризиків мікросервісної архітектури. Пропонується комплексний механізм безпечного розгортання контейнерів, що включає мінімізацію базових образів, автоматизований статичний аналіз вразливостей, криптографічну верифікацію їх цілісності та суворе обмеження привілеїв середовища виконання.*

Ключові слова. *безпека контейнеризації, ланцюг постачання ПЗ, DevSecOps, управління вразливостями, хмарні реєстри, Docker Content Trust, принцип найменших привілеїв.*

Abstract. *The research addresses security issues within the supply chain of containerized applications, arguing for the implementation of the "Shift-Left" strategy to neutralize microservice risks. The paper proposes a holistic secure deployment framework that integrates base image minimization, automated static analysis, cryptographic integrity verification, and rigorous runtime privilege enforcement.*

Keywords. *container security, software supply chain, DevSecOps, vulnerability management, cloud registries, Docker Content Trust, least privilege principle.*

Вступ. Зміна парадигми розгортання застосунків від монолітних архітектур до мікросервісів де-факто затвердила контейнери як стандарт для доставки програмного забезпечення. Хоча контейнеризація пропонує безпрецедентну гнучкість та портативність, вона створює нову та складну поверхню атаки, яку традиційні моделі безпеки часто не можуть охопити.

Однією із причин є те, що безпечне розгортання образу Docker не може бути досягнуте лише шляхом ізоляції під час використання. Натомість, необхідно впроваджувати стратегію "Shift-Left", яка ґрунтується на суворих стандартах безпеки на кожному етапі ланцюга постачання контейнерів [1].

Мінімізація поверхні атаки. Фундаментальним вектором захисту контейнерів є оптимізація базового образу. Використання дистрибутивів загального призначення (наприклад, повних версій Ubuntu) призводить до надлишкової кількості бінарних файлів та системних бібліотек, що розширює можливості експлуатації вразливостей цих компонентів. Саме тому, доцільним є використання образів із мінімальним набором утиліт (Alpine Linux) або спеціалізованих образів типу "Distroless", які позбавлені оболонки shell. Реалізація та-

кого принципу дозволяє нівелювати загрози класу "living-off-the-land", оскільки відсутність непотрібних пакетів та бібліотек ускладнює виконання зловмисного коду навіть у випадку компрометації додатка.

Верифікація на етапі збірки: Статичний аналіз та управління секретами. Критичним етапом забезпечення цілісності контейнерів є імплементація автоматизованих перевірок у конвеєри CI/CD.

- ***Автоматизований аналіз вразливостей***. Згідно з сучасними стандартами, статичний аналіз (SAST) та сканування контейнерів мають бути обов'язковими етапами захисту ланцюга постачання [1]. Варто зазначити, що результати сканування можуть варіюватися залежно від обраного інструментарію та бази сигнатур, що підтверджується порівняльними дослідженнями ефективності різних сканерів [2]. З огляду на це, пропонується використання політики "Breaking the Build" при виявленні CVE з рівнем критичності, що перевищує встановлений поріг. Додатковою рекомендацією є генерація SBOM (Software Bill of Materials) для забезпечення прозорості компонентного складу образів.
- ***Робота з секретами***. Архітектурна особливість Docker (Layer Caching) робить неприпустимим зберігання конфіденційних даних (API-ключів, сертифікатів) всередині образу. Його багатошарова природа спричиняє те, що зберігання секретів в одному кроці і видалення в наступному не призводить до їх зникнення з історії образу. Єдиним загальноприйнятим підходом є ін'єкція секретів під час виконання контейнера (runtime injection) через механізми оркестрації або спеціалізовані сховища (Vault) [3].

Розповсюдження та зберігання: Забезпечення цілісності та контролю доступу. Після етапу збірки образ завантажується до реєстру контейнерів, який у сучасних корпоративних середовищах реалізується на базі керованих хмарних сервісів, таких як AWS ECR, Azure ACR або Google Artifact Registry. Відповідно, такий підхід передбачає обов'язкове шифрування сховища та впровадження політик контролю доступу (IAM/RBAC) для мінімізації ризику несанкціонованої модифікації образів або їх підміни третіми сторонами[4].

Паралельно з контролем доступу до сховища, необхідно гарантувати логічну цілісність його вмісту через механізми Docker Content Trust (DCT). Використання цифрових підписів дозволяє верифікувати авторство коду та захистити від атак типу "Man-in-the-Middle" під час передачі даних. Додатковою перевагою використання хмарних реєстрів контейнерів є можливість безперервного сканування завантажених образів, що дозволяє оперативно виявляти вразливості, інформація про які з'явилася у базах CVE вже після завершення процесу збірки (так звані Zero-Day загрози). Це перетворює реєстр із пасивного сховища на активний інструмент моніторингу [2].

Конфігурація середовища виконання. Захист ланцюга постачання був би неповним без розгляду аспекту "Runtime". Навіть перевірений та без-

печний образ може бути скомпрометований через слабку конфігурацію оркестратора. Критично важливим є дотримання принципу найменших привілеїв: безумовна заборона запуску процесів від імені користувача “root”, використання механізмів “securityContext” для відключення зайвих повноважень ядра та монтування кореневої файлової системи в режимі "лише для читання" (Read-Only). Такий комплексний підхід унеможливлює закріплення зловмисника в системі, гарантуючи стійкість такої інфраструктури.

Висновки. Проведене дослідження дозволяє стверджувати, що безпека розгортання контейнеризованих застосунків є ітеративним процесом, а не статичним станом системи. Комплексна імплементація запропонованих заходів - починаючи з мінімізації базового образу та автоматизованого аналізу вразливостей і не обмежуючись криптографічною верифікацією та обмеженням привілеїв дозволяє забезпечити належний рівень захищеності нативних хмарних додатків без втрати гнучкості розробки.

Література

1. Кулик Ю. А., Скоринович Б. В., Гавриляк В. Р. Безсерверні та контейнеризовані архітектури: порівняльний аналіз підходів до безпеки // Безпека сучасних інформаційно-комунікаційних систем, SMICS: матеріали Міжнародної науково-технічної конференції, м. Львів, 16–18 жовтня 2025 р. – 2025. – С. 188–193.

2. B. Boles, E. O'Donoghue, A. Redempta Manzi Muneza, G. Perkins, C. Izurieta and A. Marie Reinhold, "Deciphering Discrepancies: A Comparative Analysis of Docker Image Security," 2024 IEEE International Conference on Source Code Analysis and Manipulation (SCAM), Flagstaff, AZ, USA, 7-8 жовтня 2024, С. 254-259.

3. Center for Internet Security (CIS), "CIS Docker Benchmark v1.8.0" Серпень. 2025.

4. Скоринович Б. В., Гавриляк В. Р., Кулик Ю. А. ВИКЛИКИ ТА ПЕРСПЕКТИВИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В УМОВАХ “CLOUD NATIVE” АРХІТЕКТУР // Інформаційне суспільство: технологічні, економічні та технічні аспекти становлення : матеріали міжнародної наукової інтернет-конференція, 14–15 травня 2025 р., Тернопіль, Україна, Ополе, Польща. – Вип. 99. – 2025. – С. 49–53.

УДК 004.056.5:004.7

МЕТОД ОЦІНКИ ЯКОСТІ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ ЗАХИСТУ ІНФОРМАЦІЇ У КОМП'ЮТЕРНИХ МЕРЕЖАХ

Роман ГАМРЕЦЬКИЙ[1], Віктор ГНАТЮК[2]
Державний університет «Київський авіаційний інститут»[1]
Державний науково-дослідний інститут технологій кібербезпеки та захисту інформації[2]

Анотація. *У роботі запропоновано метод кількісної оцінки якості програмного забезпечення, що реалізує функції захисту інформації в комп'ютерних мережах. Метод поєднує ISO/IEC 25010 з домен-специфічними мережевими метриками та трирівневою структурою (сервісний, функціональний, інфраструктурний рівні) для порівняння рішень і виявлення критичних компонентів.*

Ключові слова: *захист інформації; комп'ютерні мережі; якість програмного забезпечення; оцінювання якості; ISO/IEC 25010; мережеві метрики; віртуалізація.*

Abstract. *The paper presents a method for quantitative quality assessment of software that implements information security functions in computer networks. The method combines ISO/IEC 25010 with domain-specific network metrics and a three-level structure (service, functional, infrastructural) to compare solutions and detect bottlenecks.*

Keywords: *information security; computer networks; software quality; quality assessment; ISO/IEC 25010; network metrics; virtualization.*

У сучасних комп'ютерних мережах захист інформації значною мірою визначається властивостями програмного забезпечення (ПЗ), яке реалізує маршрутизацію, фільтрацію та шифрування трафіку, контроль доступу, сегментацію мережі, моніторинг і аудит подій безпеки. Від якості такого ПЗ залежить здатність мережі забезпечувати конфіденційність, цілісність і доступність інформації, протидіяти кібератакам, локалізовувати інциденти та підтримувати заданий рівень сервісу для користувачів і прикладних систем.

Класичні моделі оцінки якості ПЗ (ISO/IEC 25010 та ін.) задають загальну рамку для аналізу характеристик ПЗ, таких як функціональна придатність, надійність, продуктивність, безпека, супроводжуваність, портативність. Однак у контексті захисту інформації в комп'ютерних мережах (КМ) вони потребують доповнення домен-специфічними показниками, які прямо відображають вимоги до конфіденційності, цілісності та доступності (CIA), а також специфіку мережевих сервісів і архітектур (розподіленість, наявність віртуальних сегментів, гібридні хмарні середовища тощо).

Метою доповіді є вдосконалення та адаптація методу оцінки якості ПЗ, орієнтованого на задачі забезпечення захисту інформації в КМ, з можливістю кількісного порівняння альтернативних рішень і відстеження змін якості в процесі експлуатації.

Запропонований метод ґрунтується на поєднанні стандартних характеристик якості за ISO/IEC 25010 з домен-специфічними метриками. До таких метрик належать:

– мережеві показники: затримка та варіація затримки при обробці трафіку, пропускна здатність, відсоток втрачених пакетів, доступність сервісів;

– показники стійкості: відмовостійкість (резервування вузлів і каналів, кластерні конфігурації, автоматичне переключення при збоях), стійкість до атак типу DoS/DDoS, здатність до роботи в умовах часткових відмов;

– показники безпеки та моніторингу: повнота та детальність журналювання подій, наявність механізмів кореляції та аналізу інцидентів, ефективність виявлення аномалій;

– показники ефективності: використання ресурсів ЦП, оперативної пам'яті та мережевих інтерфейсів, масштабованість при зростанні навантаження.

Метод реалізує трирівневу структуру оцінювання:

– Сервісний рівень – аналізується відповідність характеристик мережевих сервісів (пропускна здатність, затримка, доступність, втрата пакетів) вимогам до захисту інформації та узгодженим параметрам SLA. Окремо враховується вплив активації функцій безпеки на якість обслуговування користувачів.

– Функціональний рівень – оцінюється коректність реалізації функцій, що безпосередньо впливають на захист інформації: ідентифікація й автентифікація суб'єктів доступу, авторизація, реалізація політик доступу, фільтрація трафіку, підтримка списків контролю доступу, механізми виявлення та блокування підозрілої активності, захист від типових мережевих атак.

– Інфраструктурний рівень – розглядається робота ПЗ у віртуалізованому середовищі, включаючи відмовостійкість (резервування, кластери, сценарії переключення), можливості горизонтального та вертикального масштабування, а також ефективність використання обчислювальних і мережевих ресурсів у різних сценаріях навантаження.

Для кожного рівня формується набір часткових метрик, які нормуються до єдиної шкали (наприклад, [0;1]). Вагові коефіцієнти визначаються з урахуванням важливості конкретної метрики для забезпечення конфіденційності, цілісності та доступності інформації в заданому класі мережі (корпоративна мережа, дата-центр, промислова мережа, віддалений доступ тощо). Зміна ваг дозволяє адаптувати метод до різних профілів ризику без модифікації базового набору метрик. Особливістю методу є можливість його використання як у статичному режимі (разова оцінка якості перед

впровадженням або після оновлення ПЗ), так і в динамічному режимі, коли збір метрик відбувається безперервно в процесі експлуатації.

Експериментальне дослідження методу виконано на стенді, розгорнутому у віртуалізованому середовищі Proxmox VE. До складу стенду включено типові компоненти, що використовуються для захисту інформації в КМ: міжмережевий екран, VPN-шлюз для організації захищеного віддаленого доступу, систему виявлення та запобігання вторгненням, сервер збору, зберігання та аналізу журналів подій. Окремі віртуальні машини імітують користувацькі хости та зовнішні вузли, з яких генерується як легітимний, так і потенційно шкідливий трафік.

У межах експериментів розглянуто кілька сценаріїв функціонування мережевої інфраструктури: нормальний режим з номінальним навантаженням; режим пікового навантаження з великою кількістю одночасних з'єднань; сценарії часткових відмов (відключення окремих віртуальних вузлів, деградація каналів зв'язку); а також сценарії появи аномального або шкідливого трафіку, спрямованого на порушення доступності або конфіденційності інформації.

Аналіз результатів показав, що запропонований метод дозволяє виявляти критичні компоненти у реалізації функцій, важливих для захисту інформації, а також своєчасно фіксувати деградацію параметрів, критичних з точки зору вимог до конфіденційності, цілісності й доступності даних.

Метод оцінки якості ПЗ є інструментом підтримки прийняття рішень у задачах забезпечення захисту інформації в КМ. Він дозволяє виконувати кількісно обґрунтоване порівняння альтернативних конфігурацій, сценаріїв розгортання та варіантів модернізації програмних компонентів систем захисту.

Література

1. ISO/IEC 25010:2023 Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — System and software quality models. Geneva: International Organization for Standardization, 2023.

2. Гамрецький Р., Гнатюк В. Метод оцінки якості програмного забезпечення ядра 5G // Herald of Khmelnytskyi National University. Technical Sciences. 2025. № 4 (355). С. 106–111.

3. Гамрецький Р., Гнатюк В. Огляд та аналіз методів та моделей оцінки якості програмного забезпечення в інформаційно-комунікаційних системах // Наукоємні технології. 2025. Т. 64, № 4. С. 435–448. DOI: 10.18372/2310-5461.63.19752.

4. Bondarenko L., Masesov M., Buzayeva K., Hurzhii I., Ilienko O., Gnatyuk V. Method of calculation the accessibility of the information and telecommunication networks of the tactical link of management // International Journal of Computer Networks and Information Security. 2021. Vol. 13, No. 5. P. 68–78. DOI: 10.5815/ijcnis.2021.05.06.

УДК 004.056

ЗАСТОСУВАННЯ ГЕНЕРАТОРІВ ВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ З ПУАССОНІВСЬКИМ ЗАКОНОМ РОЗПОДІЛУ В СИСТЕМАХ ЗАХИСТУ ІНФОРМАЦІЇ

Олег ГАРАСИМЧУК
Національний університет «Львівська політехніка»

Анотація. *У роботі розглянуто застосування генераторів випадкових послідовностей із пуассонівським розподілом у галузі інформаційної безпеки та кіберзахисту. Показано ефективність таких генераторів у моделюванні кібератак, виявленні аномалій мережевого трафіку, рандомізації криптографічних процесів та формуванні бітових шаблонів для автентифікації пристроїв.*
Ключові слова: *Пуассонівський розподіл; генератори випадкових послідовностей; кіберзахист; атаки, аномалії трафіку; автентифікація пристроїв.*

Abstract. *The paper considers the application of random sequence generators with Poisson distribution in the field of information security and cyber defense. The effectiveness of such generators in modeling cyber attacks, detecting network traffic anomalies, randomizing cryptographic processes, and forming bit patterns for device authentication is shown.*
Keywords: *Poisson distribution; random sequence generators; cyber defense; attacks, traffic anomalies; device authentication.*

Сучасні системи кіберзахисту працюють в умовах постійної динаміки загроз, де важливо не лише забезпечити криптографічну стійкість, але й ускладнити для зловмисника прогнозування поведінки системи. На сьогоднішній день генератори псевдовипадкових послідовностей широко використовуються в системах захисту інформації, але як правило найбільш популярними є генератори, що генерують псевдовипадкові послідовності з рівномірним законом розподілу [1]. Хоча варто також відзначити, що й генератори, на виході яких отримуються послідовності з іншими, відмінними від рівномірного, законами розподілу, також знаходять своє місце для вирішення різноманітних задач захисту інформації. Одним із перспективних та математично обґрунтованих інструментів для цього є генератори подій, що підпорядковуються пуассонівському закону розподілу. Такий процес описує появу незалежних подій з певною середньою інтенсивністю та широко використовується в теорії масового обслуговування та аналізі мережевого трафіку.

Пуассонівський процес характеризується тим, що події виникають незалежно одна від одної та з певною середньою інтенсивністю. Для систем інформаційної безпеки це відкриває можливості побудови непередба-

чуваних алгоритмів, де час і частота генерації ключових подій не піддаються тривіальному аналізу.

Пуассонівський процес визначається формулою:

$$P(N(t) = k) = \frac{(\lambda t)^k e^{-\lambda t}}{k!},$$

де λ — інтенсивність подій, t — час.

Простий пуассонівський потік, який володіє наступними трьома основними властивостями [2]:

– властивістю стаціонарності;

– властивістю відсутності післядії;

– властивістю ординарності.

Для генераторів імпульсних послідовностей з пуассонівським законом розподілу можна виокремити наступні напрями застосування в системах захисту інформації:

1. Рандомізоване керування криптографічними операціями

У сучасних криптографічних системах важливо забезпечити не лише безпеку ключів, а й непередбачуваність їхнього оновлення. Генератори, засновані на пуассонівському розподілі, дозволяють формувати випадкові проміжки між оновленнями ключів, запускати ротацію сесійних параметрів та неперіодично перемикати алгоритми у багатокомпонентних криптосистемах.

Пуассонівський підхід забезпечує варіативність часу між подіями, при цьому зберігається контрольована середня інтенсивність λ. Коли фактичні інтервали суттєво коливаються, це створює складний для прогнозування графік ротації, що підвищує стійкість системи до потенційних атак та спроб передбачити поведінку криптографічного механізму.

Приклад: при λ = 0.2 система оновлює ключі в середньому раз на 5 секунд, однак реальні проміжки між оновленнями значно різняться, формуючи стохастично непередбачувану структуру ротації.

2. Моделювання фішингових атак

Фішинг залишається одним із найвірогідніших та найуспішніших способів компрометації організаційних систем, значною мірою через стійку залежність від людського фактора. Навіть за наявності сучасних технологій захисту саме користувачі залишаються ключовою вразливістю, що робить моделювання цього типу загроз важливим елементом кіберзахисту. Пуассонівський розподіл дозволяє описувати кількість фішингових електронних листів [3], отриманих за певний інтервал часу, оскільки такі події є незалежними та мають приблизно стабільну середню інтенсивність. Моделювання фішингових подій допомагає оцінити частоту атак, визначити пікові періоди активності та зрозуміти загальний розподіл навантаження. Отримані оцінки дають змогу точніше планувати ресурси, оптимізувати

роботу аналітиків та захисних систем, а також підготувати організацію до можливих сплесків фішингової активності. Таке використання пуассонівського процесу підсилює загальну стійкість системи до одного з найрозповсюдженіших типів кіберзагроз.

3. Моделювання мережевого трафіку та виявлення аномалій

У багатьох реальних мережах інтервали між прибуттям пакетів добре описуються пуассонівською моделлю, особливо коли йдеться про великі незалежні потоки даних [4]. Це дає змогу формувати статистично обґрунтовані «нормальні» профілі трафіку та використовувати їх як базову лінію для виявлення відхилень.

Пуассонівський підхід дозволяє фіксувати аномалії, зокрема різке збільшення інтенсивності потоку λ, що є характерною ознакою DDoS-атак або інших форм ненормальної активності. Коли реальний трафік перестає відповідати очікуваному розподілу, система може оперативно визначити ймовірність інциденту.

Приклад: якщо IDS очікує середню інтенсивність трафіку близько 2000 подій/хв, але спостерігає стрибок до 15 000/хв, така подія статистично малоймовірна для пуассонівського процесу, що стає підставою для негайного формування попередження.

4. Генерація одноразових паролів (OTP) на основі пуассонівських інтервалів.

У системах автентифікації важливим є не лише криптостійкість одноразових паролів, а й непередбачуваність моментів їх формування. Використання пуассонівського процесу дає змогу генерувати OTP у випадкові часові інтервали [5], що унеможливлює появу стабільних патернів, які могли б бути проаналізовані зловмисником.

Пуассонівський підхід дозволяє формувати часову модель, у якій кожне наступне значення OTP виникає з інтенсивністю λ, але фактичні інтервали залишаються варіативними. Завдяки цьому зменшується ризик таймінгових атак, а також ускладнюється прогнозування моменту появи наступного коду, що посилює захист як мобільних генераторів, так і VPN-шлюзів чи апаратних токенів.

Приклад: якщо система генерує OTP із середньою інтенсивністю $\lambda = 0.1$ (приблизно один код кожні 10 секунд), реальний час між появою паролів може значно коливатись. Це робить часову поведінку генератора статистично непередбачуваною та ускладнює будь-які спроби синхронізації атакувального сценарію.

5. Стохастичні механізми поведінки системи

У складних інфраструктурах важливо унеможливити для зловмисника побудову передбачуваної часової моделі поведінки захисних механізмів. Використання генераторів із пуассонівським розподілом дозволяє

формувати стохастичні інтервали між окремими подіями системи, роблячи її динаміку значно менш детермінованою.

Такий підхід застосовується для випадкового перемикання портів, динамічного вибору маршрутів руху трафіку, активації пасток (honeypots) у нерегулярні моменти часу, а також для рандомізації реакцій на спроби сканування мережі. Завдяки варіативним інтервалам між активностями система формує складний, статистично непередбачуваний профіль поведінки, що значно ускладнює розвідку та планування атаки.

Приклад: у системі, де події активації honeypot генеруються пуассонівським процесом, проміжки між такими активаціями суттєво коливаються, тому зловмисник не може створити достовірну часову модель активності оборонних механізмів.

6. Моделювання бітових шаблонів для автентифікації пристроїв

Пуассонівські послідовності можуть застосовуватися для формування унікальних бітових шаблонів, призначених для автентифікації електронних пристроїв обробки інформації. Використання імпульсних генераторів із пуассонівським законом дозволяє отримати варіативні та статистично стійкі послідовності, що ускладнюють відтворення або підробку автентифікаційних характеристик.

У запропонованому підході [6] генератор пуассонівських імпульсів побудований на модифікованому адитивному генераторі Фібоначчі, що забезпечує покращені статистичні властивості вихідних сигналів. Схема моделювання включає два генератори з різними значеннями керуючих параметрів: перший формує послідовність A, що моделює внутрішні властивості поточного шаблону пристрою, тоді як другий генератор створює послідовність B, яка відображає відмінності між шаблонами різних пристроїв. Об'єднання цих послідовностей за допомогою операції XOR дає змогу формувати унікальні та стабільні бітові шаблони.

Результати імітаційного експерименту для двох пристроїв підтвердили придатність такого підходу: сформовані шаблони забезпечують чітке розмежування між пристроями та можуть використовуватися для їх однозначної автентифікації в інформаційно-технічних системах.

Приклад: поєднання фрагментів пуассонівських послідовностей A та B дозволяє створити бітовий шаблон, який водночас зберігає унікальні характеристики пристрою та містить статистично стійкі відмінності від інших шаблонів, що унеможливлює підробку автентифікаційних даних.

Підсумовуючи можна зазначити, що генератори псевдовипадкових послідовностей з пуассонівським законом розподілу демонструють широкий спектр застосувань у системах захисту інформації та кібербезпеки – від моделювання фішингових атак і виявлення аномалій трафіку до рандомізації криптографічних процедур та автентифікації пристроїв. Їхня здатність формувати статистично обґрунтовані, але водночас непередбачувані

інтервали подій підвищує складність для зловмисників і посилює стійкість інформаційних систем. Саме тому застосування таких генераторів може суттєво розширити інструментарій сучасної кібероборони та сформувати перспективний напрям подальших розробок.

Література

1. Maksymovych, V.; Shabatura, M.; Harasymchuk, O.; Karpinski, M.; Jancarczyk, D.; Sawicki, P. Development of Additive Fibonacci Generators with Improved Characteristics for Cybersecurity Needs. Appl. Sci. 2022, 12, 1519. https://doi.org/10.3390/app12031519.

2. Генератори пуассонівських імпульсних послідовностей: монографія / В.М. Максимович, О.І. Гарасимчук, М.М. Мандрона, Р.Т. Смук, Ю.Б. Сторонський. – Львів: Видавництво Львівської політехніки, 2019. – 156 с. ISBN 978-966-941-304-8.

3. Estimating Phishing Email Frequency with the Poisson Distribution in Python: A Practical Guide for Cybersecurity Risk Assessment [Електронний ресурс]. – Режим доступу: https://cybervar360.com/2024/06/27/estimating-phishing-email-frequency-with-the-poisson-distribution-in-python-a-practical-guide-for-cybersecurity-risk-assessment/.

4. Andrea Baiocchi, "Stochastic Models for Network Traffic," in Network Traffic Engineering: Stochastic Models and Applications , Wiley, 2020, pp.71-130, doi: 10.1002/9781119632498.ch3.

5. R. H. Khan and J. Miah, "Performance Evaluation of a new one-time password (OTP) scheme using stochastic petri net (SPN)," 2022 IEEE World AI IoT Congress (AIIoT), Seattle, WA, USA, 2022, pp. 407-412, doi: 10.1109/AIIoT54504.2022.9817203.

6. Maksymovych, V.; Nyemkova, E.; Justice, C.; Shabatura, M.; Harasymchuk, O.; Lakh, Y.; Rusynko, M. Simulation of Authentication in Information-Processing Electronic Devices Based on Poisson Pulse Sequence Generators. Electronics 2022, 11, 2039. https://doi.org/10.3390/electronics11132039.

УДК 621.396

ПРОБЛЕМАТИКА ІНТЕРОПЕРАБЕЛЬНОСТІ СИСТЕМ РАДІОЗВ'ЯЗКУ СИЛ БЕЗПЕКИ ТА ОБОРОНИ ПІД ЧАС ЛІКВІДАЦІЇ НАСЛІДКІВ НАДЗВИЧАЙНИХ СИТУАЦІЙ

Назар ГУЛКОВСЬКИЙ, Володимир ПИЛИПЕНКО
Львівський державний університет безпеки життєдіяльності

Анотація. *Розглянуто критичну проблему відсутності єдиного комунікаційного простору між підрозділами ДСНС та службами взаємодії (Національна поліція, НГУ, екстрена медична допомога) під час ліквідації наслідків надзвичайних ситуацій. Проаналізовано основні технічні та процедурні бар'єри, що унеможливлюють прямий радіообмін. Запропоновано тактичні рішення та стратегічні шляхи уніфікації стандартів зв'язку.*

Ключові слова. *слова: радіозв'язок, інтероперабельність, ДСНС, управління силами, DMR, TETRA, шлюзи.*

Abstract. *The abstract examines the critical problem of the lack of a unified communication space between the State Emergency Service units and interacting services (National Police, National Guard, Emergency Medical Service) during the liquidation of the emergencies. The main technical and procedural barriers preventing direct radio exchange are analyzed. Tactical solutions based on gateways and strategic ways of unifying communication standards are proposed.*

Keywords. *radio communication, interoperability, SES of Ukraine, force management, DMR, TETRA, gateways*

В умовах сьогодення, коли Україна стикається з безпрецедентними викликами, пов'язаними з повномасштабною агресією, техногенними катастрофами та постійними ракетно-дроновими атаками цивільної та критичної інфраструктури, ефективність реагування на надзвичайні ситуації (далі - НС) виходить на перший план. Ключовим елементом, що забезпечує успішну ліквідацію наслідків НС, є стійке та надійне управління силами та засобами. Основою цього управління є організація зв'язку як між підрозділами Державної служби України з надзвичайних ситуацій (далі – ДСНС) так і зі службами взаємодії.

Однак, практика ліквідації масштабних НС, де залучаються підрозділи ДСНС, Національної поліції, Національної гвардії, Збройних Сил України та бригад екстреної медичної допомоги, виявляє системну проблему. Ця проблема — відсутність єдиного комунікаційного поля. Критичною проблемою залишається технічна неможливість прямого радіообміну між підрозділами різних служб, що працюють у зоні надзвичайної ситуації.

Актуальність даного дослідження полягає у необхідності ідентифікації та аналізу бар'єрів, що перешкоджають ефективній взаємодії систем

радіозв'язку різних відомств, та пошуку шляхів їх подолання.

Радіозв'язок в оперативно-рятувальних підрозділах є не просто засобом передачі інформації, а ключовим елементом взаємодії будь-якої НС. Він забезпечує:

1. Оперативне управління: забезпечення гарантованого доведення управлінських рішень та команд від керівного складу до виконавців.

2. Міжвідомча координація: синхронізація спільних дій між різними функціональними підсистемами та службами.

3. Інформаційна підтримка: безперервний моніторинг та обмін даними про зміни оперативної обстановки в режимі реального часу.

4. Безпека особового складу: забезпечення надійного каналу для передачі сигналів екстреного оповіщення та запиту допомоги.

Проте, коли на місці НС (наприклад, ракетний удар по цивільному об'єкту) одночасно працюють ДСНС, Поліція та Швидка, їхня координація часто відбувається не через прямий радіоефір, а через представників служб взаємодії у штабі з ліквідації НС, мобільні телефони (що ненадійно при перевантаженні мереж) або, в кращому випадку, через окремі виділені канали, які є не у всіх.

Оскільки кожна силова структура розбудовувала власну інфраструктуру зв'язку ізольовано, виходячи з галузевої специфіки та бюджетних обмежень, наразі ми спостерігаємо відсутність єдиного комунікаційного простору, що проявляється у двох ключових площинах, а саме: перший — технічна, яка полягає у використанні розрізнених апаратних платформ та відсутності уніфікації частотних діапазонів. Експлуатація відомчих систем зв'язку в розрізнених частотних діапазонах, унеможливлює технічно встановлення прямого радіоканалу між підрозділами різних служб. Ситуацію ускладнює невідповідність видів модуляції та стандартів передачі даних. У той час як ДСНС здійснює планову міграцію на цифрові платформи (зокрема, стандарту DMR), суміжні служби продовжують експлуатувати конвенціональні аналогові мережі, що унеможливлює їх інтеграцію в єдиний інформаційний канал.

Інша сторона проблеми полягає у відсутності єдиних правил радіообміну. Кожна служба керується власними інструкціями, використовуючи специфічні коди та термінологію, які часто є незрозумілими для представників інших відомств. Ситуацію ускладнюють відмінні принципи формування позивних та різні формати передачі повідомлень: від суворих військових стандартів до більш спрощених регламентів цивільних служб.

Подолання окреслених бар'єрів вимагає комплексного підходу, що поєднує термінові тактичні кроки з довгостроковою державною стратегією розбудови телекомунікацій.

На оперативно-тактичному рівні першочерговим завданням є забезпечення технічної інтеграції наявних засобів. Найбільш ефективним рі-

шенням є розгортання на базі мобільних пунктів управління (МПУ) апаратних комутаційних шлюзів (типу RoIP), здатних програмно об'єднувати різнорідні радіомережі — аналогові, DMR та TETRA — в єдині голосові конференції. Технічну складову необхідно підсилити організаційними заходами: забезпеченням керівників ліквідації НС багатодіапазонними терміналами зв'язку із заздалегідь запрограмованими каналами взаємодії, а також запровадженням обов'язкових спільних тренувань, де акцент робиться саме на відпрацюванні алгоритмів міжвідомчого радіообміну.

У стратегічній перспективі єдиним сталим рішенням є відмова від клаптикової інфраструктури на користь побудови єдиної національної системи цифрового радіозв'язку для сил безпеки та оборони. Цей шлях, що базується на сучасних стандартах (TETRA або LTE Critical Communications), вже успішно реалізовано в країнах ЄС та НАТО. Імплементація такої системи має супроводжуватися уніфікацією нормативної бази: прийняттям єдиних технічних регламентів для унеможливлення закупівлі несумісного обладнання та розробкою стандартизованих протоколів комунікації (SOPs) для всіх екстрених служб.

Підсумовуючи, слід наголосити, що відсутність інтероперабельності — це не суто технічна незручність, а критична вразливість системи цивільного захисту. Ефективність найсучаснішої рятувальної техніки нівелюється за умов комунікаційного хаосу, адже від швидкості та точності передачі інформації між відомствами напряму залежить час реагування та, як наслідок, кількість врятованих життів.

Література

1. Організація зв'язку в органах та підрозділах цивільного захисту : Навчальний посібник / О. Б. Лисенко, Ю. В. Грицай, Р. М. Ткаченко. Харків : Національний університет цивільного захисту України, 2023. 215 с.

2. Ковальський В. А., Петренко І. І. Проблеми інтероперабельності систем радіозв'язку екстрених служб України // Вісник Національного університету цивільного захисту України. Серія : Державне управління. 2022. Вип. 1 (16). С. 45–52.

3. Пилипенко В. Використання сучасних цифрових засобів радіозв'язку в системі Державної служби України з надзвичайних ситуацій // Проблеми та перспективи забезпечення цивільного захисту : матеріали міжнар. наук.-практ. конф. молодих учених. Черкаси : НУЦЗУ, 2025. С. 223

4. Заїка С. В., Мельник О. П. Порівняльний аналіз стандартів цифрового транкінгового радіозв'язку (DMR та TETRA) для потреб підрозділів МВС України // Збірник наукових праць Військового інституту телекомунікацій та інформатизації імені Героїв Крут. 2021. № 3 (71). С. 101–108.

5. Кодекс цивільного захисту України : Закон України від 02.10.2012 р. № 5403-VI. URL: https://zakon.rada.gov.ua/laws/show/5403-17.

УДК 004.056

РОЛЬ ОРГАНІЗАЦІЇ КЛЮЧА У ФОРМУВАННІ КРИПТОСТІЙКОСТІ КЛАСИЧНИХ МЕТОДІВ ШИФРУВАННЯ

Максим ГУМЕНЮК, Юрій СОЛОДЮК, Наталія МАСЛОВА, Орест ПОЛОТАЙ
Львівський державний університет безпеки життєдіяльності

Анотація. *Досліджено вплив організації ключа на криптостійкість класичних шифрів. Порівняння шифрів Цезаря та шифру Вернама показало, що стійкість визначається властивостями ключа — довжиною, випадковістю та одноразовістю застосування. Встановлено, що для шифру Цезаря модифікація алгоритму не усуває вразливості до криптоаналізу, тоді як шифр Вернама забезпечує інформаційно-теоретичну стійкість за умови використання випадкового одноразового ключа. Порушення цих вимог призводить до компрометації шифру.*
Ключові слова*: криптостійкість, шифр Цезаря, шифр Вернама, ключ, безпека даних.*

Abstract. *The study examines the impact of key organization on the cryptographic strength of classical ciphers. A comparison of the Caesar cipher and the Vernam cipher demonstrated that security is determined by the properties of the key — its length, randomness, and one-time use. It was established that modifying the Caesar cipher does not eliminate its vulnerability to cryptanalysis, whereas the Vernam cipher provides information-theoretic security only when a random one-time key is applied. Violation of these requirements leads to the compromise of the cipher.*
Keywords. *cryptographic strength, Caesar cipher, Vernam cipher, key, data security.*

У сучасній практиці інформаційної безпеки існує тенденція ототожнювати криптостійкість шифру з рівнем математичної складності алгоритму. Це призводить до ситуацій, коли шифрувальні системи, формально засновані на коректних криптографічних принципах, залишаються вразливими через недосконалі підходи до управління ключами: використання занадто коротких ключів, повторне застосування однакових ключів, детерміновані правила їх формування або передавання небезпечними каналами. У результаті криптоаналітичні атаки стають можливими не через слабкість алгоритму, а через неправильну організацію процесу ключового захисту. Ключ виступає центральним компонентом, що визначає межі криптостійкості шифру.

Актуальність. Дослідження впливу властивостей ключа на рівень захищеності є актуальним як з теоретичної, так і з прикладної позиції, оскільки навіть найпростіші математичні операції можуть забезпечити абсолютний рівень захисту за умови дотримання вимог до ключа.

Метою роботи є встановлення закономірностей між властивостями організації ключів (довжина, ентропія, одноразовість, спосіб застосування) та криптостійкістю класичних методів шифрування шляхом порівняльного аналізу зокрема шифру Цезаря та шифру Вернама.

Методика дослідження. Дослідження здійснювалось за такими показниками: довжина ключа, ентропія ключа, залежність ключа від структури алфавіту, та вплив повторного використання ключа на можливість відновлення відкритого тексту.

У шифрі Цезаря ключ є фіксованою константою (зсув по алфавіту), а його простір обмежений розміром алфавіту. Завдяки цьому криптоаналітик може передбачити межі можливих перетворень і виконати перебір ключів у скінченному діапазоні. Відомо [1], що статистичні характеристики мови у шифрі Цезаря не змінюються, що робить можливим застосування частотного аналізу без необхідності знати ключ. Таким чином, шифр Цезаря фактично не допускає зміни рівня криптостійкості через модифікацію ключа: навіть розширення алфавіту збільшує простір ключів лише лінійно, не впливаючи на структурну передбачуваність перетворень.

На відміну від інших класичних алгоритмів, криптостійкість шифру Вернама не є наслідком кількості або складності математичних операцій, а формується виключно властивостями ключа [2]. У випадку шифру Вернама (рис. 1), ключ — це послідовність випадкових елементів, довжина якої дорівнює довжині повідомлення. Стійкість алгоритму зростає разом із довжиною ключа і досягає максимально можливого рівня, коли ключ стає випадковим та рівним довжині повідомлення (рис. 2).

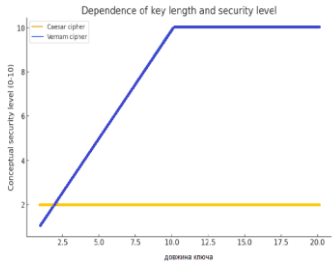

Рисунок 1 – Довжина ключа й стійкість алгоритмів

```python
def encrypt_decrypt_vernam(message, key):
    """
    Універсальна функція шифрування/розшифрування шифром Вернама (XOR).
    Працює з будь-яким Unicode-текстом.
    """
    #   Формуємо ключ до довжини повідомлення (або більше)
    key_stream = (key * (len(message) // len(key) + 1))[:len(message)]
    # XOR для кожного символу
    result = ''.join(chr(ord(m) ^ ord(k)) for m, k in zip(message, key_stream))
    return result


def generate_random_key(length):
    """
    Генерація криптографічно стійкого випадкового ключа.
    Повертає рядок символів (latin-1, бо 1 байт = 1 символ).
    """
    return secrets.token_bytes(length).decode('latin-1', errors='replace')
```

Рисунок 2 – Фрагмент програмного коду

Під час експериментальних обчислень підтверджено, що для випадкового і одноразового ключа неможливо отримати статистичний зв’язок між шифртекстом та відкритим текстом: для одного й того самого шифрте-

кcту, бо існує нескінченна кількість потенційних відкритих текстів, кожен із яких відповідає своєму можливому значенню ключа.

Показовими виявилися експериментальні випадки з повторним використанням ключа у шифрі Вернама. При повторі ключа з'являється залежність типу $C1 \oplus C2 = P1 \oplus P2$, яка є загрозою витоку інформації (C1, C2 – шифротекст, P1, P2 – відкриті повідомлення). Якщо при цьому хоча б частина одного з повідомлень стає відомою криптоаналітику, він може відновити ключ, а потім — всі повідомлення, у яких застосовано цей самий ключ. Таким чином, стійкість шифру Вернама є не властивістю алгоритму, а тільки наслідком правильної організації ключа: випадковість, довжина та одноразовість використання виступають необхідними та достатніми умовами. Структурний аналіз ключа продемонстрував, що саме ентропія ключа та відсутність повторів формують непередбачуваність алгоритму.

Зіставлення двох підходів показало, що структура алгоритму сама по собі не гарантує стійкість: у шифрі Цезаря збільшення складності трансформації не усуває передбачуваності, тоді як у шифрі Вернама одна й та сама операція XOR може забезпечити як повну стійкість, так і повну компрометацію залежно від режиму використання ключа.

Висновки. Шифр Цезаря та шифр Вернама належать до однієї історичної групи криптографічних алгоритмів (класичні), але демонструють різну стійкість в умовах зміни параметрів ключа. У дослідженні продемонстровано, що класичні шифри відображають два крайні сценарії: шифр Цезаря — приклад повної компрометованості методу через обмеження ключа, тоді як шифр Вернама — приклад абсолютної криптостійкості, досягнутої не ускладненням математичного перетворення, а коректною організацією ключа — випадковістю, довжиною та одноразовістю його використання. Таким чином, досліджені алгоритми шифрування демонструють різний рівень ефективності протидії криптоаналітичним атакам, але стійкість алгоритму ґрунтується не стільки на структурі шифрування, скільки на властивостях ключа, що контролює процес перетворення.

Література

1. Yarra Satya Sri Sowjanya, Nikitha Palakurthi, Punyamurthula V. Koushik, Marni Sriram, Vardhineedi Rajesh, N. Durga Deepti Priya. „Legacy Encryption: Unraveling the Caesar Cipher in Modern Data Security“ // International Journal of Scientific Research and Engineering Development. — 2025. — Vol. 8, Issue 2, March-April 2025. — С. 874-878. — URL: https://www.ijsred.com/volume8/issue2/IJSRED-V8I2P106.pdf

2. Kadum S. A. Developed OTP (One-Time Pad) Key Generation Method (2023) / S. A. Kadum // AIP Advances. — 2023. — Article No. 1823828. — DOI: https://doi.org/10.1063/5.0161788.

УДК 004.8

ПРОТОТИП КЛАСИФІКАЦІЇ ІНФОРМАЦІЇ ЗГІДНО З ВИМОГАМИ SOC 2 TYPE 2 ЗАСОБАМИ MICROSOFT FABRIC ТА AZURE AI FOUNDRY

Олег ДЕЙНЕКА
Національний університет «Львівська політехніка»

Анотація. *У статті описано розробку прототипу політики класифікації даних для відповідності стандарту SOC 2 Type 2, що забезпечує безпеку, доступність, цілісність обробки та конфіденційність даних. Використання хмарних сервісів Microsoft Azure з архітектурою Medallion дозволяє ефективно збирати, зберігати та обробляти як структуровані, так і неструктуровані дані. Інтеграція Microsoft Fabric і Azure OpenAI Foundry автоматизує виявлення сенситивної інформації і її безпечне зберігання на рівнях Bronze, Silver та Gold. Це забезпечує гнучку аналітику та візуалізацію даних з урахуванням ролей користувачів, підвищуючи довіру та відповідність вимогам SOC 2 Type 2.*

Ключові слова: *SOC 2 Type 2, Microsoft Fabric, Azure Open AI, Medalion Architecture, LLM, Security, Data Classification.*

Вступ. Зростання обсягів даних ставить перед організаціями нові виклики щодо їхнього ефективного зберігання та обробки. Сучасні потреби в управлінні великими масивами інформації вимагають рішень, які забезпечують її безпеку, доступність та ефективність використання. У цьому контексті пілотний проект з впровадження методики зберігання даних на базі хмарного сервісу Microsoft Azure представляє собою інноваційний підхід. Це рішення не лише відповідає вимогам щодо надійності та гнучкості, але й пропонує інтеграцію з іншими сервісами Microsoft, що сприяє оптимізації бізнес-процесів та підвищенню загальної ефективності організації.

Основні частина. Microsoft Azure є однією з провідних хмарних платформ, що надає широкий спектр можливостей для ефективного зберігання та обробки даних. Її сервіси охоплюють всі аспекти, необхідні для сучасних організацій: від базового зберігання до складних аналітичних процесів, машинного навчання та штучного інтелекту. Завдяки підтримці різних форматів, таких як Infrastructure as a Service (IaaS), Platform as a Service (PaaS) та Software as a Service (SaaS), Azure дозволяє організаціям швидко адаптуватися до змін ринку, знижуючи витрати на інфраструктуру та забезпечуючи високий рівень безпеки даних.

Azure пропонує гнучкі рішення для різних галузей, від фінансових установ до медичних компаній, дозволяючи їм інтегрувати хмарні технології у свої щоденні операції. Це забезпечує безперебійну роботу, знижує ризик втрати даних і підвищує продуктивність. Крім того, Azure надає мо-

жливість використовувати потужні інструменти для аналітики даних, які допомагають організаціям отримувати цінні інсайти з великих обсягів інформації. Це особливо актуально в умовах, коли швидкість прийняття рішень може бути вирішальною для успіху в конкурентному середовищі.

У рамках пілотного проекту було обрано архітектуру Medallion, яка структурно організує обробку даних у три послідовні шари: Bronze, Silver та Gold. Кожен з цих рівнів виконує свою роль у процесі трансформації даних, починаючи від зберігання сирих даних і закінчуючи їхньою підготовкою для бізнес-аналітики. Bronze Layer забезпечує збереження початкових даних без змін, що є важливим для аудиту та відновлення оригінальної інформації. Silver Layer виконує очищення, нормалізацію та обробку даних, усуваючи дублікати та формуючи структурований формат, готовий для аналітичних запитів. Gold Layer, в свою чергу, трансформує дані відповідно до специфічних бізнес-вимог, забезпечуючи їхню готовність для використання аналітиками та ключовими замовниками.

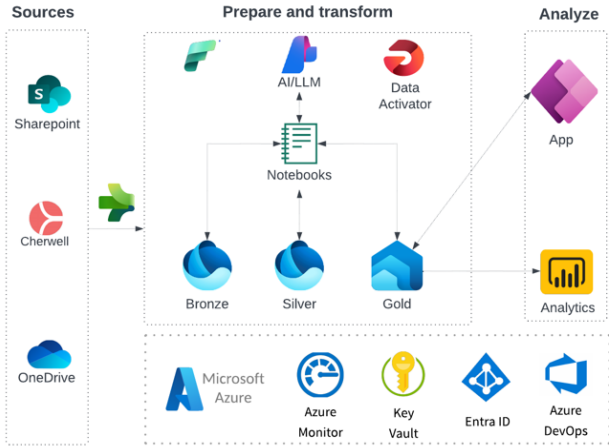

Рисунок 1 – Прототип розгортання

Опис продуктів згідно прототипу.

Для реалізації пілотного проекту обрано продукти MS Fabric та Azure Open AI, які забезпечують інтеграцію та обробку даних на різних рівнях. OneLake, як єдине озеро даних у Fabric, використовується для зберігання неструктурованих даних з джерел SharePoint та OneDrive. Data Warehouse у Fabric організовує дані на рівнях Silver та Gold, де вони вже структуровані і готові для швидких запитів та аналітичних процесів. Azure

Data Factory (ADF) відповідає за оркестрацію процесів витягнення та обробки даних для всіх трьох рівнів, інтегруючи корпоративні дані через Microsoft Graph API.

Azure OpenAI надає доступ до передових моделей штучного інтелекту для обробки природної мови, генерації тексту та аналітики. Це забезпечує високий рівень безпеки та конфіденційності даних, включаючи механізми фільтрації шкідливого контенту та моніторинг зловживань. Для ідентифікації сенситивних даних відповідно до політик безпеки, ми програмно аналізуємо неструктуровані джерела за допомогою Azure OpenAI, виявляючи такі дані та зберігаючи їх на рівні Silver Layer.

Power BI та корпоративні додатки дозволяють візуалізувати дані з Gold Layer у вигляді зручних звітів та дашбордів, забезпечуючи доступ користувачам із урахуванням їхніх ролей та прав. Це дає змогу перевіряти достовірність, цілісність та коректність класифікації даних, а також виконувати їх шифрування відповідно до корпоративних політик конфіденційності. Data Activator, як сервіс у Microsoft Fabric, відстежує ключові події та зміни в даних у реальному часі, запускає автоматизовані тригери й надсилає адаптовані нотифікації, що забезпечує оперативне виконання політик безпеки.

Висновки. Пілотний проект на базі Microsoft Azure демонструє значний потенціал для оптимізації бізнес-процесів завдяки надійності та гнучкості хмарної платформи. Архітектура Medallion забезпечує ефективне управління якістю даних, попри деякі недоліки, такі як ускладнення потоків даних. Інтеграція з Azure OpenAI та іншими продуктами Microsoft дозволяє використовувати передові технології для аналізу та обробки даних, що підвищує безпеку та конфіденційність. Використання Power BI для візуалізації даних сприяє прийняттю обґрунтованих рішень, а Data Activator забезпечує оперативне реагування на зміни в даних. Загалом, проект демонструє, як хмарні технології можуть допомогти організаціям ефективно управляти даними та реагувати на зміни ринку.

Література

1. Hosne Ara Mohna,Tonmoy Barua,Mohammad Mohiuddin,Md Mostafizur Rahman "AI-READY DATA ENGINEERING PIPELINES: A REVIEW OF MEDALLION ARCHITECTURE AND CLOUD-BASED INTEGRATION MODELS" DOI: https://doi.org/10.63125/51kxtf08

2. https://learn.microsoft.com/en-us/fabric/fundamentals/

3. https://learn.microsoft.com/en-us/azure/ai-foundry/

4. Piethein Strengholt “Building Medallion Architectures,” year 2025, pages: 394, ISBN: 9781098178833

УДК 004.056.5

КОМПЛЕКСНИЙ АНАЛІЗ ЕФЕКТИВНОСТІ ХМАРНИХ ПЛАТФОРМ ДЛЯ АВТОМАТИЗОВАНОГО ВИЯВЛЕННЯ ТА НЕЙТРАЛІЗАЦІЇ ШКІДЛИВИХ ФАЙЛІВ

Андрій ДЕНЕГА, Валентина ЯЩУК, Андрій ІВАНУСА
Львівський державний університет безпеки життєдіяльності

Анотація. *Досліджено сучасні підходи до аналізу хмарного програмного забезпечення з метою виявлення шкідливих файлів. Розвиток хмарних сервісів та SaaS-рішень значно збільшив обсяг оброблюваних даних, що підвищує ризики компрометації корпоративної інформації. Особливу увагу приділено методам статичного та динамічного аналізу, поведінковій аналітиці та машинному навчанню для класифікації шкідливих об'єктів. Запропоновано інтегративну модель оцінки ризику, яка поєднує технічні, поведінкові та контекстні параметри, що забезпечує підвищену точність та швидкість виявлення загроз у хмарних середовищах.*

Ключові слова: *хмарне програмне забезпечення, шкідливі файли, машинне навчання, аналіз поведінки, кіберзахист.*

Abstract. *Modern approaches to analyzing cloud software for the purpose of detecting malicious files are investigated. The development of cloud services and SaaS solutions has significantly increased the amount of processed data, which increases the risks of compromising corporate information. Particular attention is paid to static and dynamic analysis methods, behavioral analytics, and machine learning for classifying malicious objects. An integrative risk assessment model is proposed that combines technical, behavioral, and contextual parameters, which provides increased accuracy and speed of threat detection in cloud environments.*

Keywords: *cloud software, malicious files, machine learning, behavioral analysis, cyber security.*

Хмарні платформи забезпечують високу масштабованість, гнучкість та доступність, але водночас стають привабливою мішенню для кібератак, включно зі шкідливими файлами, що маскуються під легітимний контент. Основними векторами загроз у хмарних сервісах є виконувані файли (.exe), скрипти (.bat, .ps1), макроси VBA (.docm, .xlsm), PDF-файли з вбудованим JavaScript, архіви з паролем та виконувані об'єкти у контейнерах OLE. Сучасні шкідливі файли часто використовують обфускацію, енкрипцію payload та техніку Living-Off-the-Land (LOLbins) для обходу антивірусних сканерів і sandbox-середовищ.

Сьогодні виділено три ключові напрями виявлення шкідливих файлів у хмарному середовищі. Перший напрям – статичний аналіз, який передбачає перевірку хешів, сигнатур файлів, метаданих та інтеграцію з базами Threat Intelligence. Прикладом такого підходу є виявлення шкідливого

макросу з командою CreateObject("WScript.Shell") та викликом URLDownloadToFile для завантаження payload. Для PDF-файлів застосовується аналіз вбудованого JavaScript та перевірка на відомі уразливості за стандартом CVE. Другий напрям – динамічний аналіз, який здійснюється у sandbox або емуляторі хмарного середовища; під час запуску файлу відстежується його поведінка, включно зі створенням процесів, мережею активністю, маніпуляціями з файловою системою та доступом до критичних ресурсів. Наприклад, це може бути запуск PowerShell-скрипта для завантаження шкідливих DLL-файлів у пам'ять без запису на диск (in-memory attack). Третій напрям – поведенкова аналітика та машинне навчання, що дозволяє класифікувати об'єкти на основі аномальної активності, включаючи нестандартні виклики API, підозрілі комбінації параметрів у скриптах, повторювані мережеві запити та незвичні ланцюжки процесів. Використання алгоритмів класифікації, таких як Random Forest та XGBoost, а також нейронних мереж, дозволяє автоматично виявляти обфусковані та zero-day загрози.

Щодо архітектури обробки файлів у хмарному середовищі, пропонується багаторівнева схема (рис.1).

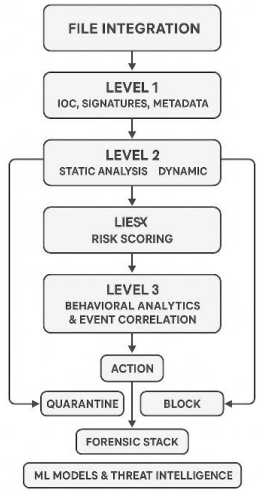

Рисунок 1 – Блок-схема архітектури багаторівневої обробки файлів у хмарному середовищі

На першому рівні здійснюється прийом і первинна перевірка файлу на сигнатури та відомі індикатори компрометації (IOC). Другий рівень забезпечує статичний та динамічний аналіз із застосуванням sandbox і емуляторів операційних систем, де відстежується поведінка файлів та виявля-

ються потенційні атаки in-memory. На третьому рівні інтегруються поведінкові алгоритми та моделі машинного навчання для оцінки аномалій та кореляційного аналізу подій у SIEM. Заключний етап включає автоматичне блокування або поміщення в карантин файлів з високим ризиком, а також збереження логів для подальшого розслідування. Така архітектура дозволяє реалізувати превентивний підхід, знижуючи ймовірність пропуску шкідливих об'єктів у корпоративну хмарну інфраструктуру.

Блок-схема архітектури багаторівневої обробки файлів у хмарному середовищі ілюструє процес проходження інгрестованих файлів первинної перевірки (Level 1 — IOC, сигнатури, метадані), далі розподіляються на статичний і/або динамічний аналіз (Level 2), на основі отриманих індикаторів формується ризик-скор і передається на рівень поведінкової аналітики та кореляції подій (Level 3). За результатами приймається автоматизоване рішення (карантин/блок/сповіщення), а артефакти й логи направляються у форензик-стік та для підживлення ML-моделей і Threat Intelligence.

Отже, для ефективного виявлення шкідливих файлів у хмарних сервісах необхідне комплексне поєднання статичного, динамічного та поведінкового аналізу з використанням алгоритмів машинного навчання. Запропонована багаторівнева архітектура обробки файлів забезпечує точність, швидкість реагування та адаптивність до нових типів загроз, включно із zero-day атаками. Подальші дослідження можуть зосередитися на інтеграції Zero Trust принципів для контролю доступу, оптимізації алгоритмів машинного навчання для реального часу та масштабуванні систем раннього попередження у великих корпоративних хмарних середовищах.

Література

1. Ящук В.І., Івануса А.І., Маслова Н.О., Ткачук Р.Л., Брич Т.Б. Концептуалізація інтегративного використання баз даних вразливостей у контексті системного менеджменту інформаційної безпеки // Вісник Львівського державного університету безпеки життєдіяльності. – 2025. – Т. 31. – С. 59–61

2. Ящук В.І. Simulation Of Investment It Project Management Tasks / В.І. Ящук // Інновінг сучасних трендів в менеджменті безпеки: національна безпека та оборона»: збірник тез доповідей Всеукраїнської науково-практичної конференції м. Львів, 23 травня 2025 року. Львів: ЛДУ БЖД, 2025. 460 с. (С.247-253).

3. Valentina Yashchuk, Andriy Ivanusa, Nataliya Maslova, Rostyslav Tkachuk, Taras Brych INTEGRATION OF VULNERABILITY DATABASES INTO ISMS – A PATH TO ENHANCING CYBER RESILIENCE OF CRITICAL SYSTEMS // Resilient Systems: Secure Digital Technologies and Critical Infrastructure: Proceedings of 1st International Scientific and Practical Conference. Drohobych: Donetsk National Technical University, 2025. 184 p.60-66.

УДК 004.056

ВИКОРИСТАННЯ БЛОКЧЕЙН-ТЕХНОЛОГІЙ ДЛЯ ПІДВИЩЕННЯ ДОВІРИ В АУДИТІ ТА АКРЕДИТАЦІЇ ІНФОРМАЦІЙНИХ СИСТЕМ

Назарій ДМИТРІВ[1], Валерія БАЛАЦЬКА[2]

1. Приватний вищий навчальний заклад «Європейський університет»,м. Київ

2. Львівський державний університет безпеки життєдіяльності

Досліджено можливості використання блокчейн-технологій у процесах аудиту, ліцензування та акредитації ін-формаційних систем. Запропоновано концепцію цифрового аудиту з використанням permissioned blockchain для забез-печення прозорості, незмінності та відтворюваності результатів перевірки. Розглянуто підходи до підвищення довіри між акредитуючими органами, розробниками та користувачами систем.

Ключові слова: *блокчейн, аудит, акредитація, КСЗІ, довіра, ліцензування, цифровий контроль, ризик-менеджмент..*

The potential of blockchain technologies in auditing, licensing, and accreditation of information systems is explored. A concept of digital audit using a permissioned blockchain is proposed to ensure transparency, immutability, and traceability of verification results. The approach enhances trust among accreditation authorities, system developers, and end users.

Keywords: *blockchain, audit, accreditation, ISPS, trust, licensing, digital control, risk management*

Розвиток цифрового врядування, розширення електронних сервісів та інтеграція державних реєстрів вимагають підвищення рівня довіри до процесів аудиту, ліцензування та акредитації інформаційних систем. У традиційній моделі перевірки ефективність і достовірність результатів залежать від суб'єктивних чинників – компетентності експертів, якості підготовленої документації, людського контролю та адміністративного впливу [1]. Такий підхід формує ризики фальсифікації результатів, вибіркового ставлення, конфлікту інтересів і неузгодженості між акредитуючими органами, що особливо небезпечно для державних систем, які обробляють критичні дані.

Блокчейн-технології відкривають можливість усунення цих проблем шляхом створення незмінного децентралізованого реєстру аудиторських дій, у якому кожен запис фіксується як транзакція з часовою міткою та криптографічним підписом [2]. У такій моделі жоден учасник не має можливості самостійно змінювати чи видаляти дані перевірки, що забезпечує прозорість і відтворюваність кожного етапу контролю. Такий підхід підвищує рівень цифрової довіри, дозволяє автоматично перевіряти достовірність звітів і запобігає маніпуляціям під час акредитації.

Запропонована модель системи блокчейн-аудиту побудована на основі permissioned blockchain, де кожен вузол належить визначеному суб'єкту процесу: акредитуючому органу, розробнику, власнику інформаційної системи, незалежному аудитору та державному регулятору. Усі вузли взаємодіють у режимі контрольованого консенсусу, який гарантує узгоджене збереження результатів. Кожен етап перевірки – від тестування ефе-

ктивності КСЗІ до оцінки політик безпеки – фіксується у блокчейні, формуючи ланцюг довіри (chain of trust) [3].

Для підвищення об'єктивності пропонується використати математичну модель інтегрального індексу довіри (Trust Index), що враховує результати попередніх аудитів і вагомість виявлених невідповідностей:

$$T_{sys} = \alpha A_{rep} + \beta A_{comp} + \gamma A_{risk},$$

де A_{rep} – рівень репутаційної надійності аудитора, A_{comp} – середня оцінка відповідності стандартам, A_{risk} – показник ризиковості системи; α, β, γ – вагові коефіцієнти *(α+β+γ=1)*.

Якщо $T_{sys} \geq 0,8$, система визнається такою, що заслуговує довіри й може бути акредитована; при $0,6 \leq T_{sys} < 0,8$ – потрібні додаткові перевірки; нижче *0,6* – акредитація неможлива. Така формалізація мінімізує вплив людського чинника та перетворює процес аудиту на цифрово підтверджувану процедуру, що відповідає принципам ISO/IEC 17065:2022 і вимогам GDPR щодо контролю обробки персональних даних [4].

Важливою складовою моделі є створення єдиного децентралізованого реєстру сертифікованих інформаційних систем, який містить структуровані метадані про статус акредитації, дати перевірок, типи впроваджених КСЗІ, чинні сертифікати відповідності, результати аудитів і рівень довіри до системи. Такий реєстр може бути реалізований у форматі permissioned blockchain, де запис здійснюють лише уповноважені органи, а перегляд окремих параметрів можливий для громадськості через відкритий вебінтерфейс. Це забезпечує поєднання прозорості та конфіденційності: відкритими залишаються лише контрольні хеші, дати й статуси акредитації, тоді як внутрішні звіти зберігаються у зашифрованому вигляді.

Використання такого механізму підвищує рівень довіри громадськості до органів контролю у сфері інформаційної безпеки, створює умови для взаємної перевірки між суб'єктами й спрощує процес верифікації сертифікатів. Сторонні аудитори або постачальники послуг можуть підтверджувати дійсність сертифікатів без запитів до центральних баз, що підвищує ефективність контролю в реальному часі.

Інтеграція смарт-контрактів аудиту дає змогу автоматично перевіряти відповідність КСЗІ мінімальним вимогам [5]. Алгоритми контрактів верифікують наявність криптографічних модулів, резервного копіювання, політик доступу, журналювання інцидентів тощо. У разі виявлення невідповідностей смарт-контракт формує цифровий звіт, який додається до блокчейну та може ініціювати повторну оцінку системи. Це частково автоматизує аудит, зменшує вплив людського чинника та скорочує тривалість акредитації з кількох тижнів до кількох днів.

Імітаційне моделювання у середовищі Hyperledger Fabric підтвердило практичну ефективність підходу. Система містила три типи вузлів: регулятор, аудитор і розробник. За результатами експериментів середній час обробки заявки скоротився на 32 %, а кількість логічних помилок у звітно-

сті – на 19 %. Крім того, жоден запис не міг бути змінений без підтвердження більшістю вузлів мережі, що доводить стійкість рішення до внутрішніх маніпуляцій.

Крім технічних переваг, важливими є організаційно-правові аспекти. Чинні нормативні акти (Постанова КМУ № 373, Закон України «Про захист інформації в ІТС») не враховують децентралізованих моделей аудиту. Проте блокчейн може функціонувати як доповнення до чинних процедур експертизи КСЗІ, забезпечуючи цифрову фіксацію дій експертів, незалежну верифікацію рішень і можливість перевірки достовірності сертифікатів у будь-який момент часу.

У перспективі це створить підґрунтя для національного електронного реєстру акредитованих систем, інтегрованого з державними платформами «Дія» та ДССЗЗІ. Такий підхід забезпечить централізоване, але децентралізовано верифіковане зберігання даних, автоматичний моніторинг чинності сертифікатів і контроль термінів їх поновлення.

Впровадження блокчейн-технологій у процеси аудиту, ліцензування та акредитації формує нову модель цифрової довіри, у якій кожна дія має криптографічне підтвердження, а історія змін зберігається у розподіленому середовищі. Це підвищує стійкість до кіберзагроз, достовірність даних і створює основу для реалізації національної стратегії кіберстійкості та гармонізації українських підходів із міжнародними стандартами ISO/IEC 27001, 27701 і 17065.

Література

1. Балацька В. С., Дмитрів Н. Міжорганізаційний обмін конфіденційними персональними даними на основі дозвільного блокчейн // Кібербезпека: освіта, наука, техніка. – 2025. – № 2(29). – С. 178–193. DOI: https://doi.org/10.28925/2663-4023.2025.29.875.

2. Балацька В. С., Опірський І. Р. Забезпечення конфіденційності персональних даних і підтримки кібербезпеки за допомогою блокчейну // Кібербезпека: освіта, наука, техніка. – 2023. – № 4(20). – С. 6–19. DOI: https://doi.org/10.28925/2663-4023.2023.20.619.

3. Опірський І., Побережник В., Балацька В. Method for Ensuring Data Integrity and Authenticity Based on Blockchain Technology Integration // CEUR Workshop Proceedings: DECaT'2025 – Digital Economy Concepts and Technologies. – Kyiv, 2025. – P. 70–80. URL: https://ceur-ws.org/Vol-4029/.

4. Wang Y., Singh S., Al-Bahadili H. Blockchain-Based Audit Framework for Ensuring Integrity and Trust in Digital Certification Systems // IEEE Access. – 2024. – Vol. 12. – P. 48756–48771. DOI: https://doi.org/10.1109/ACCESS.2024.3456712.

5. Балацька В. С., Побережник В. О., Стефанків А. В., Шевчук Ю. А. Розробка методу забезпечення достовірності та безпеки персональних даних у блокчейн-системах державних реєстрів // Комп'ютерні системи та мережі. – 2025. – Т. 7, № 1. – С. 1–16. DOI: https://doi.org/10.23939/csn2025.01.001.

УДК 004.056

СУЧАСНІ ЗАГРОЗИ В МЕРЕЖАХ І ЗАХИСТ КОРИСТУВАЧА ЗІ ШІ

Романія ЖИДАК
Львівський державний університет безпеки життєдіяльності

Анотація. *Розглянуто основні загрози комп'ютерних мереж та методи захисту користувача. Наведено приклади атак: MITM, фішинг, typosquatting та ШІ-атаки (Prompt Injection, Data Poisoning, соціальний інжиніринг). Представлено засоби захисту: firewall, VPN, шифрування та ШІ для аналізу трафіку.*
Ключові слова: *кібербезпека, мережеві атаки, захист користувача, MITM, фішинг, ШІ, VPN, шифрування.*

Abstract. *The paper examines major threats in computer networks and user protection methods. Examples include MITM, phishing, typosquatting, and AI-based attacks (Prompt Injection, Data Poisoning, social engineering). Protection methods include firewall, VPN, encryption, and AI traffic analysis.*
Keywords: *cybersecurity, network attacks, user protection, MITM, phishing, AI, VPN, encryption.*

Сучасні мережі піддаються численним загрозам, що можуть порушувати конфіденційність, цілісність і доступність даних. Використання firewall, VPN, шифрування та автоматизованого аналізу трафіку за допомогою ШІ дозволяє ефективно знижувати ризики атак.

1. Приклади атак у мережі

1.1 MITM (Man-in-the-Middle)

Атака полягає у перехопленні трафіку між користувачем і сервером, особливо у відкритих Wi-Fi мережах. Зловмисник може отримати доступ до логінів, паролів та інших конфіденційних даних. Використання HTTPS та VPN значно зменшує ризик таких атак, забезпечуючи шифрування переданої інформації та захищені канали зв'язку.

1.2 Фішинг та Typosquatting

Фішингові атаки та typosquatting використовують підроблені сайти або листи, що маскуються під відомі сервіси, для отримання конфіденційних даних користувачів. Захист включає уважну перевірку URL, використання менеджерів паролів, двофакторну автентифікацію та обережне ставлення до електронної пошти від невідомих відправників.

1.3 Використання ШІ у мережевих атаках (Prompt Injection, Data Poisoning та соціальний інжиніринг)

Штучний інтелект може бути використаний як знаряддя атак: Prompt Injection і Data Poisoning дозволяють «отруїти» моделі та змусити їх виконати команди зловмисника. Також ШІ застосовується для створення

переконливих фішингових повідомлень у соціальному інжинірингу. Методи захисту включають фільтрацію вхідних даних, перевірку джерел повідомлень і підвищення обізнаності користувачів.

2. Методи захисту інформації

2.1 Firewall

Контролює мережеві з'єднання, дозволяючи лише необхідний трафік та блокуючи підозрілі або небажані запити. Він може працювати як за заданими правилами користувача, так і автоматично визначати потенційно небезпечні порти та підключення.

2.2 Штучний інтелект у мережевій безпеці користувача

ШІ аналізує мережевий трафік, визначає типи протоколів, виявляє аномалії та потенційно небезпечні підключення, оцінює ризики і надає рекомендації користувачу. Це скорочує час аналізу, підвищує ефективність виявлення потенційно небезпечної поведінки та допомагає захищати дані у сучасних зашифрованих мережах.

2.3 VPN і шифрування

VPN забезпечує безпечний тунель для передавання даних у відкритих мережах. Шифрування гарантує конфіденційність інформації навіть при перехопленні трафіку. Використання VPN і шифрування разом дозволяє зменшити ризик атак та забезпечити безпеку користувачів у будь-яких умовах.

Висновки

Сучасні атаки використовують різні вектори — MITM, фішинг та ШІ-атаки. Комбіновані заходи захисту (firewall, VPN, шифрування, ШІ) дозволяють своєчасно виявляти аномалії та потенційні ризики, підвищуючи безпеку користувачів. Освіченість користувачів і контроль доступу залишаються критично важливими для мінімізації ризиків.

Література

1. Pfleeger, C.P., Pfleeger, S.L. Security in Computing. Prentice Hall, 2015.

2. Scarfone, K., Mell, P. Guide to Intrusion Detection and Prevention Systems (IDPS). NIST, 2007.

3. Phishing.org. Examples and Education. https://www.phishing.org

4. OWASP Foundation. OWASP Top Ten Web Application Security Risks, 2021.

5. Stallings, W. Cryptography and Network Security. Pearson, 2020.

6. Goodfellow, I., Bengio, Y., Courville, A. Deep Learning. MIT Press, 2016.

7. Wireshark Foundation. Wireshark User Guide, 2024.

8. Cloudflare. QUIC and HTTP/3 Protocol Overview, 2023.

УДК 621.391.8:355.4:004.056

МЕТОДИ ЗАХИСТУ СУПУТНИКОВИХ КОМУНІКАЦІЙ STARLINK/VSAT У ЗОНАХ БОЙОВИХ ДІЙ

Вікторія ЖУРАВЕЛЬ, Василь ЛУЧИК
Харківський національний університет внутрішніх справ

Анотація. *У цьому дослідженні розглядаються ключові методи забезпечення кіберзахисту супутникових систем зв'язку. Аналізуються потенційні загрози, методи перехоплення та можливості застосування завад і РЕБ.*
Ключові слова: *супутниковий зв'язок, Starlink, VSAT, РЕБ, кіберзахист.*

Abstract. *This study analyzes the main methods of cybersecurity protection for modern satellite communication systems. It examines threats, interception techniques, and countermeasures including jamming and electronic warfare.*
Keywords: *satellite communication, cybersecurity, jamming.*

Супутниковий зв'язок Starlink та VSAT відіграє критичну роль у забезпеченні стійкої комунікації військових підрозділів у зоні бойових дій. В умовах війни, де наземна інфраструктура знищена або недоступна, саме супутникові системи забезпечують безперервність командування, передачу розвідданих, роботу БПЛА, навігацію та координацію підрозділів. Разом із тим, висока залежність від супутникових каналів робить їх привабливою ціллю для противника, який застосовує радіоелектронну боротьбу, кібератаки та інформаційні впливи з метою порушення роботи систем. Це створює потребу в удосконаленні методів захисту на технічному та організаційному рівнях.

Мета та завдання дослідження.

Мета: Проаналізувати сучасні методи захисту супутникових каналів зв'язку Starlink і VSAT у бойових умовах та визначити їх ефективність.

Завдання:

Описати основні загрози супутниковим комунікаціям у зоні бойових дій.

Розглянути технічні методи захисту каналів передачі даних.

Проаналізувати підходи до захисту термінального обладнання та мережевої інфраструктури.

Надати рекомендації щодо підвищення кіберстійкості Starlink/VSAT у військових операціях.

Основні загрози для супутникових систем у бойових умовах

Супутниковий зв'язок піддається широкому спектру загроз, серед яких:

- радіоелектронне придушення (jamming);

- спуфінг сигналів навігації чи телеметрії;
- спроби перехоплення або аналізу трафіку;
- кібератаки на термінали, маршрутизатори, Wi-Fi-модулі;
- мережеві атаки на інфраструктуру супутникового оператора;
- фізичне знищення терміналів або антенних систем.

У бойових умовах особливо небезпечними є РЕБ-атаки, що спрямовані на придушення Starlink у робочому діапазоні 10–12 ГГц, а також спроби отримати доступ до локальної мережі підрозділу через вразливості терміналу.

Методи технічного захисту супутникових каналі

Криптографічний захист і шифрування трафіку

Сучасні системи Starlink та VSAT використовують TLS і AES-базовані протоколи шифрування, що унеможливлюють перехоплення даних у відкритому вигляді. Використання протоколів end-to-end encryption дозволяє запобігати атакам «чоловік посередині», навіть за умови часткового компрометування каналу.

Адаптивні антенні системи та спрямовані промені

Фазовані антени Starlink здатні динамічно змінювати напрямок променя, знижуючи вплив перешкод та ускладнюючи спуфінг. Адаптивне формування променя підвищує завадостійкість, що особливо важливо при роботі у зоні дії РЕБ.

Частотне маневрування

Використання частотного хопінгу (FHSS) і адаптивного вибору частоти дозволяє уникати зон придушення. Це мінімізує вплив спрямованих завад на конкретні діапазони.

Захист термінального обладнання

Сюди входить:

- регулярне оновлення прошивок;
- апаратна автентифікація обладнання;
- відключення непотрібних інтерфейсів (Wi-Fi, BLE);
- використання мережевих екранів і VPN для ізоляції військової мережі.

Методи кіберзахисту та мережевої безпеки

Сегментація мережі

Термінал Starlink/VSAT має бути ізольований у окремому VLAN або підмережі, що запобігає розповсюдженню атак на внутрішні системи підрозділу.

Використання багаторівневих фільтрів та IDS/IPS

Системи виявлення вторгнень необхідні для блокування шкідливих пакетів, спроб сканування портів та ін’єкційних атак.

Контроль доступу

Захист включає автентифікацію користувачів, багаторівневі паролі, прив'язку до MAC-адрес, вимкнення гостьових точок доступу.

Операційні заходи безпеки:

- маскування розташування терміналів;
- мінімізація часу роботи антени у фіксованій позиції;
- використання камуфляжу для зменшення теплової та радіолокаційної видимості.

Практичні рекомендації для підвищення стійкості Starlink/VSAT:

Використовувати додаткові апаратні фільтри та екранування для зменшення ефективності РЕБ.

Встановлювати VPN поверх основного шифрування, що додає ще один рівень захисту.

Регулярно оновлювати ПЗ та прошивки терміналів і маршрутизаторів.

Проводити тестування на проникнення для виявлення локальних вразливостей.

Застосовувати тактичні процедури, включно зі зміною місцезнаходження терміналів і режимів роботи.

Резервувати канали, використовуючи Starlink, VSAT і радіорелейні системи одночасно.

Висновки

Захист супутникових комунікацій Starlink/VSAT у зонах бойових дій потребує поєднання криптографічних, апаратних, мережевих і тактичних рішень. Ефективність захисту визначається здатністю системи адаптуватися до радіоелектронного придушення та кібератак, а також організаційною дисципліною при розгортанні та експлуатації обладнання. Комплексний підхід забезпечує стійкість зв'язку, що є критично важливою умовою успішного ведення бойових операцій.

Література

1. Державна служба спеціального зв'язку та захисту інформації України (ДССЗЗІ). Аналітичні огляди щодо стану кібербезпеки та радіочастотного середовища. Режим доступу: https://cip.gov.ua

2. Міністерство цифрової трансформації України. Публікації про використання супутникового зв'язку Starlink в Україні під час війни. Режим доступу: https://thedigital.gov.ua

3. Національна безпекова стратегія України (2020). Розділи щодо захисту критичної інфраструктури та зв'язку.

УДК 004.056.55:004.8:004.934.2

DEEPFAKE-ФІШИНГ: НОВИЙ РІВЕНЬ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ ТА МОДЕЛІ ВИЯВЛЕННЯ

Вікторія ЖУРАВЕЛЬ, Василь ЛУЧИК
Харківський національний університет внутрішніх справ

Анотація. *У статті аналізується загроза deepfake-фішингу як нової форми соціальної інженерії. Розглянуто технології створення глибоких підробок, їх вплив на жертв та сучасні методи виявлення. Запропоновано комплексний підхід до протидії, що поєднує технології, політики безпеки й підвищення обізнаності.*
Ключові слова: *deepfake-фішинг, соціальна інженерія, глибокі підробки, штучний інтелект, біометрична безпека, виявлення маніпуляцій, кібербезпека.*

Abstract. *The article examines deepfake phishing as an advanced form of social engineering. It analyzes deepfake generation technologies, their psychological impact, and modern detection methods. A comprehensive countermeasure approach is proposed, integrating technological solutions, security policies, and user awareness to mitigate deepfake-driven cyber threats.*
Keywords: *deepfake phishing, social engineering, deepfakes, artificial intelligence, biometric security, manipulation detection, cybersecurity.*

Стрімкий розвиток технологій штучного інтелекту (ШІ), зокрема генеративних змагальних мереж (GANs), призвів до появи складних методів маніпуляції аудіовізуальним контентом, відомих як "deepfakes". Ці технології, спочатку створені для розваг та мистецтва, все частіше використовуються зловмисниками в кібератаках. Deepfake-фішинг є еволюційним стрибком у соціальній інженерії, оскільки долає основну вразливість традиційного фішингу – відсутність довіри. Відео- або аудіозапис, де керівник або колега віддає переконливу команду, має набагато вищу довіру, ніж текстовий email.

Актуальність дослідження зумовлена зростаючою доступністю інструментів для створення deepfakes, їхньою технологічною досконалістю та потенційною шкодою для бізнесу та суспільства. Протидія цій загрозі вимагає нового, комплексного підходу, що поєднує передові технології виявлення з глибоким розумінням кіберпсихології.

Мета дослідження: проаналізувати загрозу deepfake-фішингу, дослідити механізми його впливу на жертв та оцінити ефективність сучасних моделей його виявлення для розробки комплексних заходів протидії.

Завдання дослідження:

Дослідити технологічні основи створення deepfakes та їх застосування в фішингових атаках.

Проаналізувати психологічні аспекти впливу deepfake-фішингу на прийняття рішень жертвою.

Систематизувати та оцінити сучасні моделі та методи виявлення deepfake-контенту.

Розробити рекомендації щодо формування комплексної системи захисту від deepfake-фішингу для організацій.

Результати дослідження та їх обговорення

Технологічні основи та сценарії атак deepfake-фішингу

Deepfake-фішинг базується на використанні AI-згенерованого відео, аудіо або зображень для імітації реальної людини з метою виманювання грошей, конфіденційної інформації або отримання несанкціонованого доступу.

Сценарії атак:

Відео-фішинг: Зловмисник створює відеозвернення "CEO", який наказує фінансовому відділу терміново переказати кошти на рахунок під контролем зловмисників.

Аудіо-фішинг (голосовий фішинг): Імітація голосу керівника по телефону або через месенджери з проханням надати доступ до системи або відправити конфіденційні файли.

Комбіновані атаки: Використання deepfake-відео в поєднанні з скомпрометованими корпоративними email-акаунтами для підвищення правдоподібності.

Кіберпсихологічні аспекти ефективності deepfake-фішингу

Ефективність цих атак ґрунтується на ключових психологічних принципах:

Довіра до аудіовізуального контенту: Людський мозок схильний більше довіряти інформації, отриманій через кілька каналів сприйняття (відео + аудіо). Deepfake експлуатує цю довіру.

Соціальний інжиніринг, заснований на упізнаванні: Ми швидше виконуємо накази людини, яку впізнаємо (обличчя, голос).

Ефект терміновості: Атаки часто сконструйовані так, щоб викликати стресову ситуацію ("це терміново!", "це конфіденційно!"), що відключає критичне мислення жертви.

Моделі та методи виявлення deepfakes

Боротьба з deepfakes ведеться в технологічній площині за допомогою різних моделей:

Методи, засновані на аналізі артефактів: Штучний інтелект шукає недоліки в згенерованому контенті: нереалістичне блимання, артефакти навколо обличчя, невідповідність освітлення, неестественні руху губ.

Аналіз біометричної неспроможності: Перевірка фізіологічної послідовності (наприклад, співвіднесення пульсу зі змінами кольору шкіри).

Форезійні методи: Аналіз цифрових "відбитків" файлів, пошук слідів стиснення та маніпуляцій.

Використання блокчейну: Створення цифрових сертифікатів для автентифікації оригінального відео та відстеження його модифікацій.

Бачення завдань: Клавдіатурні, поведінкові біометричні системи, які аналізують унікальну манеру користувача працювати з пристроями.

Обговорення обмежень та комплексного підходу

Жодна модель виявлення не є панацеєю. Зловмисники постійно вдосконалюють технології, а системи виявлення завжди відстають. Тому необхідний комплексний захист:

Технологічний рівень: Впровадження AI-інструментів виявлення deepfakes в корпоративні системи безпеки, використання багатофакторної аутентифікації (MFA) для критичних операцій.

Процедурний рівень: Впровадження чітких процедур підтвердження фінансових та інших конфіденційних операцій (наприклад, обов'язковий дзвінок за допомогою перевіреного номеру телефону).

Людський рівень: Регулярне навчання співробітників, проведення тренувань з симуляцією deepfake-атак, підвищення обізнаності про цю загроз

Висновки

Deepfake-фішинг становить серйозну загрозу кібербезпеці, значно підвищуючи ефективність соціальної інженерії за рахунок експлуатації базової довіри людини до аудіовізуальної інформації.

Ефективна протидія неможлива без розуміння кіберпсихологічних механізмів, що лежать в основі успіху цих атак, таких як ефект упізнавання та маніпуляція через створення терміновості.

Сучасні моделі виявлення deepfakes, засновані на ШІ, є потужним інструментом, але не абсолютним захистом через постійне протиборство технологій атаки та захисту.

Стійкість організації до deepfake-фішингу може бути забезпечена лише за допомогою комплексного підходу, що інтегрує технологічні рішення, перевірені процедури безпеки та постійне навчання співробітників, спрямоване на вироблення "кібергігієнічної" культури.

Література

1. Кіберполіція України. (2023). Попередження про deepfake-атаки на українські компанії. Офіційний сайт Національної поліції України. [Електронний ресурс]. Режим доступу: https://www.npu.gov.ua/

2. Державна служба спеціального зв'язку та захисту інформації України. (2024). Рекомендації щодо захисту від атак з використанням технологій штучного інтелекту. [Електронний ресурс]. Режим доступу: https://cip.gov.ua/

3. Український кібербезпековий портал «Кіберзахисник». (2023). Deepfake-фішинг: як розпізнати штучне відео та аудіо. [Електронний ресурс]. Режим доступу: https://cyberdefense.org.ua/

4. Коцюба, І. В., & Петренко, С. О. (2022). Штучний інтелект як інструмент кібервойни: загроза deepfake-технологій для інформаційної безпеки України. Вісник Київського національного університету імені Тараса Шевченка. Інформатика, кібербезпека, 45(2), 56-67.

5. СБУ. (2024). Огляд кіберзагроз: використання deepfake для цілеспрямованих атак. Служба безпеки України. [Електронний ресурс]. Режим доступу: https://ssu.gov.ua/

6. Український інститут кібербезпеки. (2023). Навчальний посібник з виявлення маніпуляцій з медіа-контентом. Київ: Видавництво УІК.

УДК 004.738.5:316.774:355.45

РОЛЬ ТА ПРОБЛЕМИ МЕСЕНДЖЕРІВ І СОЦІАЛЬНИХ МЕРЕЖ У ІНФОРМАЦІЙНИХ ВІЙНАХ

Матвій ЗАПОРОЖЦЕВ
Львівський національний університет ветеринарної медицини та біотехнологій імені С.З. Ґжицького

Анотація. *Досліджується критична роль соціальних медіа та месенджерів як інструментів гібридного протистояння в умовах повномасштабної агресії РФ. На основі емпіричних даних (ОПОРА, ЦЕДЕМ) представлено кількісні показники використання соцмереж українцями та проаналізовано ключові виклики модерації контенту. Визначено специфіку застосування ворожих інструментів впливу (дезінформація, астротурфінг) та охарактеризовано проблеми українських медіа, зокрема блокування, самоцензура та неадекватність глобальних стандартів до воєнного контексту. Запропоновано конкретні напрями оптимізації взаємодії з платформами.*

Ключові слова: *гібридна війна, соціальні медіа, дезінформація, модерація, самоцензура, Meta, Telegram.*

Abstract. *The critical role of social media and messengers as tools of hybrid confrontation in the context of full-scale aggression by the Russian Federation is being studied. Based on empirical data (OPORA, CEDEM), quantitative indicators of social media use by Ukrainians are presented and key challenges of content moderation are analyzed. The specifics of the use of hostile instruments of influence (disinformation, astroturfing) are identified and the problems of Ukrainian media, in particular blocking, self-censorship, and the inadequacy of global standards to the military context, are characterized. Specific directions for optimizing interaction with platforms are proposed..*

Keywords: *hybrid warfare, social media, disinformation, moderation, self-censorship, Meta, Telegram.*

Сучасне інформаційне протиборство, що є ключовим компонентом гібридної війни, критично залежить від платформ соціальних медіа. Воно було вепонізовано. З початку повномасштабного вторгнення ці платформи перетворилися на головний канал комунікації в Україні: за даними, емпірично отриманими мережею ОПОРА, за 2023 рік 77,9% українців визнали соцмережі основним джерелом новин. Ця висока проникність робить їх ідеальною ціллю для реалізації агресивних інформаційно-психологічних операцій (ІПСО).

Вороже використання платформ ґрунтується на їх масштабі, швидкості та анонімності. Аналіз свідчить, що соціальні медіа застосовуються для: збору розвідданих (на основі геотегів та відкритих

даних); таргетингу; кібероперацій (зламування акаунтів, поширення фішингу); а також для ведення інформаційно-психологічної війни. При цьому активно застосовуються технології астротурфінгу - імітації масової народної ініціативи через ботоферми - та діяльність "гібридних тролів", які координуються державою-агресором. Наприклад, цілі російської дезінформації у 2023 році сфокусувалися на двох найбільш чутливих темах: корупція (зокрема, "армійська") та мобілізація.

Критичним викликом для українського інформаційного простору є неадаптованість глобальних стандартів модераці (зокрема, Meta/Facebook) до воєнних реалій. Українські медіа та блогери регулярно стикаються з видаленням контенту, зниженням охоплення та блокуванням через публікацію чутливих матеріалів про війну. Найбільші обмеження прилітають за мову ворожнечі щодо окупантів ("орки", "свинособаки") та кадри російської агресії.

Результати дослідження The FIX, проведеного на замовлення Центру демократії та верховенства права (ЦЕДЕМ), виявили, що блокування акаунтів більш поширене серед блогерів, ніж серед медіа. Обидві групи вказали на Facebook та Instagram як на джерела найбільших труднощів. Унаслідок такої жорсткої, часто контекстно-сліпої, модерації, більшість опитаних медіа та блогерів вдаються до самоцензури, утримуючись від публікації певного суперечливого контенту, щоб зберегти свої платформи.

Особливі проблеми виникають через нездатність алгоритмів розпізнати сатиру та контекст історичних паралелей, наприклад, видання Liga.net отримало чотиримісячний бан за добірку мемів про похід вагнерівців, оскільки Facebook класифікував це як пропаганду небезпечної організації. Подібні помилки трапляються при модеруванні контенту про підрозділ Азов або порівнянь Путіна з Гітлером, які не враховують захисний характер української позиції.

Для оптимізації роботи в цифровому просторі - необхідний постійний діалог та тиск на глобальні платформи. ЦЕДЕМ, виступаючи як довірений партнер Facebook в Україні, лише за 2023 рік подав понад 800 апеляцій, що підкреслює високу частоту виникнення спірних ситуацій. Експерти також зазначають, що співпраця є плідною у випадках відновлення зламаних хакерами сторінок та боротьби з дезінформацією, яка зараз "більше доби не живе". Водночас, розгляд деяких складних кейсів може тривати з осені.

На основі цього досвіду були розроблені чіткі рекомендації для соціальних мереж:

1. Контекстуальна модерація: Розглянути можливість не блокувати контент з образливими висловлюваннями (на зразок "орки") на адресу загарбників, а не всіх росіян.

2. Визнання права на самооборону: Розглянути можливість не блокувати контент із закликами до насильства проти керівництва РФ, оскільки Україна захищається від агресії.
3. Розробка «білого списку»: Створити спільно з українськими партнерами білий список медіа, щоб спрямувати трафік до надійних, верифікованих джерел інформації.
4. Створення представництв: Створити сприятливі умови для відкриття представництв соціальних мереж в Україні для кращого розуміння локального контексту.

Керівниця регіональної політики Meta, Катерина Крук, підтвердила, що не існує московського офісу Facebook, а функція "заблюреного зображення" (розмитого екрану) використовується для збереження свідчень злочинів без зняття охоплення дописів. Можливість оскаржувати рішення до Наглядової ради Meta також залишається важливим механізмом впливу, який, хоча і обмежений у ресурсах, розглядає найважливіші та найпринциповіші питання, які стосуються публічного інтересу.

Отже, аналіз підтверджує: існує критичний конфлікт між універсальними стандартами модерації глобальних цифрових платформ та потребами цифрової оборони України. Ця невідповідність веде до системної самоцензури медіа та створює вразливість перед ворожими ІПСО. Стратегічний вихід полягає у негайній імплементації чітких рекомендацій - від контекстуальної модерації до створення "білих списків" верифікованих джерел. Міжнародна спільнота має використати досвід України для створення нового стандарту, який зобов'яже великі платформи краще усвідомлювати їх відповідальність у цій справі та протидіяти цифровим та інформаційним небезпекам.

Література

1. Соціальні мережі під час війни: український досвід модерації контенту [Електронний ресурс] / Центр демократії та верховенства права (ЦЕДЕМ). – Київ, 2023. – Режим доступу: https://cedem.org.ua/news/sotsialni-merezhi-pid-chas-viyny/.

2. "Ваш допис було вилучено". Вплив соціальних мереж на український інформаційний простір після початку повномасштабного вторгнення : Аналітичний звіт. Київ: The FIX, 2023.

3. Nissen T. E. Social Media as a Tool of Hybrid Warfare. Riga: NATO Strategic Communications Centre of Excellence, 2015. 107 p.

4. Кучмій О., Фролова О. Використання соціальних медіа як ефективного інструменту гібридної війни у сучасному світі // Acta de Historia & Politica: Saeculum XXI. – 2023. – Special Issue. – С. 93–101. – DOI: 10.26693/ahpsxxi2023.si.093. – Режим доступу: https://ahpsxxi.org/index.php/journal/article/view/99.

УДК 004.056.5

ПРОТИДІЯ ГІБРИДНИМ ІНФОРМАЦІЙНИМ ВІЙНАМ У ЦИФРОВОМУ СЕРЕДОВИЩІ

Даниіл ЗАХАРЕВИЧ, Валентина ЯЩУК, Ростислав ТКАЧУК
Львівський державний університет безпеки життєдіяльності

Анотація. *Досліджено сутність, структуру та особливості гібридних інформаційних війн у сучасному цифровому середовищі, проаналізовано ефективні стратегії протидії цим явищам. Визначено основні технологічні, психологічні та комунікаційні інструменти, що використовуються для дестабілізації суспільної свідомості, впливу на політичні процеси та руйнування інформаційної безпеки держави. Розкрито роль цифрових медіа, соціальних мереж, штучного інтелекту та автоматизованих бот-мереж у створенні та поширенні дезінформації. Запропоновано системний підхід до протидії гібридним інформаційним впливам, що базується на поєднанні технологічних, освітніх та регуляторних інструментів.*

Ключові слова: *гібридна війна, інформаційна безпека, дезінформація, цифрове середовище, кіберзахист.*

Abstract. *The essence, structure and features of hybrid information wars in the modern digital environment are studied, effective strategies for countering these phenomena are analyzed. The main technological, psychological and communication tools used to destabilize public consciousness, influence political processes and destroy the information security of the state are identified. The role of digital media, social networks, artificial intelligence and automated botnets in the creation and spread of disinformation is revealed. A systematic approach to countering hybrid information influences is proposed, based on a combination of technological, educational and regulatory tools.*

Keywords: *hybrid war, information security, disinformation, digital environment, cyber defense.*

У XXI столітті інформаційний простір став ключовим театром ведення гібридних конфліктів, у яких цифрові технології використовуються як зброя стратегічного впливу. Гібридна інформаційна війна поєднує традиційні засоби пропаганди з інноваційними технологіями кібернетичного, психологічного та когнітивного тиску на масову свідомість. Особливістю сучасного етапу є синергія між класичними інформаційними операціями та інструментами штучного інтелекту — генерацією контенту (deepfake), таргетованими кампаніями у соціальних мережах, маніпуляціями з метаданими та автоматизованим поширенням фейкової інформації через бот-мережі.

Гібридна агресія спрямована не лише на підрив політичної стабільності, а й на формування викривлених уявлень про реальність. Її головна мета — не знищення інформаційної інфраструктури, а дестабілізація сус-

пільної довіри до державних інституцій, ЗМІ та наукової спільноти. У цьому контексті інформаційна війна набуває характеру довготривалого процесу, де межа між миром і конфліктом стає розмитою.

Для ефективної протидії гібридним інформаційним впливам необхідна комплексна стратегія, що поєднує технічні, організаційні та освітні підходи. На технологічному рівні першочерговим є створення систем раннього виявлення дезінформаційних кампаній, здатних здійснювати автоматичний моніторинг інформаційних потоків у реальному часі із застосуванням методів машинного навчання, аналізу соціальних графів та семантичного кластерування контенту. Такі системи дозволяють ідентифікувати координацію між бот-акаунтами, виявляти ознаки штучної вірусності контенту та визначати першоджерела інформаційних атак.

На когнітивно-комунікативному рівні актуальним є розвиток медіаграмотності та критичного мислення як базових компетенцій громадян цифрової доби. Формування здатності розпізнавати маніпуляції, фейки та інформаційні пастки знижує вразливість суспільства до деструктивного впливу. У цьому контексті важливим завданням держави та освітніх інституцій є інтеграція навчальних програм з інформаційної гігієни, фактчекінгу та етичного споживання медіаконтенту на всіх рівнях освіти.

Водночас, стратегічна протидія потребує інституційного зміцнення системи національної інформаційної безпеки, удосконалення законодавства щодо відповідальності за поширення дезінформації, регулювання діяльності цифрових платформ і створення незалежних аналітичних центрів для оцінювання інформаційних ризиків. Особливе значення має співпраця державних структур із науковими установами, медіа та громадським сектором, що забезпечує багаторівневу координацію та ефективність протидії гібридним загрозам.

З огляду на стрімкий розвиток технологій штучного інтелекту, особливо в галузі оброблення природної мови (Natural Language Processing, NLP), одним із найбільш перспективних напрямів сучасних досліджень є створення інтелектуальних систем автоматичного виявлення дезінформації на основі глибинних нейронних мереж. Такі системи мають на меті аналізувати текстові повідомлення з урахуванням їхніх синтаксичних, семантичних і прагматично-емоційних характеристик, що дає змогу виявляти не лише відверті неправдиві твердження, а й приховані маніпулятивні патерни, риторичні викривлення та когнітивні упередження.

У межах цього підходу застосовуються архітектури нейронних мереж типу Transformer (зокрема, BERT, RoBERTa, GPT, T5), які здатні враховувати контекст між словами та реченнями, моделюючи смислові зв’язки в тексті. Аналіз дезінформації відбувається у кілька етапів: семантична нормалізація (очищення тексту від шумових елементів), векторизація (перетворення лінгвістичних ознак у числові представлення), класифі-

кація (розмежування достовірної й маніпулятивної інформації) та оцінка впевненості моделі.

Водночас проблема достовірності джерел інформації залишається ключовою. У цьому контексті перспективним є поєднання технологій штучного інтелекту з блокчейн-архітектурою, яка може забезпечити верифікацію походження інформаційних повідомлень і незмінність цифрових записів. Застосування блокчейну дозволяє створити децентралізовану систему маркування контенту, де кожне повідомлення має унікальний цифровий підпис, що підтверджує його джерело, час створення та історію змін. Такий підхід сприяє підвищенню рівня довіри до інформаційних ресурсів і формуванню механізмів відповідальності за поширення фейків. Таким чином, розвиток нейромережевих систем детекції дезінформації у поєднанні з блокчейн-технологіями є ключовим елементом формування стійкої цифрової інфраструктури безпеки, яка базується на принципах прозорості, достовірності та відповідальності за інформаційний вплив.

Протидія гібридним інформаційним війнам потребує системного підходу, який поєднує технологічні інновації, освітню політику та державне регулювання. Ефективність інформаційного захисту визначається не лише наявністю технічних засобів моніторингу, а й рівнем критичного мислення населення, здатністю суспільства протистояти маніпуляціям і формувати власний аналітичний погляд на інформаційні процеси. Запропонована концепція багаторівневої протидії, що включає кіберзахист, аналітичні системи, освіту та міжнародну співпрацю, є основою побудови сталого інформаційного простору. У перспективі подальші дослідження мають бути спрямовані на розроблення моделей когнітивної безпеки, систем штучного інтелекту для виявлення фейків і створення етичних стандартів комунікації в цифровому середовищі.

Література

1. Yashchuk V. The Role And Place Of Cyber Weapons In Ensuring The Information Security Of The State / Yashchuk V. // Інноваційні технології в лінгвістиці та перекладі: Зб. наук. праць Міжнародної наукової конференції. – Львів: ЛДУ БЖД, 2024. – С.41-44.

2. Ящук В.І. Роль та місце стратегії кібербезпеки України у забезпеченні інформаційної безпеки держави / В.І.Ящук // Moderní aspekty vědy: XLII. Díl mezinárodní kolektivní monografie / Mezinárodní Ekonomický Institut s.r.o.. Česká republika: Mezinárodní Ekonomický Institut s.r.o., 2024. str. 364 (С. 259-286) 1,5 д.а. https://doi.org/10.52058/42-2024

3. Yashchuk, V., Demyanchuk, Y., & Savitska, V. (2025). Integrative approach to the analysis, modeling, and ensuring cyber security of critical information infrastructure under modern threats. Baltic Journal of Economic Studies, 11(2), 273-286. https://doi.org/10.30525/2256-0742/2025-11-2-273-286

УДК 4.8:004.056.5

ШТУЧНИЙ ІНТЕЛЕКТ У ПІДВИЩЕННІ БЕЗПЕКИ ПЕРСОНАЛЬНИХ ДАНИХ

Олег ЗАЧЕК
Львівський державний університет внутрішніх справ

Анотація. *У роботі досліджено загрози персональним даним у кіберінформаційних системах, що посилилися в умовах війни, та вразливості цифрового середовища. Проаналізовано можливості штучного інтелекту у виявленні, попередженні й нейтралізації кібератак. Показано ефективність ШІ у підвищенні безпеки даних і автоматизації реагування на інциденти.*

Ключові слова: *персональні дані; кібербезпека; кібератаки; соціальний інжиніринг; фішинг; штучний інтелект; виявлення загроз; захист інформації.*

Abstract. *The study examines threats to personal data in cyber-information systems, which have intensified during the war, as well as vulnerabilities of the digital environment. The potential of artificial intelligence in detecting, preventing, and neutralizing cyberattacks is analyzed. The effectiveness of AI in enhancing data security and automating incident response demonstrated.*

Keywords: *personal data; cybersecurity; cyberattacks; social engineering; phishing; artificial intelligence; threat detection; information protection*.

Актуальність захисту персональних даних зростає через широке використання кіберінформаційних систем у фінансах, освіті, медицині та соціальних мережах, а також збільшення обсягу цифрових даних. У воєнний час інтенсивність кібератак різко зросла: зламують державні, військові та приватні інформаційні системи, а викрадені персональні дані використовують для шантажу, дезінформації чи переслідування. Додаткові ризики для витоку даних створюють мобілізаційні процеси та переміщення населення. Основні загрози включають кіберзлочини, недостатній захист баз даних, маніпуляції персональними даними, соціальний інжиніринг і фішинг. Війна посилює небезпеки військових кібероперацій, викрадення інформації з державних реєстрів, таргетованих атак на активних громадян, дезінформації та фішингових схем, замаскованих під теми війни.

У 2022 році CERT-UA зафіксувала поширення в популярних месенджерах фішингових повідомлень, у яких під виглядом соціальних виплат для українських біженців користувачів спонукали перейти за посиланням і ввести дані онлайн-банкінгу. Зловмисники створювали підроблені сайти, що імітували ресурси українських банків [1]. У 2024 році CERT-UA також повідомила про кампанію угруповання UAC-0102, яке розповсюджувало листи з архівами, що містили HTML-файли. Після відкриття користувача

перенаправляло на підроблену сторінку UKR.NET, де введені облікові дані передавалися зловмисникам, а на комп'ютер жертви завантажувався файл-приманка [2]. Подібних спроб викрадення персональних даних громадян України під час воєнного стану фіксується значна кількість.

Вразливості та недоліки захисту персональних даних під час війни є наступними:

- Відсутність ресурсів і часу на оновлення систем безпеки у критичних інфраструктурах.
- Підвищений обсяг даних, що циркулює через онлайн-сервіси (реєстрація ВПО, гуманітарна допомога).
- Використання громадянами небезпечних або ненадійних додатків для зв'язку та обміну даними.
- Ризики атак на хмарні сервіси, де зберігаються резервні копії баз даних.

Одним із ефективних способів посилення захисту персональних даних є застосування штучного інтелекту (ШІ) для виявлення загроз в автоматичному режимі. Завдяки можливості швидко аналізувати великі масиви даних, здійснювати прогноз ризиків та реагувати на інциденти, ШІ стає ключовим елементом кіберзахисту. На відміну від традиційних інструментів і роботи аналітиків, які не встигають за складністю сучасних атак, ШІ безперервно моніторить трафік, поведінку користувачів і системні журнали, виявляючи аномалії. Такі системи здатні фіксувати найменші ознаки компрометації та автоматично запускати захисні дії. Крім того, моделі ШІ постійно вдосконалюються, навчаючись на нових видах атак і оновлюючи механізми протидії кіберагресії [3].

Можливості ШІ у захисті персональних даних охоплюють широкий спектр завдань [4]:

1. Виявлення аномалій: ШІ аналізує поведінку користувачів у реальному часі та фіксує підозрілі дії, наприклад масові запити до баз даних.

2. Протидія фішингу: Алгоритми обробки природної мови розпізнають фішингові повідомлення та автоматично блокують їх або попереджають користувача.

3. Шифрування даних та контроль доступу: ШІ формує адаптивні системи шифрування та керує правами доступу відповідно до ролі й поведінки користувача.

4. Захист від Zero-Day атак: Аналізуючи численні шаблони атак, ШІ може виявляти нові загрози ще до їх офіційної ідентифікації.

5. Запобігання витоку даних: DLP-системи на основі ШІ контролюють передачу конфіденційної інформації й виявляють несанкціоноване копіювання чи пересилання.

6. Моделювання атак: ШІ проводить автоматичні симуляції кібератак для виявлення вразливостей, зокрема ризиків від внутрішніх користувачів.

7. Автоматична реакція: Системи ШІ можуть блокувати облікові записи, ізолювати заражені пристрої та сповіщати адміністраторів.

8. Підвищення кібергігієни: Інструменти ШІ навчають безпечній поведінці, дають рекомендації щодо зміцнення захисту, наприклад у разі слабких паролів.

9. Опрацювання великих даних: ШІ класифікує масиви персональних даних, оцінює їх чутливість та контролює доступ до них.

10. Прогнозування загроз: Моделі машинного навчання дозволяють передбачати нові вектори атак і тенденції поширення певних типів загроз.

Практичними прикладами застосування ШІ для подолання кіберзагроз можуть бути:

1. Darktrace – платформа кібербезпеки, що використовує ШІ для того щоб виявляти та нейтралізувати загрози у режимі реального часу.

2. Microsoft Azure Sentinel – хмарна система, яка інтегрує ШІ для аналізу великих обсягів журналів безпеки та пошуку аномалій.

3. Palo Alto Networks Cortex XDR – використовує ШІ для виявлення, розслідування та ліквідації кіберзагроз.

Висновок. Отже, ШІ значно підвищує ефективність систем захисту персональних даних, даючи змогу оперативно виявляти, аналізувати загрози та реагувати на них. Інтеграція ШІ в системи захисту інформації є критичною необхідністю в умовах стрімкого зростання кіберзагроз і обсягів обробки персональної інформації. Тому вважаю, що в умовах загроз, які виникають під час воєнного стану, необхідно дедалі ширше використовувати засоби ШІ для захисту персональних даних. Але для повноцінного використання цих технологій важливо забезпечити надійність алгоритмів, уникати їх упередженості та забезпечити відповідність етичним нормам.

Література

1. Онлайн-шахрайство з використанням тематики "допомоги від Червоного Хреста" (CERT-UA#5063) // Новини CERT-UA від 27.07.2022. URL: https://cert.gov.ua/article/6280345 (дата звернення: 21.11.2025).

2. Кібератаки UAC-0102 з метою викрадення автентифікаційних даних облікових записів користувачів UKR.NET (CERT-UA#10381) // Новини CERT-UA від 24.07.2024. URL: https://cert.gov.ua/article/6280183 (дата звернення: 21.11.2025).

3. AI in Cybersecurity: Smarter Threat Detection and Response // DATAFOREST from November 19, 2024. URL: https://dataforest.ai/blog/ai-in-cybersecurity-smarter-threat-detection-and-response (дата звернення: 21.11.2025).

4. Zehan Wang. Artificial Intelligence in Cybersecurity Threat Detection. // International Journal of Computer Science and Information Technology. Vol. 4 No. 1 (2024). Pp. 203-209. URL: https://www.researchgate.net/publication/384127618_Artificial_Intelligence_in_Cybersecurity_Threat_Detection (дата звернення: 21.11.2025).

УДК 004.056:004.7

ПРОЕКТУВАННЯ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ ДЛЯ МЕРЕЖ ІНТЕРНЕТУ РЕЧЕЙ

Андрій ІВАНУСА, Мар'ян ТКАЧ, Андрій ПЕТРОВИЧ, Юрій ТКАЧ
Львівський державний університет безпеки життєдіяльності

Анотація. *У роботі спроектовано архітектуру захищеної IoT-системи та розроблено комплексний підхід до її захисту. Запропоноване рішення поєднує шифрування TLS/SSL, апаратний модуль TPM, рольовий контроль доступу та поведінкову аналітику UBA для забезпечення надійності та протидії загрозам у мережах Інтернету речей.*

Ключові слова: *інтернет речей, кібербезпека, протоколи IoT, TPM, MQTT, шифрування, контроль доступу.*

Abstract. *he paper designs the architecture of a secure IoT system and develops a comprehensive approach to its protection. The proposed solution combines TLS/SSL encryption, a TPM hardware module, role-based access control, and User Behavior Analytics (UBA) to ensure reliability and counter threats in Internet of Things networks.*

Keywords: *Internet of Things, cybersecurity, IoT protocols, TPM, MQTT, encryption, access control.*

Стрімкий розвиток технологій Інтернету речей вимагає нових підходів до проектування мережевої інфраструктури, де питання безпеки стають критично важливими. При проектуванні мережі Інтернету речей необхідно включати дві складові: фізичне проектування мережі, яке охоплює пристрої та протоколи, та логічне проектування, що представляє абстрактне розуміння сутностей і процесів . Відсутність єдиних стандартів безпеки робить вразливими більшість сучасних IoT-систем, що зумовлює необхідність розробки комплексних рішень захисту на всіх рівнях архітектури.

В основі розробленої системи лежить чотирирівнева модель протоколів, що забезпечує надійну взаємодію між пристроями та сервером. На канальному рівні використовуються технології IEEE 802.11 (WiFi) для всіх сенсорів, хоча також можуть застосовуватися Ethernet, WiMax та LR-WPAN. Мережевий рівень базується на протоколі IPv4, що забезпечує ідентифікацію хостів та адресацію, з підтримкою 6LoWPAN для малопотужних мереж. Транспортний рівень реалізує підтримку TCP для надійного зв'язку та UDP для швидкої передачі даних. На рівні додатків використовуються протоколи MQTT для міжмашинної взаємодії, WebSocket для двостороннього зв'язку, а також HTTP та CoAP.

Для практичної реалізації системи було обрано топологію, що включає розумний дверний замок, датчик відкриття вікна, розумну лампу, дат-

чик включення світла та шлюз, який виконує роль базової станції . Шлюз відповідає за маршрутизацію даних, при цьому мережа Інтернету речей ізольована в адресному просторі 192.168.25.0/24, що ускладнює несанкціонований доступ зловмисників. Взаємодія компонентів системи базується на моделі "запит-відповідь" та Push-Pull із використанням REST та WebSocket API.

Оскільки дослідження показують, що більшість IoT систем не шифрують трафік, у розробленій системі впроваджено багаторівневу модель захисту, графічне зображення якої наведено на рисунку нижче. Запропонована концепція безпеки охоплює забезпечення безпеки зв'язку, контроль доступу, апаратний захист та операційні заходи безпеки.

Для захисту каналів передачі даних обрано метод Еліптичної криптографії, який є ефективним для пристроїв з обмеженими обчислювальними ресурсами. Шифрування та аутентифікація реалізуються через протокол TLS/SSL поверх MQTT на платформі IBM Watson IoT Platform. Замість прямого підключення датчиків використовується смартфон з додатком, що проходить етап аутентифікації через токени. Додатково в систему впроваджено сертифікат безпеки X.509 для унікальної ідентифікації пристроїв, що дозволяє визначити довірені вузли та обмежити доступ для непідтверджених девайсів.

Важливим елементом захисту є впровадження контролю доступу та безпеки управління через рольову модель. Створено спеціальні ролі, які обмежують права пристроїв та шлюзу, дозволяючи їм виконувати лише необхідні операції. Для виявлення загроз використовується аналітична система безпеки UBA, яка будує модель поведінки користувача та виявляє аномальну активність. Також проводиться регулярний місячний аудит інфраструктури за допомогою сервісу AWS IoT Device Defender.

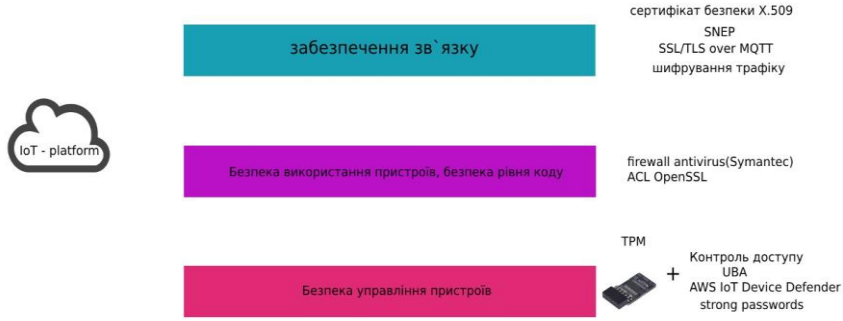

Рисунок 1 – Система методів безпеки для спроектованої системи

Для підвищення захищеності від фізичного злому та підробки ключів впроваджено апаратний модуль TPM. Він забезпечує цілісність пристрою, створює корінь довіри та генерує ключі шифрування, працюючи в безпечному режимі для мінімізації шкоди від шкідливого програмного забезпечення . На рівні коду безпека забезпечується використанням бібліотеки OpenSSL для перевірки автентичності, а також обмеженням функціоналу програмного коду пристроїв лише виконанням специфічних завдань, що запобігає їх використанню у ботнетах.

Додаткові операційні заходи безпеки включають використання брандмауера для контролю вхідного і вихідного трафіку, встановлення антивірусного програмного забезпечення Symantec, регулярне оновлення прошивок із перевіркою безпечного завантаження та використання надійних унікальних паролів .

У підсумку, в роботі спроектовано захищену IoT систему, що базується на комплексному підході до інформаційної безпеки. Реалізована архітектура поєднує ізольовану мережеву топологію з використанням надійних протоколів. Основна наукова та практична цінність полягає у впровадженні комбінованої системи захисту, яка включає криптографічний захист трафіку, сувору аутентифікацію, апаратний захист та інтелектуальний аналіз загроз. Такий підхід дозволяє нівелювати ризики компрометації пристроїв та забезпечити цілісність і конфіденційність даних у мережі Інтернету речей.

Література

1. Cirani S., Ferrari G., Picone M., Veltri L. Internet of Things: Architectures, Protocols and Standards. Hoboken : Wiley, 2018. 376 p.

2. Suthar S., Das R. Demystifying Internet of Things Security : Successful IoT Device/Edge and Cloud Security Design. Berkeley : Apress, 2019. 339 p.

3. MQTT Version 3.1.1 : OASIS Standard / ed. by A. Banks, R. Gupta. OASIS, 2014. URL: http://docs.oasis-open.org/mqtt/mqtt/v3.1.1/os/mqtt-v3.1.1-os.html (дата звернення: 27.10.2025).

4. Arthur W., Challener D. A Practical Guide to TPM 2.0: Using the Trusted Platform Module in the New Age of Security. New York : Apress, 2015. 343 p.

5. Shelby Z., Hartke K., Bormann C. The Constrained Application Protocol (CoAP) : RFC 7252. IETF, 2014. 112 p. URL: https://tools.ietf.org/html/rfc7252 (дата звернення: 27.10.2025).

УДК 004.7:004.056

ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ КОРПОРАТИВНИХ СИСТЕМ НА ОСНОВІ ТЕХНОЛОГІЇ SD-WAN

Андрій ІВАНУСА, Андрій ПЕТРОВИЧ, Мар'ян ТКАЧ, Юрій ТКАЧ
Львівський державний університет безпеки життєдіяльності

Анотація. *У роботі розглянуто впровадження технології SD-WAN для модернізації корпоративної мережі підприємств енергетичного сектору. Проаналізовано переваги програмно-визначальних мереж над традиційними MPLS-каналами, зокрема в аспектах кібербезпеки, автоматизації управління та інтеграції з хмарними сервісами. Описано етапи реалізації проекту на прикладі підприємства енергетики для забезпечення кіберстійкості інфраструктури.*

Ключові слова: *SD-WAN, інформаційна безпека, корпоративна мережа, автоматизація, хмарні технології.*

Abstract. *The paper considers the implementation of SD-WAN technology to modernize the corporate network of energy sector enterprises. The advantages of software-defined networks over traditional MPLS channels are analyzed, in particular in the aspects of cybersecurity, management automation, and integration with cloud services. The stages of project implementation are described using the example of an energy enterprise to ensure cyber resilience of the infrastructure.*

Keywords: *SD-WAN, information security, corporate network, automation, cloud technologies.*

Глобальні мережі протягом тривалого часу залишаються критично важливим елементом розвитку технологій, забезпечуючи передачу даних на великі відстані як для військових, так і для корпоративних потреб. Здатність долати географічні обмеження стала рушійною силою вдосконалення систем захисту інформації. Однак традиційні підходи, такі як використання виділених каналів MPLS, перестають відповідати вимогам сучасного хмарного середовища, яке швидко розвивається. Це зумовило появу та активне впровадження програмно-визначальних глобальних мереж (SD-WAN), що дозволяють шифрувати дані в накладених тунелях та забезпечують гнучкість управління трафіком.

Технологія дозволяє об'єднувати різні типи фізичних з'єднань, такі як широкосмуговий інтернет, 4G LTE та MPLS, у єдиний логічний канал зв'язку для підвищення відмовостійкості. Це створює надійну віртуальну надбудову, яка відокремлює програмне забезпечення від фізичного обладнання та забезпечує безперервність сервісів навіть при збоях окремих ліній.

На відміну від традиційної архітектури, модель SD-WAN розроблена для повної підтримки програм, розміщених у локальних центрах обробки даних, а також у публічних і приватних хмарах. Технологія дозволяє

автоматично та динамічно перенаправляти трафік найбільш ефективним шляхом, враховуючи умови мережі, вимоги безпеки та якість обслуговування (QoS). Важливою перевагою є централізоване керування, що підвищує продуктивність додатків та знижує витрати на IT-інфраструктуру. Здатність ідентифікувати підозрілі програми та віртуалізувати послуги WAN, включаючи MPLS та 4G/LTE, дозволяє підприємствам безпечно використовувати широкосмуговий зв'язок як основний канал передачі даних.

Завдяки підтримці ініціалізації без участі користувача (Zero Touch Provisioning), конфігурація нових пристроїв завантажується автоматично одразу після підключення до мережі. Такий підхід усуває необхідність фізичної присутності кваліфікованих інженерів на кожній локації, що скорочує час запуску нових філій з кількох днів до лічених годин.

Особливої актуальності впровадження SD-WAN набуває для стратегічно важливих підприємств, таких як Група ДТЕК, що працюють в умовах підвищених ризиків воєнного часу. Складність мережевої інфраструктури та організаційна розгалуженість компанії вимагають підвищення надійності підключення для сотень територіально розподілених філій . Модернізація корпоративної мережі на базі рішення VMware SD-WAN дозволяє уніфікувати підключення, забезпечити гнучку взаємодію з хмарними середовищами та автоматизувати рутинні завдання керування.

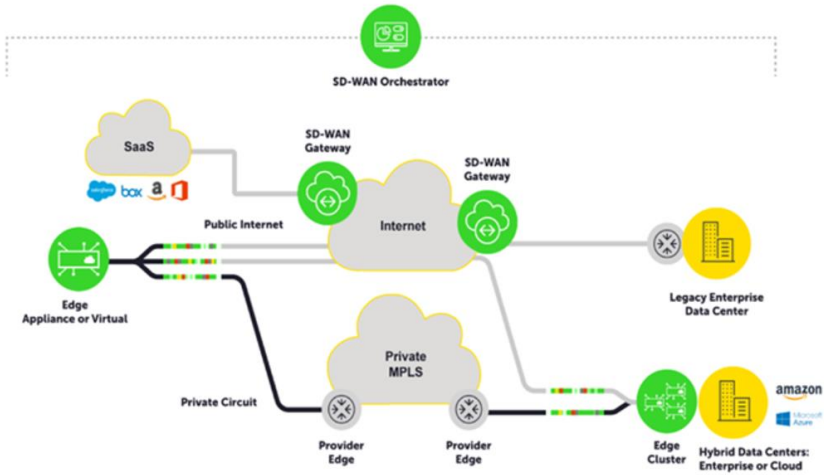

Рисунок 1 – Архітектура рішення SD-WAN

Система здатна автоматично розпізнавати та пріоритезувати чутливий до затримок трафік, зокрема для засобів відеоконференцзв’язку та платформи Microsoft Teams. Це дозволяє забезпечити стабільно високу якість

уніфікованих комунікацій для ефективної взаємодії територіально розподілених команд незалежно від їхнього розташування.

Проект імплементації включає повний життєвий цикл: від аналізу потреб та проектування до впровадження пілотного рішення та інтеграції з існуючими системами безпеки. В результаті впровадження програмно-конфігурованої архітектури компанія отримує гнучку мережу, що легко масштабується, спрощене централізоване керування та можливість швидкого підключення нових філій . Це критично важливо для ефективної роботи розподілених команд та забезпечення безперервності бізнес-процесів в енергетичному секторі, який є критичною інфраструктурою для України.

Ключовим аспектом нової архітектури є підвищення рівня кібербезпеки. Мережа забезпечує повну видимість трафіку, підтримку сучасних методів шифрування та сегментацію для мінімізації збитків у разі порушень периметра . Окрім того, автоматизація процесів дозволяє усунути ризики, пов'язані з людським фактором, та звільнити ресурси IT-фахівців для стратегічних проектів розвитку. Таким чином, перехід на SD-WAN є комплексним рішенням, що забезпечує не лише технічну модернізацію, але й стратегічну стійкість та безпеку корпоративних систем.

Література

1. Goransson P., Black C., Culver T. Software Defined Networks: A Comprehensive Approach. 2nd ed. Morgan Kaufmann, 2016. 436 p.

2. Kerravala Z. The width and breadth of software-defined WAN. Network World. 2018. URL: https://www.networkworld.com/article/3268802/the-width-and-breadth-of-software-defined-wan.html (дата звернення: 11.11.2025).

3. Troia S. et al. SD-WAN: An Enabler for Network Function Virtualization and Software Defined Networking. IEEE Communications Magazine. 2020. Vol. 58, no. 5. P. 98–104.

4. Стенлі Д. Віртуалізація мережевих функцій та SD-WAN: революція у корпоративних комунікаціях. Кібербезпека та комп'ютерна інженерія. 2021. № 2(34). С. 45–52.

5. VMware SD-WAN Security Architecture : White Paper. VMware, Inc., 2022. 18 p. URL: https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/sd-wan/vmware-sd-wan-security-architecture-wp.pdf (дата звернення: 11.11.2025).

УДК : 004.056.5:004.056.55

МОДЕЛЬ ЗАХИСТУ ДАНИХ ВІД OSINT НА ОСНОВІ МЕТОДУ КОМПАРТМЕНТАЛІЗАЦІЇ

Валерія ІВКОВА
Національний університет «Львівська політехніка»

Анотація. *Обґрунтовано необхідність протидії загрозам, що виникають внаслідок структурованого аналізу відкритих даних (OSINT). Запропоновано модель захисту на основі компартменталізації, що є проактивною стратегією структурованої ізоляції інформаційних активів. Сутність моделі полягає у дихотомічному поділі даних на непов'язані сегменти , що мінімізує ризик агрегування та істотно підвищує трудомісткість OSINT-аналізу.*

Ключові слова. *захист даних, OSINT, counter-OSINT, компартменталізація.*

Загальна кількість аналітиків, які здійснюють OSINT-розвідку точно невідома, оскільки така діяльність не має централізованості та стандартизації. Велика частина користувачів всесвітньої павутини використовують OSINT-технології для особистих або професійних потреб. Проте, точно можна стверджувати, що в світі інтерес до OSINT постійно зростає і цей процес не зупиняється.

В загальному розумінні OSINT - це процес збору та аналізу відкритих даних, тобто відомостей доступ до яких не обмежено володільцем.

На думку, Денисенко Б.А., OSINT необхідно розглядати як процес, інструмент, механізм збору та продажу програмних продуктів. OSINT є спільною, інтегрованою методологією та процесом створення, де вимоги клієнта щодо аналітичної розвідки співпадають з наданою дієвою аналітичною розвідкою (actionable intelligence), створеною через процес синтезу та аналізу репрезентативної вибірки інформації з відкритих джерел, яка була валідованою, є надійною, вчасною та точною [1, с.44]. Зазначене поняття найбільш повно розкриває сутність OSINT.

В кібербезпеці OSINT-технології більше сприймаються як методи, що дозволяють виявити відомості у відкритому доступі та визначити потенційні об'єкти для кібератак. Відкриті дані та великий перелік джерел таких відомостей, за умов їх структурованого аналізу, а також витоку конфіденційних даних породжують потенційно небезпечні наслідки у вигляді несанкціонованих втручань в роботу електронно-обчислювальної техніки, автоматизованих систем або комп'ютерних мереж, тощо. В умовах гібридної війни питання захисту інформації у відкритих джерелах гостро постає в контексті національної безпеки та захисту прав громадян.

Компартменталізація являє собою фундаментальний принцип кібербезпеки, що полягає в ізоляції окремих сегментів системи, наборів даних або

функціональних процесів. Ключове завдання цього підходу полягає в мінімізації потенційних ризиків та збитків, які можуть виникнути внаслідок компрометації одного з компонентів, чим досягається локалізація загрози та запобігання її горизонтальному поширенню на всю цілісність системи [2].

Даний метод знаходить активне застосування в галузі інформаційної безпеки, зокрема для захисту критично важливих (закритих) систем та забезпечення безпеки окремих програмних модулів (компонентів програмного забезпечення).

Модель захисту інформаційних активів від OSINT, що імплементується на методології компартменталізації, є проактивною стратегією структурованої ізоляції публічно доступних даних. Її першочерговою функцією є мінімізація ризику несанкціонованого агрегування та кумулятивного аналізу дискретних інформаційних фрагментів, отриманих з відкритих джерел.

Основна сутність моделі полягає у дихотомічному поділі сукупності даних (як корпоративних, так і індивідуальних) на логічно або фізично відокремлені, непов'язані сегменти (компартменти).

Ключовою метою є запобігання формуванню критично важливого інформаційного масиву шляхом кореляції розрізнених, імпліцитно безпечних даних, які можуть бути ідентифіковані OSINT-аналітиком. Таким чином, компрометація або ідентифікація інформації в межах одного компартменту не забезпечує суб'єкту доступу можливості для експлуатації або розуміння сутності інших ізольованих сегментів.

Ефективна реалізація моделі досягається шляхом дотримання низки взаємопов'язаних принципів.

Фундаментальною основою моделі є процедура ієрархічної класифікації наявних інформаційних активів, які потенційно можуть бути виявлені у відкритому доступі. Ця класифікація здійснюється на підставі критерію конфіденційності та розрахунку потенційної кумулятивної шкоди, спричиненої агрегацією даних. У результаті класифікації формуються взаємно виключні компартменти (логічні сегменти). Ключова мета полягає у забезпеченні гарантованої відсутності прямої кореляційної залежності між фрагментами даних, ідентифікованими зловмисником у різних сегментах, що унеможливлює формування цілісного та критично важливого інформаційного масиву.

Застосування принципу найменших привілеїв (PoLP) спрямоване на встановлення внутрішньої ізоляції даних. Доступ до інформації, локалізованої у кожному компартменті, надається суб'єктам або автоматизованим системам виключно на основі суворої службової необхідності (need-to-know basis). Така внутрішня політика мінімізує ймовірність несанкціонованого трансферу даних через внутрішні вектори атак, а також суттєво обмежує обсяг інформації, який може бути скомпрометований внаслідок порушення безпеки одного внутрішнього контуру.

Принцип мінімізації цифрового сліду передбачає проактивне зниження невпорядкованості чутливих даних, які потрапляють у публічну сферу. Він реалізується через розробку та імплементацію формалізованих регламентів, що регулюють обсяг, зміст та формат публікаційної активності. Обов'язковим елементом є систематична санітизація всіх технічних ідентифікаторів та метаданих (зокрема, геолокаційних даних, інформації про авторство чи програмне забезпечення) з документів, які призначені для відкритого доступу, чим досягається зменшення вектора атаки OSINT [3, с. 174].

Заключний принцип дезінтеграції асоціативних зв'язків - фокусується на штучному порушенні логічних та фізичних кореляцій між публічними ідентифікаторами, що належать різним компартментам. Це досягається, зокрема, через використання незалежних мережевих ресурсів (наприклад, різних діапазонів IP-адрес, незалежних доменних імен) та унеможливлення прямого зв'язку між зовнішніми профілями співробітників та внутрішніми конфіденційними організаційними структурами. Ця стратегія забезпечує істотне підвищення трудомісткості OSINT-аналізу та вимагає від зловмисника значних ресурсів для відновлення штучно дезінтегрованих асоціативних зв'язків.

Таким чином зазначена модель є критично важливою у контексті сучасного кіберзахисту. Вона зміщує парадигму захисту з орієнтації на класичний периметр системи на ізоляцію самої інформації у відкритому інформаційному просторі.

Література

1. Денисенко Б.А., МЕТОДОЛОГІЧНІ ЗАСАДИ OSINT / Актуальні питання та перспективи розвитку кримінального аналізу в правоохоронній системі України: матеріали міжвідом. наук.-практ. конф. Режим доступу: https://elar.navs.edu.ua/server/api/core/bitstreams/b993bb75-5950-4259-934e-83733f4fe8ab/content

2. Javorsek, D., Rose, J., Marshall, C., & Leitner, P. (2015). A Formal Risk-Effectiveness Analysis Proposal for the Compartmentalized Intelligence Security Structure. International Journal of Intelligence and CounterIntelligence, 28(4), 734–761. https://doi.org/10.1080/08850607.2015.1051830

3. Івкова, В., & Опірський, І. (2025). OSINT-ТЕХНОЛОГІЇ ЯК ЗАГРОЗА КІБЕРБЕЗПЕЦІ ДЕРЖАВИ. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3(27), 165–179. ht10tps://doi.org/10.28925/2663-4023.2025.27.749

УДК 004.8:004.056:004.738.5

ІНТЕГРАЦІЯ SIEM, АВТОМАТИЗОВАНОГО МОНІТОРИНГУ ТА МОДЕЛЕЙ ПОВЕДІНКОВОГО АНАЛІЗУ ДЛЯ КОРПОРАТИВНОЇ БЕЗПЕКИ

Артем ІЩЕНКО[1], Ростислав ТКАЧУК[1,2], Валерія БАЛАЦЬКА[1]
[1] Львівський державний університет безпеки життєдіяльності,
[2]Національний університет «Львівська політехніка»

Проаналізовано систему захищеного віддаленого доступу в «Київстар», виявлено ключові вразливості та загрози. Розглянуто VPN, IPsec, SSL/TLS, Zero Trust, IAM, SIEM і MDM, оцінено ефективність їх впровадження. Наведено дворівневу архітектуру та результати тестування в Ubuntu Server із Wireshark, Nmap і Fail2ban. Запропоновано політику доступу з мінімізацією привілеїв. Дослідження підтверджує ефективність рішення для безпечного віддаленого доступу та підвищення кіберстійкості.

Ключові слова: *захищений віддалений доступ, VPN, Zero Trust, IPsec, SSL/TLS, SIEM, багатофакторна автентифікація, кібербезпека, MDM, корпоративна мережа, WireGuard, тестування безпеки, кіберзагрози.*

The secure remote access system at Kyivstar was analyzed, key vulnerabilities and threats were identified. VPN, IPsec, SSL/TLS, Zero Trust, IAM, SIEM and MDM were considered, and the effectiveness of their implementation was assessed. A two-tier architecture and testing results in Ubuntu Server with Wireshark, Nmap and Fail2ban were presented. An access policy with privilege minimization was proposed. The study confirms the effectiveness of the solution for secure remote access and increasing cyber resilience.

Keywords: *secure remote access, VPN, Zero Trust, IPsec, SSL/TLS, SIEM, multi-factor authentication, cybersecurity, MDM, corporate network, WireGuard, security testing, cyber threats.*

Аналіз системи захищеного віддаленого доступу в «Київстарі» засвідчив наявність низки критичних загроз та вразливостей, пов'язаних із використанням застарілого програмного забезпечення, слабкою сегментацією мережі, недостатнім рівнем захисту кінцевих пристроїв і відсутністю повноцінної багатофакторної автентифікації. Поширені ризики — фішингові атаки, brute-force, MITM, атаки на сесії — становлять особливу загрозу для корпоративного трафіку та персональних даних. Інциденти 2023–2024 років підтверджують необхідність глибокої модернізації інфраструктури безпеки та підвищення стійкості до складних кібератак.

Порівняльний аналіз технологій VPN, IPsec, SSL/TLS, Zero Trust та хмарних інтеграцій показав, що класичні VPN-рішення вже не забезпечують належного рівня захисту в умовах масштабності мережі та значної кількості мобільних пристроїв. Ефективним напрямом є впровадження Zero Trust-архітектури, централізованого управління доступом (IAM), систем моніторингу SIEM, пове-

дінкового аналізу та рішень MDM для контролю мобільних і BYOD-пристроїв. Ці засоби дозволяють мінімізувати ризики компрометації облікових записів та зменшити площу атаки в розподіленій інфраструктурі [1–3].

Для підвищення кіберстійкості великих ресурсів, таких до прикладу, як «Київстар» більш дієве комплексне оновлення системи безпеки: модернізацію протоколів шифрування, запровадження розширеного моніторингу подій, інтеграцію багатофакторної автентифікації, посилення контролю кінцевих точок та використання штучного інтелекту для виявлення аномалій у трафіку. Такий підхід забезпечить надійний захист критичних компонентів, зменшить імовірність несанкціонованого доступу та підвищить рівень готовності до сучасних кіберзагроз [4].

Модель захищеного віддаленого доступу, що використовується оператором «Київстар», ґрунтується на дворівневій архітектурі, яка поєднує шифрування трафіку та централізовану автентифікацію. На першому рівні застосовується захищений тунель, створений за протоколами IPSec або SSL/TLS, що забезпечує конфіденційність і цілісність переданих даних. Другий рівень передбачає автентифікацію користувачів через домен або Active Directory, застосування сертифікатів та контроль доступу відповідно до політик безпеки.

Основними компонентами архітектури є клієнтське програмне забезпечення на робочих станціях, VPN-шлюз, який виконує установлення та підтримку захищених сесій, а також сервер автентифікації, що перевіряє права доступу та керує обліковими записами. Усі події доступу логуються та можуть передаватися до системи моніторингу або SIEM для виявлення підозрілої активності й подальшого аналізу інцидентів.

Рішення забезпечує базовий захист корпоративного трафіку та дозволяє контролювати підключення співробітників до внутрішніх ресурсів із зовнішніх мереж. Водночас ефективність моделі значною мірою залежить від правильної конфігурації, регулярного оновлення компонентів безпеки та інтеграції з сучасними механізмами контролю доступу. Її подальша модернізація може бути спрямована на впровадження принципів Zero Trust, багатофакторної автентифікації та розширених засобів моніторингу для підвищення стійкості до актуальних кіберзагроз.

Для впровадження архітектури захищеного віддаленого доступу в компанії «Київстар» було створено тестове середовище у VirtualBox з установленим Ubuntu Server. Після розгортання ОС проведено налаштування мережі, SSH-доступу та основних сервісів безпеки. Це забезпечило можливість перевірити працездатність рішення до етапу інтеграції у виробниче середовище.

Практичне тестування проводилось за допомогою Wireshark, Nmap і Fail2ban. Wireshark дозволив оцінити затримки та ефективність трафіку, Nmap — перевірити доступність і конфігурацію сервісів, а Fail2ban — протестувати захист від brute-force атак. Тестові показники підтвердили очікувану різницю продуктивності між алгоритмами шифрування: ECDSA за-

безпечив найшвидше встановлення з'єднання, AES — оптимальний баланс між швидкістю і безпекою, RSA — найбільші затримки [5–6].

Fail2ban продемонстрував ефективність автоматичного блокування підозрілих IP-адрес, що значно знижує ризики несанкціонованих підключень. Комплексний аналіз підтвердив, що система витримує типові мережеві загрози та забезпечує стабільний рівень захисту в умовах навантаження.

У межах проєкту також сформовано оновлену політику доступу, яка передбачає мінімальні привілеї, багатофакторну автентифікацію та використання умовних обмежень доступу. Це створює додатковий рівень контролю та зменшує ризики компрометації облікових записів.

Орієнтовна вартість впровадження рішення включає налаштування інфраструктури, навчання персоналу та інтеграцію SIEM-системи. Незважаючи на безкоштовність WireGuard, загальні витрати можуть становити 50 000–100 000 USD, а впровадження SIEM — 100 000–250 000 USD на рік. Проте автоматизація безпеки та зниження кількості інцидентів забезпечують суттєву економію й підвищену стійкість інфраструктури.

Тестування та аналіз підтвердили ефективність запропонованої архітектури: система забезпечує швидке та безпечне віддалене підключення, стійка до brute-force атак і забезпечує необхідний рівень контролю. Рекомендовано подальше впровадження WireGuard, моделі Zero Trust та SIEM-моніторингу в реальному часі для повної інтеграції рішення у корпоративне середовище «Київстар».

Література

1. Балацька В.С., Ткачук Р.Л., Маслова Н.О. Еволюція КСЗІ та інтеграція блокчейн-технологій у кіберзахисті державних інформаційних систем України. Кібербезпека: освіта, наука, техніка. Спеціальний випуск : електронне фахове наукове видання Київ, 2025. № 2 (30). С. 316–332. DOI: https://doi.org/10.28925/2663-4023.2025.30.975

2. VPN (OpenVPN, WireGuard, SSH, RDP): технічні аспекти налаштування та використання.

3. SIEM: Моніторинг подій безпеки. Використання технологій Splunk, IBM QRadar для аналізу загроз.

4. Ivanusa A., Tkachuk R., Brych T., Balatska V., Tkachenko A. Методи та моделі проєктування системи автоматизованого пошуку вразливостей у WEB-додатках. Вісник Львівського державного університету безпеки життєдіяльності : зб. наук. пр. Львів : ЛДУ БЖД, 2024. № 30. С. 110–122. DOI: https://doi.org/10.32447/20784643.30.2024.11

5. Філіпчук Б., Ткачук Р. Л. Порівняльний аналіз захищених каналів, побудованих на протоколах Wireguard та OpenVPN. Інформаційна безпека та інформаційні технології : зб. наукових праць V Міжнародної науково-практичної конференції, ІБІТ 2024. (Львів, 27 листопада 2024 р.). Львів : ЛДУБЖД, 2024. С. 166–170.

6. Wireshark. Network Protocol Analyzer Documentation [Електронний ресурс]. – Режим доступу: https://www.wireshark.org/docs/.

УДК 004.056.5

ШЛЯХИ УДОСКОНАЛЕННЯ ПРОЦЕСУ ОБРОБКИ КІБЕРІНЦИДЕНТІВ ДЛЯ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНОЇ СИСТЕМИ ДСНС

Єгор КАЛЬЧЕНКО, Аркадій СНІГУРОВ
Харківський національний університет радіоелектроніки

В дослідженні пропонується підхід для удосконалення процесу обробки кіберінцидентів для інформаційно-комунікаційної системи ДСНС з урахуванням найкращих практик, представлених в сімействах стандартів ISO/IEC 27000. Пропонується взаємопов'язати процеси оцінювання ризику та обробки інцидентів з урахуванням специфіки інформаційно-комунікаційної системи ДСНС.

Кіберінциденти, ризики, інформаційно-комунікаційна система ДСНС. Cyber incidents, risks. information and communication system of the State Emergency Service of Ukraine.

Відповідно до аналітики інцидентів, опрацьованих Урядовою командою реагування на комп'ютерні надзвичайні події України CERT-UA та SOC Державного центру кіберзахисту Держспецзв'язку за 2024 рік спостерігається зростання загальної кількості кіберінцидентів [1]. Так якщо у 2021 році було зафіксовано 1350, у 2022 році - 2194, у 2023 році - 2543 кіберінцидентів, то у 2024 році зафіксовано вже 4315 кіберінцидентів. Від початку 2025 року CERT-UA фіксує в середньому близько 15 кіберінцидентів на день. Основним джерелом кібератак залишається російська федерація [2]. В цих умовах удосконалення процесу обробки кіберінцидентів для інформаційно-комунікаційної системи (ІКС) Державної служби України з надзвичайних ситуацій (ДСНС) з урахуванням світового досвіду є актуальним завданням.

Світові підходи розглядають процес обробки кіберінцидентів як один із процесів системи управління інформаційною безпекою (СУІБ). Слід зазначити, що при побудові СУІБ для структурних підрозділів ДСНС, потрібно враховувати не тільки кіберінциденти, а й інші інциденти інформаційної безпеки (ІБ), такі як витік інформації по акустичним каналам, компрометуючим випромінюванням цифрової техніки, реалізація загроз через механізми соціальної інженерії, технічні та природні загрози критичним активам і процесам тощо.

На даний момент існує ряд міжнародних стандартів, які регламентуються вимоги та практичні підходи до побудови СУІБ організацій та установ, складних інформаційних систем. Одними з найкращих практик, на наш погляд, є стандарти сімейства ISO/IEC 27000 (зокрема, 27001:2022, 27005:2022, 27035-1:2023). Стандарт ISO/IEC27001:2022 впроваджує вимоги до СУІБ, при яких пропонується комплексний підхід до забезпечення ІБ у вигляді сукупності взаємопов'язаних процесів, стандарт ISO/IEC27005:2022 запроваджує механізм реалізації менеджменту ризиків

ІБ, стандарт ISO/IEC27035-1:2023 запроваджує стандартизований процес реагування на інциденти ІБ.

В дослідженні з урахуванням підходів цих стандартів пропонується використання теорії ризиків ІБ для визначення потенційних ризиків для ІКС ДСНС, обрання на підставі цього процесу захисних заходів, пріоритезація ризиків та організація процесу обробки кіберінцидентів, як одного з механізмів оцінювання якості прогнозу. Такий підхід дозволяє підійти до класифікації та пріоритезації кіберінцидентів, притаманних ІКС ДСНС, обрати організаційні заходи та технічні засоби виявлення кіберінцидентів. В дослідженні за основу для оцінювання ризиків ІБ взята методика CRAMM, яка доробляється з урахуванням специфіки ІКС ДСНС в напрямку класифікації критичних активів та визначення вразливостей.

Література

1. Російські кібероперації. Аналітика за II півріччя 2024 року. Державна служба спеціального зв'язку та захисту інформації України. 2025. – 23 с. URL: https://docs.google.com/viewer?url=https://cip.gov.ua/services/cm/api/attachment/download?id=68769&embedded=true&a=bi (дата звернення: 20.10.2025).

2. Огляд кіберзагроз та стратегій захисту в 2025 році: досвід CERT-UA. Державна служба спеціального зв'язку та захисту інформації України. 2025. URL: https://cip.gov.ua/ua/news/cyber-threat-overview-and-defense-strategies-in-2025-cert-ua-s-experience (дата звернення: 10.10.2025).

УДК 004.8:004.056.5:004.9

ГІБРИДНА АНТИВІРУСНА СИСТЕМА З МОДУЛЬНОЮ АРХІТЕКТУРОЮ ДЛЯ СУЧАСНИХ КОМП'ЮТЕРИЗОВАНИХ СЕРЕДОВИЩ

Даниїл КАШУБА[1] Ростислав ТКАЧУК[1,2], Орест ПОЛОТАЙ [1,2]
[1]Львівський державний університет безпеки життєдіяльності
[2]Національний університет «Львівська політехніка»

У роботі розглянуто сучасні підходи до забезпечення інформаційної безпеки комп'ютеризованих систем та обґрунтовано доцільність створення гібридної антивірусної системи з модульною архітектурою. Проаналізовано ефективність сигнатурного, евристичного та поведінкового аналізу, а також застосування математичних моделей для детекції шкідливого програмного забезпечення. Розроблено антивірусне ПЗ із високопродуктивним ядром на C++ та графічним інтерфейсом на C# / WPF, що забезпечує багаторівневий захист, модульність, масштабованість та можливість інтеграції з іншими застосунками. Описано технічну реалізацію, включно з використанням SQLite, OpenSSL та механізмів багатопоточності, а також експортовані функції ядра для інтеграції та розширення системи.

Ключові слова: *інформаційна безпека, антивірусна система, гібридний аналіз, сигнатурний аналіз, поведінковий аналіз, модульна архітектура, C++, C# / WPF, шкідливе ПЗ, Zero-Day загрози, SQLite, OpenSSL.*

The paper considers modern approaches to ensuring information security of computerized systems and justifies the feasibility of creating a hybrid antivirus system with a modular architecture. The effectiveness of signature, heuristic and behavioral analysis, as well as the use of mathematical models for detecting malicious software, is analyzed. Antivirus software with a high-performance C++ kernel and a C# / WPF graphical interface is developed, which provides multi-level protection, modularity, scalability and the ability to integrate with other applications. The technical implementation is described, including the use of SQLite, OpenSSL and multi-threading mechanisms, as well as exported kernel functions for system integration and expansion.

Keywords: *information security, antivirus system, hybrid analysis, signature analysis, behavioral analysis, modular architecture, C++, C# / WPF, malware, Zero-Day threats, SQLite, OpenSSL.*

Інформаційна безпека є критичним фактором стабільного функціонування сучасних комп'ютеризованих систем. Щодня фіксуються тисячі нових шкідливих програм, здатних викрадати дані, порушувати роботу операційних систем або атакувати інфраструктуру. Традиційні сигнатурні антивіруси часто виявляються неефективними проти нових та модифікованих загроз. Практичним прикладом є атака вірусу-вимагача у 2023 році, що уразила понад 50 000 робочих станцій у підприємствах Європи, незважаючи на наявність стандартних антивірусних програм [1].

Сучасні дослідження підкреслюють важливість гібридних рішень, що поєднують сигнатурний та поведінковий аналіз. Такий підхід дозволяє

не лише перевіряти хеші файлів, а й виявляти аномальні процеси в режимі реального часу, підвищуючи ефективність захисту. Розробка власного антивірусного ядра з прозорою архітектурою сприяє глибшому розумінню принципів роботи захисного ПЗ, що важливо як у наукових, так і в освітніх проєктах [2].

Аналіз сучасних антивірусних рішень показав, що комерційні системи забезпечують високу точність і багаторівневий захист, проте є закритими, ресурсомісткими та малопридатними для кастомізації. Відкриті рішення, такі як ClamAV, забезпечують гнучкість та інтегровуваність, але потребують доопрацювання для реалізації сучасних функцій, зокрема поведінкового аналізу. Порівняння методів детекції виявило, що сигнатурний підхід ефективний для відомих загроз, евристичні методи здатні виявляти нові загрози, проте характеризуються високим рівнем хибнопозитивів, а поведінковий аналіз є найбільш перспективним для виявлення Zero-Day загроз, хоча потребує значних обчислювальних ресурсів. Математичні моделі — автоматні, статистичні, логічні та ML-моделі — демонструють ефективність лише при комплексному застосуванні [3].

Створення антивірусного ПЗ вимагає поєднання високопродуктивного системного ядра та зручного користувацького інтерфейсу, при цьому компоненти мають бути модульними, безпечними, масштабованими та придатними до подальшого розвитку [2]. Основна проблема полягає у виборі таких засобів розробки й архітектури, які одночасно забезпечать:

– доступ до низькорівневих функцій ОС для поведінкового та сигнатурного аналізу;

– високу швидкодію та оптимізацію;

– безпечний та сучасний графічний інтерфейс;

– легкість оновлення, розширення та інтеграції;

– відповідність вимогам реальних середовищ Windows.

Враховуючи ці обмеження, доцільним є створення гібридної антивірусної системи з модульною архітектурою, що поєднує сигнатурний та поведінковий аналіз з можливістю подальшого розширення евристичними та ML-методами. Такий підхід забезпечує оптимальний баланс між точністю, швидкодією, масштабованістю та адаптивністю до нових загроз [4, 5].

Для реалізації високопродуктивного ядра обрано мову C++ з доступом до низькорівневих механізмів Windows та підтримкою багатопоточності. Графічний інтерфейс створено на C# / WPF, що забезпечує інтеграцію з .NET, сучасну UI-архітектуру та легкість підтримки. Система побудована за трирівневою архітектурою (ядро — інтеграційний рівень — інтерфейс), що гарантує модульність, масштабованість і незалежність компонентів. Використані інструменти (Visual Studio 2022, MSVC, NuGet) та бібліотеки (SQLite, OpenSSL, WinAPI, WPF) забезпечують безпечну, продуктивну та керовану розробку, а апаратні вимоги відповідають типовому обладнанню Windows [6, 7].

Антивірусне ПЗ реалізовано на основі багаторівневої модульної архітектури, що розмежовує функції аналізу загроз, керування даними та

взаємодії з користувачем. Основу системи становить високопродуктивне ядро як динамічна бібліотека C++, що виконує сигнатурний та поведінковий аналіз, працює з локальною базою сигнатур і формує результати перевірки. Інтеграція з .NET-клієнтом здійснюється через C++/CLI або P/Invoke, поєднуючи native-продуктивність з керованою логікою та WPF-інтерфейсом.

Інтерфейс користувача реалізовано за шаблоном MVVM, що забезпечує ізоляцію бізнес-логіки та уніфіковане оновлення даних. Кожен функціональний компонент оформлений як окремий модуль із власною ViewModel, а стилі та ресурси структуруються у словниках для єдності дизайну. Сигнатурна база на SQLite завантажується в оперативну пам'ять для забезпечення O(1) перевірки хешів, а сигнатурний аналіз здійснюється за алгоритмами SHA-256 та MD5 (OpenSSL). Поведінковий модуль моніторить процеси та порівнює їх зі списком ризикових шаблонів, а фонове виконання й атомарні структури гарантують коректність багатопотокових операцій.

Ядро надає експортовані функції (ScanDirectory, IsFileMalicious) для інтеграції в інші застосунки та автоматичної інсталяції через NuGet-пакет, що забезпечує масштабованість, розширюваність і можливість подальшої інтеграції з хмарними сервісами аналізу шкідливих файлів.

Література

1. CISA. Cyberattack Against MGM Resorts [Електронний ресурс] // U.S. Cybersecurity and Infrastructure Security Agency (CISA), 2023. — Режим доступу: https://www.cisa.gov/news-events/alerts/aa23-239a

2. Філіпчук Б., Ткачук Р. Л. Захист персонального комп'ютера від шкідливого програмного забезпечення. Актуальні проблеми пожежної безпеки та запобігання надзвичайним ситуаціям в умовах сьогодення : зб. тез доповідей Всеукраїнської науково-практичної конференції з міжнародною участю (Львів, 25 жовтня 2022 р.). Львів : ЛДУБЖД, 2022. С. 478–481.

3. Боднар О., Ткачук Р. Л. Тактика моделей cyber kill chain і unified kill chain: розкриття анатомії кібератак. Інформаційна безпека та інформаційні технології : зб. тез доповідей VI Всеукраїнської науково-практичної конференції молодих учених, студентів і курсантів. Львів : ЛДУБЖД, 2023. С. 22–27.

4. GitHub. SharpCompress – Modern compression library for .NET. URL: https://github.com/adamhathcock/sharpcompress

5. Ткачук Р. Л., Полотай О. І., Балацька В. С., Брич Т. Б., Кухарська Н. П. Моделювання захисту операційних систем від реалізації кібератак з використанням критерію Пірсона. Вісник Львівського державного університету безпеки життєдіяльності : зб. наук. пр. Львів : ЛДУ БЖД, 2025. № 31. С. 117–125. DOI: https://doi.org/10.32447/20784643.31.2025.12

6. AV-Test Institute. Test Results – Antivirus Software for Windows (April 2024). URL: https://www.av-test.org/en/antivirus/home-windows/

7. SQLite. SQLite. URL: https://www.sqlite.org/docs.html – Дата звернення: 10.06.2025.

УДК 004.9:355.45

РОЛЬ МЕДІАГРАМОТНОСТІ В БОРОТЬБІ З ІНФОРМАЦІЙНИМИ ВІЙНАМИ

Олександр КИДИСЮК, Юрій КЛИМЮК, Діана РАЙТА
Львівський державний університет безпеки життєдіяльності

У роботі розглядається явище інформаційних війн як інструменту впливу на свідомість людей. Проаналізовано основні методи — фейки, дезінформацію, пропаганду та кіберзломи. Показано досвід України у протидії інформаційній агресії та важливість розвитку медіаграмотності й критичного мислення для захисту суспільства від маніпуляцій.

Ключові слова: *інформаційна війна, дезінформація, фейки, пропаганда, медіаграмотність, критичне мислення, кібербезпека, гібридна війна, інформаційна безпека, свідомість суспільства, маніпуляція, інформаційний простір, Україна.*

The work examines the phenomenon of information war as a tool for influencing people's consciousness. It analyzes the main methods — fake news, disinformation, propaganda, and cyberattacks. The experience of Ukraine in countering information assault is shown, highlighting the importance of developing media literacy and critical thinking to protect society from manipulation.

Keywords: *information war disinformation, fake news, propaganda, media literacy, critical thinking, cybersecurity, hybrid war, information security, public consciousness, manipulation, information space, Ukraine.*

У сучасному світі інформація перетворилася на стратегічний ресурс, який має не менше значення, ніж природні або військові ресурси. Вона здатна формувати суспільну думку, впливати на політичні процеси, створювати або руйнувати імідж держави. У зв'язку з цим дедалі частіше говорять про явище інформаційних війн — боротьбу за свідомість людей, у якій зброєю стають не танки й ракети, а слова, зображення, новини та маніпуляції. Інформаційні війни — це невід'ємна частина сучасних гібридних конфліктів, у яких інформаційний простір використовується для досягнення політичних, економічних і військових цілей. В умовах глобалізації та розвитку цифрових технологій вони набули небаченого масштабу й стали реальністю для кожної країни світу.

Інформаційна війна — це складний і багатогранний феномен, що охоплює систематичне використання різноманітних інформаційних інструментів для впливу на свідомість противника. Її основна мета полягає не в безпосередньому знищенні чи захопленні територій, а в зміні психологічного стану населення, формуванні сумніву, страху та ворожнечі, а також у поширенні недовіри до державних інституцій, армії, союзників і національних цінностей. Такий підхід робить інформаційну війну максимально

підступною, бо вона діє на рівні свідомості, свободи мислення та громадянської єдності. Для досягнення своїх цілей учасники інформаційних воєн використовують різні методи, серед яких — створення і поширення фейкових новин, цілеспрямована дезінформація та пропаганда, вплив через соціальні мережі, кібератаки на критично важливі інформаційні системи, психологічні операції, що мають розколоти суспільство чи позбавити його довіри до себе. Завдяки інтернету та цифровим технологіям ці методи поширення інформації стали надзвичайно швидкими, масштабними і часто непомітними для звичайного користувача, що значно ускладнює виявлення і протидію їм.

Навіть у періоди миру інформаційні війни не припиняються — держава, що володіє потужними медіа-ресурсами, може формувати вигідний для неї інформаційний простір, впливати на внутрішню та зовнішню політику, зміцнювати свій авторитет на міжнародній арені. Водночас країни, які потерпають від інформаційних атак, стикаються з серйозними наслідками: втратою довіри суспільства, політичною нестабільністю, розколом громадян та зниженням ефективності державних органів. Такі процеси погіршують безпекову ситуацію і відкривають шлях для подальших агресивних дій. Яскравим прикладом жорстокої інформаційної війни є ситуація в Україні з 2014 року. В цей період росія активізувала масштабну інформаційну кампанію, намагаючись дискредитувати нашу державу як всередині країни, так і на міжнародній арені. Через численні фейки, викривлення історичних фактів, маніпуляції в медіа та соціальних мережах, а також кібератаки було створено негативний образ України, спрямований на посіяти розбрат у суспільстві та послабити державні інститути. Ці дії спричинили значний тиск на українську інформаційну сферу і стали однією із складових гібридної війни.

Для протидії таким викликам Україна активно розвиває широкомасштабну систему інформаційної безпеки, яка включає заходи кіберзахисту, створення надійних медіа-ресурсів і підвищення рівня медіаграмотності населення. Особливу роль відіграють незалежні журналісти, які дотримуються фактчекінгових стандартів і сприяють відкритості інформації, а також волонтерські ініціативи, що допомагають виявляти й спростовувати безпідставні твердження і фейки. Не менш важливим елементом є освітні програми, які навчають громадян критично сприймати інформацію, розпізнавати маніпуляції і не піддаватись пропаганді. Таким чином, інформаційна війна — це складний процес, що вимагає комплексного підходу для своєї подолання. Перемога в ній залежить від здатності суспільства бути свідомим, критично мислячим і активним у захисті власної інформаційної безпеки. Водночас роль держави, медіа і освітніх інституцій є вирішальною для створення надійного щита проти інформаційних атак і формування стійкого національного інформаційного поля.

Інформаційні війни стали невід'ємним і надзвичайно серйозним викликом сучасного світу. Вони мають потенціал завдавати руйнівних наслідків, які не поступаються масштабами та впливом навіть збройним конфліктам, оскільки основною їхньою зброєю є свідомість людини — найцінніший ресурс будь-якого суспільства. Умови сьогодення вимагають від держав, медіа, освітніх установ і кожного громадянина об'єднати зусилля для ефективної протидії цим загрозам. Успіх у боротьбі з інформаційними атаками можливий лише за умови тісної й скоординованої співпраці між усіма ланками суспільства. Держава має створювати та впроваджувати дієві національні інформаційні стратегії, які захищатимуть інформаційний простір від зовнішніх і внутрішніх маніпуляцій. Медійні структури повинні дотримуватися високих стандартів об'єктивності та прозорості, а освітні заклади – активно впроваджувати програми з розвитку навичок критичного мислення та медіаграмотності. Особливо важливо формувати у громадян усвідомлення власної відповідальності за поширення інформації, розуміння механізмів маніпуляцій і фейкових новин. Адже ключ до перемоги в інформаційній війні — це освічене, свідоме й критично налаштоване суспільство, яке не піддається впливу пропаганди й викривленого наративу. Підвищення рівня медіаграмотності, громадська активність і підтримка національної інформаційної політики створять міцний фундамент для захисту національної безпеки та стабільності.

Література

1. Сопілко І.М. Соціально-правові основи інформаційної безпеки держави, суспільства та особи в Україні // Юридична наука. – 2023. – № 4. – С. 18–25.

2. Зачко О.Б., Головатий Р.Р. Мультиагентна модель управління безпекою при плануванні проектів створення об'єктів з масовим перебуванням людей // Вісник НТУ «ХПІ». Серія: Стратегічне управління, управління портфелями, програмами та проектами. – Х.: НТУ «ХПІ», 2017. – № 2 (1224) – С. 46-51.

3. Лисенко С. Information wars as a threat to the information security of Ukraine // Scientific Notes of Institute of Journalism. – 2021. – № 1. – С. 33–40.

4. Антіпова О.В. Strategic communications as a component of state information security policy // Law Journal of the NAIA. – 2023. – Т. 13, № 1. – С. 44–52.

УДК: 004.056.55:519.6

ЕКСПЕРИМЕНТАЛЬНИЙ АНАЛІЗ ПЕРІОДИЧНОСТІ ГЕНЕРАТОРА LCG

Тарас КІС, Наталія МАСЛОВА, Андрій ЛАГУН
Львівський державний університет безпеки життєдіяльності

У роботі проведено експериментальне дослідження залежності довжини періоду псевдовипадкових послідовностей, що формуються лінійним конгруентним генератором (LCG), від взаємного розташування його параметрів: множника a, *зсуву* c, *модуля* m *та початкового значення* X_0.

Ключові слова: *лінійний конгруентний генератор, період, параметри. теорема Халла–Добелла*

An experimental study was conducted to investigate how the period length of pseudorandom sequences generated by a *linear congruential generator (LCG) depends on the configuration of its parameters: multiplier* a, *increment* c, *modulus* m, *and initial value* X_0.

Keywords*: linear congruential generator, period, parameters, Hull–Dobell theorem.*

Псевдовипадкова генерація чисел є основою сучасних криптографічних систем, статистичного моделювання та симуляційних процесів. Забезпечення достатньої довжини періоду та рівномірності розподілу послідовностей безпосередньо впливає на якість отриманих результатів і стійкість алгоритмів, що їх використовують.

Метою дослідження є встановлення закономірностей формування повного або часткового періоду лінійного конгруентного генератора залежно від співвідношення параметрів, перевірка виконання умов теореми Халла–Добелла.

Актуальність. Надійність псевдовипадкових чисел залишається ключовою складовою криптографічного захисту, моделювання стохастичних процесів, машинного навчання та комп'ютерної симуляції. Лінійний конгруентний генератор (LCG) залишається одним із найпоширеніших інструментів у цих сферах завдяки простоті реалізації, високій швидкодії та низьким обчислювальним витратам. Водночас помилки під час вибору параметрів LCG можуть призвести до суттєвого скорочення довжини періоду та формування статистично передбачуваних підциклів, що критично впливає на безпеку та достовірність моделювання.

Методика дослідження. Для наборів параметрів обчислювався період шляхом покрокової генерації до повторення $\mathbf{X_0}$. Реалізовано частотний і серійний тести для оцінки рівномірності та структури отриманих послідовностей.

Математична модель лінійного конгруентного генератора:

$$X_{n+1}=(\mathbf{a}\, X_n+c) \bmod m$$

Залежність довжини періоду LCG від параметра a при Заданому X_0 та фіксованих c=13 та m=12 відображена рисунку 1.

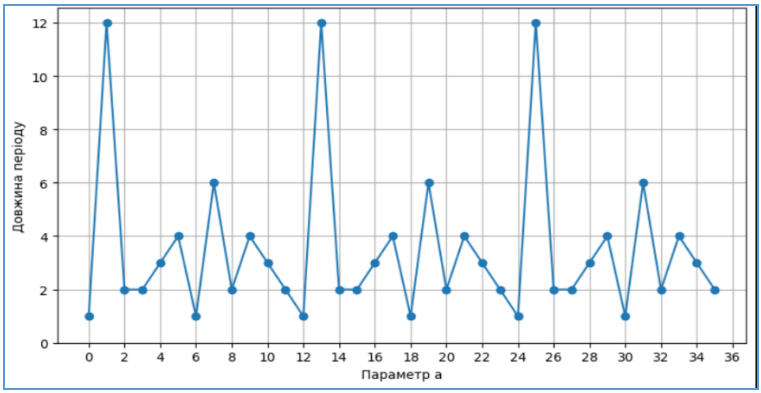

Рисунок 1 – Залежність довжини періоду LCG від параметра a при c=13, m=12, X_0=199

Рисунок демонструє повторюваність періоду LCG й те, його поведінка залежить від значення $a \bmod m$. Тож повні періоди виникають, коли $a-1$ кратне m. Так, для m=12 → a=1,13,25,37. Інші значення дають короткі цикли (2, 3, 4, 6), що призводить до нерівномірного розподілу, зниження випадковості й непридатності LCG для криптографії.

Таким чином, параметр a — головний чинник періодичності LCG при фіксованих c і m.

Проведемо ще серію експериментів, в яких значення параметрів X_0, a, c,та m обирались випадковим чином й дослідим зміни періоду при різних значеннях вказаних параметрів (Таблиця 1).

Таблиця 1 – Експериментальні результати генератора LCG

№	X_0	a	c	Тип й значення m	Умова Халла–Добелла	Виконання	Період ::Характеристика послідовності
1	217	31	17	Простий, m=13	(a-1)=30 не кратне 13	Ні	p=4 :: короткий цикл, нерівномірність
2	311	13	19	Простий, m=11	gcd(c,m)=1	Так	p=11 :: повний період, рівномірний розподіл
3	131	29	21	Простий, m=17	(a-1)=28 не кратне 17	Ні	p=8 :: частковий період
4	253	21	7	Парний, m=10	gcd(7,10)=1	Так	p=10 :: повний, лінійна гістограма
5	167	43	29	Ступінь 2, m=16	(a-1)=42 не кратне 4	Ні	p=8 :: рівномірний підцикл, період половинний
6	199	20	7	Парний, m=12	gcd(7,12)=1, але (a-1)не кратне 3	Ні	p=2 :: короткий, чергування 2 значень

7	199	25	7	Парний, m=12	(a-1)=24 кратне 3 і 4	Так	p=12 :: повний період, рівномірність підтверджено
8	274	22	53	Складений, (3^2), m=9	gcd(8,9)=1	Так	p=9 :: повний цикл, рівномірний розподіл
9	307	29	49	Парний, m=14	gcd(7,14)=7	Ні	p=2 :: короткий період, парні цикли
10	307	29	29	Парний, m=14	gcd(1,14)=1	Так	p=14 :: повний період
11	157	18	3	Складений, m=15	gcd(3,15)=3	Ні	p=4 :: неповний цикл, зсув серій
12	157	6	3	Складений, m=15	a змінене: (a-1=5)	Не повністю	p=5 :: цикл довжиною 5

Результати. Експериментально підтверджено, що:

– повний період досягається лише за виконання всіх умов теореми Халла–Добелла, а саме: gcd (c,m)=1, кратності ($a-1$) усім простим дільникам **m**, та кратності 4, якщо **m** ділиться на 4;

– порушення хоча б однієї умови призводить до скорочення періоду в 2–5 разів;

– для модулів, кратних степеню двійки, порушення кратності a−1 до 4 одразу зменшує період удвічі;

– парні модулі зберігають лінійний характер гістограми, але можуть утворювати короткі повтори, якщо gcd(c,m)≠1;

– заміна одного параметра (наприклад, a) може радикально змінити довжину циклу, що показано в експерименті №12.

Висновки. Експериментальні результати показали, що довжина періоду лінійного конгруентного генератора повністю залежить від добору параметрів a, c та m. Повний період виникає лише за виконання всіх умов теореми Халла–Добелла. Найсуттєвіший вплив має множник a, зміна якого навіть за сталих c і m здатна перетворити рівномірну послідовність на короткий повторюваний підцикл. Отже, коректний вибір параметрів є критичним для забезпечення повного періоду й рівномірності генерації псевдовипадкових чисел.

Література

1. Q. Sun, Z. Liu, H. Wang. An Online Evaluation Method for Random Number Entropy and Pseudo-Random Number Generators. *Entropy*. 2025. Vol. 27, № 2, 136. URL: https://www.mdpi.com/1099-4300/27/2/136. MDPI

2. E. Faure, E. Fedorov, I. Myronets, S. Sysoienko. Method for Generating Pseudorandom Sequence of Permutations Based on Linear Congruential Generator. *CEUR Workshop Proceedings*. 2022, Vol. 3137, pp. 15-24. URL: https://ceur-ws.org/Vol-3137/paper15.pdf.

УДК 004.056.2:004.421.5

ВЕРИФІКАЦІЯ ОПТИМАЛЬНИХ СТЕПЕНІВ ХАРАКТЕРИСТИЧНИХ ПОЛІНОМІВ МОДИФІКОВАНОГО ГЕНЕРАТОРА ДЖИФФІ ЗА ДОПОМОГОЮ ТЕСТІВ NIST

Михайло КІХ, Олена НЄМКОВА
Національний університет "Львівська Політехніка"

Проведено емпіричну верифікацію оптимальних параметрів поліномів для модифікованого генератора Джиффі. Досліджено п'ять конфігурацій із найвищими степенями від 23 до 71 за допомогою пакету NIST SP 800-22. Встановлено, що конфігурація (59, 53, 47) забезпечує найкращий баланс між статистичною безпекою та обчислювальною ефективністю, успішно проходячи всі 188 тестів.
Ключові слова: *генератор Джиффі, LFSR, псевдовипадкова послідовність, характеристичний поліном, NIST SP 800-22, кібербезпека.*

An empirical verification of the optimal polynomial parameters for the modified Jiffy generator was carried out. Five configurations with the highest degrees from 23 to 71 were investigated using the NIST SP 800-22 package. It was found that the configuration (59, 53, 47) provides the best balance between statistical safety and computational efficiency, successfully passing all 188 tests.
Keywords: *Geffe generator, LFSR, pseudorandom sequence, characteristic polynomial, NIST SP 800-22, cybersecurity.*

Модифікована структура генератора Джиффі зберігає базовий принцип класичного Geffe-генератора — використання трьох незалежних лінійних регістрів зсуву зворотного зв'язку (LFSR), сигнали яких об'єднуються за допомогою нелінійної комбінуючої функції [1, 2].

У запропонованій схемі вдосконалено структуру вихідної функції, яка формує фінальний біт послідовності як нелінійну комбінацію старших бітів регістрів [3]. Для цього використано спрощену, але більш збалансовану булеву функцію виду:

$$f(x, y, z) = z \oplus (x \cdot y), \tag{1}$$

де x, y, z — вихідні біти трьох регістрів.

Метою дослідження є емпірична верифікація оптимальності обраних степенів характеристичних поліномів для регістрів X, Y, Z модифікованого генератора Джиффі через порівняння альтернативних конфігурацій за допомогою пакету тестів NIST SP 800-22 [2].

Для аналізу було обрано прості числа як найвищі степені поліномів у діапазоні від 23 до 71. Кількість tap-позицій зафіксована на рівні 5-ти для кожного регістра, що відповідає базовій архітектурі [2]. Характеристичні поліноми підбиралися з урахуванням примітивності для забезпечення мак-

симального періоду (таблиця 1) [1, 2]. Тестування виконувалося за допомогою пакету NIST SP 800-22 (188 тестів) на псевдовипадкових послідовностях (ПВП) довжиною 100 000 000 біт для кожного варіанту [3]. Результати тестування представлені у таблицях 2 і 3.

Таблиця 1 – Параметри досліджуваних конфігурацій генератора Джиффі

№	Назва	Регістр X	Регістр Y	Регістр Z	Довжина	Період
1	Варіант 1	[0, 13, 17, 19, 23]	[0, 11, 13, 17, 19]	[0, 7, 11 , 13, 17]	59 біт	$\sim 2^{59}$
2	Варіант 2	[0, 17, 23, 31, 37]	[0, 13, 19, 23, 29]	[0, 11, 17, 19, 23]	89 біт	$\sim 2^{89}$
3	Варіант 3	[0, 19, 31, 41, 47]	[0, 19, 29, 37, 43]	[0, 13, 23, 31, 37]	127 біт	$\sim 2^{127}$
4	Варіант 4	[0, 19, 31, 43, 59]	[0, 17, 29, 41, 53]	[0, 13, 23, 37, 47]	159 біт	$\sim 2^{159}$
5	Варіант 5	[0, 29, 47, 61, 71]	[0, 31, 43, 59, 67]	[0, 23, 37, 47, 59]	197 біт	$\sim 2^{197}$

Таблиця 2 – Результати статистичного тестування NIST

№	Статистичний тест	Варіант 1	Варіант 2	Варіант 3	Варіант 4	Варіант 5
1	Frequency	0.000000	0.045675	0.924076	0.334538	0.350485
2	Block Frequency	0.000000	0.574903	0.437274	0.534146	0.401199
3	Cumulative Sums (forward)	0.000000	0.005762	0.816537	0.616305	0.637119
	Cumulative Sums (backward)	0.000000	0.042808	0.955835	0.028817	0.637119
4	Runs	0.000000	0.026948	0.595549	0.224821	0.759756
5	Longest Run	0.000000	0.474986	0.275709	0.798139	0.474986
6	Rank	0.108791	0.637119	0.350485	0.474986	0.236810
7	FFT	0.000000	0.000000	0.213309	0.514124	0.971699
8	NonOverlapping Template	Множинні відмови	Переважно	Всі	Всі	Всі
	(середнє p-value)	~0.15	~0.45	~0.55	~0.52	~0.48
	(кількість відмов)	98/148	0/148	1/148	0/148	0/148
9	Overlapping Template	0.000000	0.779188	0.025193	0.494392	0.911413
10	Universal	0.000000	0.971699	0.897763	0.137282	0.595549
11	Approximate Entropy	0.000000	0.275709	0.719747	0.162606	0.574903
12	Random Excursions (8 тестів)	Множинні відмови	Всі	1 відмова	Всі	Всі
	(середнє p-value)	—	~0.58	~0.45	~0.35	~0.28
13	Random Excursions Variant (18 тестів)	Множинні відмови	Всі	2 відмови	Всі	1 відмова
	(середнє p-value)	—	~0.42	~0.35	~0.32	~0.30
14	Serial (2 тести)	0.000000	0.678686	0.236810	0.066882	0.058984
		0.000000	0.350485	0.455937	0.534146	0.897763
15	Linear Complexity	0.494392	0.002043	0.455937	0.437274	0.085587

Таблиця 3 – Підсумкова статистика

Показник	Варіант 1	Варіант 2	Варіант 3	Варіант 4	Варіант 5
Загальна кількість тестів	188	188	188	188	188
Пройдено тестів	18	175	185	188	187
Не пройдено тестів	170	13	3	0	1
% успішності	9.6%	93.1%	98.4%	100%	99.5%
Критичні відмови	Так	Так (FFT)	Ні	Ні	Ні
Придатність для криптографії	Ні	Обмежено	Так	Так	Так

Варіант 1 не відповідає криптографічним вимогам: більшість тестів NIST не пройдено, спостерігається низька ентропія та висока передбачуваність ПВП. Варіант 2 показав покращення, але залишився обмежено придатним через критичну відмову в тесті FFT, що свідчить про залишкову періодичність. Варіант 3 вперше забезпечив повне проходження NIST-тестів, високу ентропію та збалансовану лінійну складність, що робить його придатним для криптографічного використання. Варіант 4 виявився найстабільнішим: усі тести пройдено успішно, показники ентропії та автокореляції близькі до ідеальних. Це оптимальний варіант за співвідношенням “якість – ресурсомісткість”. Варіант 5 має результати, подібні до варіанта 4, проте не дає помітного підвищення безпеки при дещо більших обчислювальних витратах.

Отже, оптимальною конфігурацією є варіант 4 (59, 53, 47), який забезпечує найкращий баланс між статистичною безпекою та ефективністю реалізації генерування ПВП для систем кібербезпеки.

Література

1. Максимович В.М., Шевчук М.С., Мандрона М.М. Дослідження ГПВБП на основі генератора Джиффі. Інформаційна Безпека: науковий журнал Східноєвропейського Національного університету ім. В. Даля. – 2017. – №3(23) №4(24). – С. 130-135.

2. Шевчук М. С., Максимович В. М., Мандрона М. М. Дослідження генератора псевдовипадкових бітових послідовностей Джиффі на основі FCSR. Міжнародний науковий журнал “Інтернаука”;. – 2018. – №19.

3. Kikh M., Nyemkova E. Практична схема гібридного генератора псевдовипадкових послідовностей на основі аудіоентропії та нелінійних булевих функцій // Кібербезпека: освіта, наука, техніка. – 2025. – № 2 (30). – С. 180–194.

УДК 004.056

ЗАГРОЗИ І БАЗОВІ ПОНЯТТЯ В ОЦІНЦІ РИЗИКІВ ІБ ПІДПРИЄМСТВА

Тетяна КОРОБЕЙНІКОВА, Марта КІЩАК
Національний університет "Львівська Політехніка"

Робота присвячена оцінці загроз інформаційній безпеці підприємства, класифікації активів, загроз та вразливостей. Розглянуто технічні, організаційні та людські фактори ризику, а також вплив ланцюгів постачання й хмарних сервісів. Запропоновано практичні заходи захисту та підходи до ефективного ризик-менеджменту.

Ключові слова: *інформаційна безпека, вразливості, людський фактор, ланцюги постачання, захист даних.*

Інформаційна безпека підприємства є критично важливою складовою стабільної діяльності, оскільки будь-які загрози можуть вплинути на безперервність бізнес-процесів, конфіденційність даних та цілісність інформаційних ресурсів. Для коректної оцінки ризиків необхідним є формування чіткого понятійного апарату, що включає активи, загрози, вразливості, події, інциденти та ризики. Активами виступають не лише технічні засоби, а й дані, ПЗ, персонал і операційні процеси, які забезпечують діяльність підприємства. Загрози визначають потенційні чинники, що можуть завдати шкоди активам, тоді як вразливості відображають слабкі місця системи, через які ці загрози можуть реалізуватися. Події та інциденти демонструють фактичну реалізацію загроз, а ризики характеризують імовірність та масштаб можливих збитків [1]. Класифікація загроз є ключовим елементом процесу управління ризиками, оскільки дозволяє визначити найбільш критичні напрями захисту. Технічні загрози охоплюють атаки на мережеву інфраструктуру, програмне забезпечення та апаратні засоби, включно зі шкідливим ПЗ, несанкціонованим доступом і порушенням функціонування серверів. Організаційні загрози виникають через недоліки політик, процесів та управлінських процедур, а людський фактор проявляється у помилках, неуважності або навмисних діях персоналу. В умовах сучасної цифрової трансформації важливим джерелом ризиків стають також ланцюги постачання та використання хмарних сервісів, де частина відповідальності за безпеку лежить на зовнішніх провайдерах [2].

У практичній діяльності підприємства розуміння базових понять і структуризація загроз дозволяють будувати реалістичні сценарії ризиків та впроваджувати конкретні заходи захисту. Наприклад, класифікація технічних загроз дає змогу обґрунтувати необхідність розгортання

міжмережевих екранів, систем виявлення та запобігання вторгненням, сегментації мереж та багатофакторної аутентифікації. Аналіз людського фактору допомагає формувати програми безпекового навчання, політики управління паролями та заходи із запобігання фішингу. Ідентифікація ризиків у ланцюгах постачання дозволяє підприємству встановлювати вимоги до контрагентів, проводити безпекові аудити та підвищувати рівень контролю при передачі даних і використанні зовнішніх сервісів. Таким чином, чітка класифікація загроз у поєднанні з коректним визначенням базових понять інформаційної безпеки є основою ефективного ризик-менеджменту. Це не лише підсилює теоретичну складову, але й забезпечує можливість практичного впровадження системи захисту, орієнтованої на реальні загрози, специфіку бізнес-процесів та сучасні моделі атак. Завдяки цьому підприємство отримує стійку та адаптивну систему ІБ, здатну мінімізувати потенційні збитки та підвищувати рівень кіберстійкості в умовах зростання кіберзагроз [3-4].

Література

1. Stoneburner, G., Goguen, A., & Feringa, A. (2002). Risk Management Guide for Information Technology Systems (NIST SP 800-30).

2. Peltier, T. R. Information Security Risk Analysis. CRC Press, 2016

3. Коробейнікова Т. І. Вимоги до захисту мережевої інфраструктури компанії / Т. І. Коробейнікова, М.М. Кіщак, Н.М. Лужецька // «Global science and education in the modern realities 2024» : Міжнародна наукова конференція, 21 травня 2024 р. : тези доповідей. – Seattle, Washington, USA: «ProConference», 2024. – С. 23–28.

4. Коробейнікова Т.І. Технологічний ланцюжок захисту мережевої інфраструктури компанії / Коробейнікова Т.І., Кіщак М.М., Лужецька Н.М. // International periodical scientific journal «SWorldJournal» – 2024. – № 25 (part 1) (May, 2024). – С. 75–81

УДК 004.056.5 : 004.738.5

МЕТОД KNN З ОЗНАКОВИМ ЗБАГАЧЕННЯМ ДЛЯ ВИЯВЛЕННЯ ІН'ЄКЦІЙНИХ АТАК У ВЕБ-ЗАПИТАХ

Назар КРАВЧУК, Тетяна КОРОБЕЙНІКОВА
Національний університет «Львівська політехніка»

У роботі досліджено застосування алгоритму k-найближчих сусідів (KNN) для виявлення ін'єкційних атак у HTTP-запитах - SQL-ін'єкцій, XSS та ін'єкцій команд. Проведено експерименти на трьох публічних наборах даних із використанням стратифікованої крос-валідації.Результати показали, що оптимізована модель KNN (k = 5, косинусна метрика, зважування за відстанню) досягає точності 99,77 % і F_1 = 0,998, перевершуючи базову конфігурацію TF-IDF без додаткових обчислювальних витрат.

***Ключові слова**: KNN, ін'єкційні атаки, SQLi, XSS, IDS/WAF, інженерія ознак, TF-IDF, метрики відстані, абляційний аналіз, хибнопозитивні спрацювання.*

The paper explores the application of the k-nearest neighbors (KNN) algorithm for detecting injection attacks in HTTP requests, including SQL injections, XSS, and command injections. Experiments were conducted on three public datasets using stratified cross-validation. The results showed that the optimized KNN model (k = 5, cosine metric, distance weighting) achieves 99.77% accuracy and an F_1 score of 0.998, outperforming the baseline TF-IDF configuration without additional computational cost.

***Keywords**: KNN, injection attacks, SQLi, XSS, IDS/WAF, feature engineering, TF-IDF, distance metrics, ablation analysis, false positives.*

Основний матеріал. Ін'єкційні атаки залишаються однією з найпоширеніших і найнебезпечніших категорій уразливостей вебзастосунків. Згідно з OWASP Top-10 , SQLi та XSS постійно перебувають серед ключових загроз для веб-інфраструктур. Попри розвиток сигнатурних і евристичних методів у сучасних IDS/WAF, їхня ефективність знижується через нові техніки обфускації, варіативність синтаксису та контекстну неоднозначність запитів [1-2].

Моделі глибинного навчання (CNN, LSTM, Transformer) демонструють високу точність, однак потребують значних обчислювальних ресурсів, тривалого навчання та великих обсягів маркованих даних. Це ускладнює їх застосування на рівні прикладних шлюзів [3-4].

Основна ідея дослідження полягає у збагаченні базового TF-IDF-подання доменними та статистичними ознаками, що підвищують стійкість до обфускацій і зміщень між наборами даних.

Таким чином, мета дослідження — створити легковаговий і пояснюваний модуль виявлення ін'єкцій, що поєднує точність, стабільність і простоту інтеграції в існуючі системи безпеки.

Методика. Запропонований метод складається з трьох послідовних етапів: 1) попередня обробка та представлення даних, що включає нормалізацію тексту та векторизацію за допомогою TF-IDF; 2) базова класифікація за алгоритмом KNN із систематичним дослідженням параметрів моделі; 3) розширення набору ознак для підвищення роздільної здатності моделі.

. Для оцінювання якості класифікації використовуються чотири стандартні метрики, що обчислюються на основі елементів матриці неточностей (confusion matrix): TP (істинно позитивні), TN (істинно негативні), FP (хибнопозитивні) та FN (хибнонегативні) спрацювання.

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad (1)$$

$$Precision = \frac{TP}{TP+FP} \quad (2)$$

$$Recall = \frac{TP}{TP+FN} \quad (3)$$

$$F_1 = 2 \times \frac{Precision \times Recall}{Precision+Recall} \quad (4)$$

Точність (Accuracy) (1) вимірює загальну правильність класифікації; прецизійність (ROC-AUC) (2) відображає надійність передбачень атак; повнота (Recall) (3) характеризує повноту виявлення; а F_1 (4), що поєднує обидві попередні метрики у вигляді гармонійного середнього, що є особливо інформативним у випадках дисбалансу класів.

Для навчання та оцінювання було використано три публічно доступні корпуси даних із платформи Kaggle: HttpParamsDataset (Evg3n1j, 2024) - використовується як основний набір даних для навчання та тестування і містить навантаження HTTP-параметрів, марковані як "norm" або "anom"; SQL Injection Dataset (Sajid 576, 2024) - застосовується для перехресного оцінювання узагальнювальної здатності (generalization) щодо атак типу SQLi; OS Command Injection Dataset (Sanket Pawase, 2024) - слугує гетерогенним тестовим стендом для виявлення атак типу Command Injection.

Базові результати. Таблиця 1 узагальнює три найефективніші конфігурації KNN на наборі даних InitialHttpParamsDataset.

Таблиця 1 - Базові результати KNN (InitialHttpParamsDataset)

k	Metric	Weights	Accuracy	$F_{1-\text{weighted}}$	$F_{1-macro}$
5	Cosine	Uniform	0.9874	0.9874	0.9866
3	Cosine	Uniform	0.9869	0.9869	0.9861
7	Cosine	Uniform	0.9870	0.9869	0.9861

Найефективніша конфігурація *k*=5, де косинусна метрика, однорідне зважування - досягла 98,74 % точності та зваженого F_1-показника 0,987. Детальний аналіз помилково класифікованих навантажень показав, що деякі обфусковані або контекстно неоднозначні зразки були неправильно розпізнані. Для розв'язання цих випадків було розроблено доповнювальний набір із семи числових ознак, обчислених безпосередньо зі сирих рядків навантажень.

Сконструйовані (інженерні) ознаки:

- Довжина корисного навантаження.
- Кількість цифр.
- Кількість великих літер.
- Кількість спеціальних символів.
- Ентропія символів за Шенноном (Відображає різноманітність символів у навантаженні, дозволяючи виявляти випадковість, спричинену кодуванням або конкатенацією.)
- Індикатор тавтології.
- Індикатор файлової системи/виконання.

Результати для найкращих конфігурацій узагальнено у Таблиці 2.

Таблиця 2 – Покращені результати KNN (ImprovedHttpParamsDataset)

k	Metric	Weights	Accuracy	$F_{1-\text{weighted}}$	$F_{1-macro}$
3	Cosine	Uniform	0.9977	0.9977	0.9975
5	Cosine	Distance	0.9977	0.9977	0.9975
7	Cosine	Distance	0.9976	0.9976	0.9974

Література

1. Nafiiev, A., Lande, D. (2023). Malware Detection Model based on Machine Learning. Bulletin of Cherkasy State Technological University, 28(3). URL: https://bulletin-chstu.com.ua/en/journals/t-23-3-2023/model-viyavlennya-shkidlivogo-programnogo-zabezpechennya-na-osnovi-mashinnogo-navchannya.

2. Кравчук Н. В. Безпечний доступ до серверів інформаційних систем, забезпечений ML-моделлю для блокування шкідливих запитів / Н.В. Кравчук, Т.І. Коробейнікова // Вісник Хмельницького національного університету. – 2024. – Том 341, №5. – С. 327–333.

3. Tavasoli, S. (2025). 10 Types of Machine Learning Algorithms and Models. Simplilearn Solutions. URL: https://www.simplilearn.com/10-algorithms-machine-learning-engineers-need-to-know-article.

4. Кравчук Н., Коробейнікова Т. (2024). Огляд проблематики захищеного доступу до вебсерверів. Вісник Львівського державного університету безпеки життєдіяльності, 30, 78-89.

УДК 004.056.5

СОЦІАЛЬНА ІНЖЕНЕРІЯ: МЕТОДИ АТАК І СПОСОБИ ЗАХИСТУ

КУНДО Б.М., СВІТЛИЧНИЙ В.А.
Харківський національний університет внутрішніх справ

У тексті розглянуто явище соціальної інженерії як один із найнебезпечніших методів кібератак. Описано поширені маніпулятивні техніки та психологічні механізми впливу, а також наведено ефективні стратегії протидії, що поєднують освітні та технічні заходи безпеки.

***Ключові слова**: хмарні технології, система зберігання даних, віртуалізація, безпека, масштабованість, контейнеризація.*

The text examines the phenomenon of social engineering as one of the most dangerous methods of cyberattacks. It describes common manipulative techniques and psychological influence mechanisms, as well as effective counterstrategies that combine educational and technical security measures.

***Keywords:** social engineering, cyberattacks, phishing, manipulation, human factor, information security, psychological influence, data protection, cyber threats, network security.*

Соціальна інженерія є одним із найнебезпечніших і водночас найпідступніших методів атак у сфері інформаційної безпеки, оскільки її головною мішенню є не технічні системи, а людина. На відміну від кібератак, що використовують програмні вразливості або недоліки мережевих протоколів, соціально-інженерні методи спрямовані на технологічні слабкості людської психології: довірливість, страх, бажання допомогти, цікавість або поспіх. Саме тому навіть найнадійніші цифрові системи можуть бути зламані, якщо користувач піддається маніпуляціям і добровільно передає конфіденційну інформацію або відкриває доступ до ресурсів.

Сутність соціальної інженерії полягає у створенні умов, за яких людина сама виконує бажані для зловмисника дії - вводить пароль, переходить за шкідливим посиланням, відповідає на фальшивий запит або надає доступ до приміщення. Найпоширенішим методом таких атак є фішинг - розсилання підроблених повідомлень, які імітують офіційні листи від банків, державних служб чи відомих компаній. Такі листи містять переконливі логотипи, стилістику й повідомлення про нібито термінову проблему, примушуючи користувача діяти швидко та без обдумування. Більш цілеспрямованою формою є спірфішинг, де зловмисники використовують персональну інформацію жертви, що робить атаку майже непомітною. На кшталт фішингу діють і телефонні атаки - вішинг, коли шахраї видають себе за працівників банку чи технічної підтримки, та смішинг – маніпулятивні SMS-повідомлення.

Іншим типовим методом соціальної інженерії є претекстинг, що передбачає створення штучної, але правдоподібної легенди з метою викликати довіру та отримати потрібні дані. Соціальний інженер може видавати себе за співробітника служби безпеки, керівника, перевіряючого або колегу, який «терміново» потребує доступу. Значну загрозу становлять також фізичні методи, такі як «tailgating», коли зловмисник проходить у приміщення разом зі співробітником, користуючись його ввічливістю або невпевненістю відмовити. Ефективність цих технік зумовлена тим, що вони активують емоційні реакції, які пригнічують критичне мислення. Улюбленими інструментами зловмисників є створення відчуття терміновості, страху або вигоди: повідомлення про заблокований рахунок, «виграш», загрозу покарання чи привабливу пропозицію. Людина, перебуваючи в емоційно напруженому стані, частіше ухвалює імпульсивні рішення, не перевіряючи достовірності інформації.

Захист від соціальної інженерії базується на поєднанні освітніх, організаційних і технічних заходів. Найважливішим є підвищення обізнаності користувачів: навчання персоналу розпізнавати фішингові повідомлення, перевіряти джерела інформації, не надавати конфіденційні дані у відповідь на підозрілі запити. Розвиток критичного мислення і розуміння того, що ніхто не має права вимагати у користувача пароль чи особисті дані, є ключовими факторами протидії. Технічні механізми – такі як багатофакторна автентифікація, антивірусні програми, фільтри спаму, оновлення систем безпеки - здатні істотно знизити ризики, оскільки навіть у разі компрометації пароля доступ до системи буде ускладнений.

Організації повинні впроваджувати чіткі політики безпеки, що регламентують комунікацію, порядок обміну інформацією та перевірки запитів. Імітаційні навчання – такі як симульований фішинг - допомагають оцінити рівень готовності співробітників та виявити слабкі місця. В сфері фізичної безпеки важливими є системи контролю доступу, службові посвідчення та правила недопущення сторонніх осіб без перевірки.

Таким чином, соціальна інженерія становить серйозну загрозу для інформаційної безпеки, оскільки експлуатує природні людські реакції і здатна обійти найскладніші технічні механізми захисту. Єдиний ефективний спосіб протидії - це формування високого рівня обізнаності, критичності та відповідальності як у окремих користувачів, так і в організацій загалом. Лише поєднання психологічної грамотності й сучасних технологічних засобів може забезпечити надійний захист від маніпуляцій та зловживань, спрямованих на отримання конфіденційної інформації.

Література

1. Що таке соціальна інженерія? Напади, методи та запобігання – HackYourMom. HackYourMom. URL: https://hackyourmom.com/kibervijna/shho-take-soczialna-inzheneriya-napady-metody-ta-zapobigannya (дата звернення: 20.11.2025).

УДК 004.056.5

СУЧАСНІ ТИПИ АТАК ПРОГРАМ-ВИМАГАЧІВ ТА ЇХНІЙ ДЕСТРУКТИВНИЙ ВПЛИВ НА КІБЕРСТІЙКІСТЬ МАЛОГО БІЗНЕСУ В УМОВАХ ЕВОЛЮЦІЇ ЦИФРОВИХ ЗАГРОЗ

Анастасія ЛАНЧЕВИЧ, Валентина ЯЩУК, Наталія МАСЛОВА
Львівський державний університет безпеки життєдіяльності

Розглянуто сучасні типи атак програм-вимагачів (ransomware) та їхній вплив на кіберстійкість суб'єктів малого підприємництва. Проаналізовано основні тенденції еволюції ransomware, їхні тактичні особливості та наслідки для економічної, операційної й репутаційної стабільності бізнесу. Визначено ключові типи атак, зокрема Crypto-ransomware, Double Extortion, Ransomware-as-a-Service (RaaS) та гібридні моделі, що поєднують фішинг, експлуатацію вразливостей і соціальну інженерію. Доведено, що малий бізнес є найбільш уразливим сектором через обмежені ресурси для впровадження систем кіберзахисту та недостатню обізнаність персоналу. Запропоновано комплекс заходів із підвищення кіберстійкості, який передбачає багаторівневий захист, регулярне резервне копіювання, впровадження багатофакторної автентифікації, поведінковий моніторинг (EDR/XDR), навчання персоналу та розроблення планів реагування на інциденти. Ефективна протидія програмам-вимагачам вимагає переходу від реактивних підходів до проактивної кібербезпеки, орієнтованої на попередження загроз і зменшення площини атаки.

Ключові слова: *програми-вимагачі, ransomware, кіберстійкість, малий бізнес, EDR/XDR, цифрові загрози, інформаційна безпека.*

Modern types of ransomware attacks and their impact on the cyber resilience of small businesses are considered. The main trends in the evolution of ransomware, their tactical features and consequences for the economic, operational and reputational stability of businesses are analyzed. Key types of attacks are identified, including Crypto-ransomware, Double Extortion, Ransomware-as-a-Service (RaaS) and hybrid models that combine phishing, vulnerability exploitation and social engineering. It is proven that small businesses are the most vulnerable sector due to limited resources for implementing cyber protection systems and insufficient staff awareness. A set of measures to increase cyber resilience is proposed, which includes multi-layered protection, regular backups, implementation of multi-factor authentication, behavioral monitoring (EDR/XDR), staff training and development of incident response plans. It is concluded that effective countermeasures against ransomware require a shift from reactive approaches to proactive cybersecurity focused on threat prevention and attack surface reduction.

Keywords: *ransomware, ransomware, cyber resilience, small business, EDR/XDR, digital threats, information security.*

У сучасних умовах цифрової трансформації бізнесу спостерігається стрімке зростання кількості кібератак із використанням програм-вимагачів. Їхня еволюція — від простих шкідливих скриптів до багатокомпонентних платформ Ransomware-as-a-Service — зумовлює суттєве підвищення рівня загрози

навіть для підприємств із невеликим масштабом діяльності. Малий бізнес, як правило, не має достатніх фінансових, кадрових та технологічних ресурсів для впровадження комплексних засобів кіберзахисту, що робить його вразливою ціллю для злочинців, орієнтованих на швидку монетизацію атак.

Основними сучасними типами програм-вимагачів (ransomware) є locker-атаки, crypto-ransomware та моделі подвійного вимагання (double extortion), кожна з яких характеризується ускладненням механізмів компрометації та підвищенням рівня деструктивного впливу на цільові системи. Locker-атаки спрямовані на блокування доступу користувача до операційної системи або критично важливих функцій пристрою, при цьому дані не шифруються, але взаємодія із системою стає неможливою без сплати викупу. Натомість crypto-ransomware реалізують більш складну модель шифрування, використовуючи стійкі криптографічні алгоритми, такі як AES, RSA або ChaCha20, що робить процес дешифрування без ключа фактично неможливим.

Окрему загрозу становлять атаки типу double extortion, у межах яких зловмисники не лише шифрують дані жертви, але й здійснюють їх попереднє копіювання для подальшого шантажу — зокрема, шляхом публікації або продажу викраденої інформації у dark web. Такий підхід збільшує тиск на постраждалих організацій, адже навіть відновлення систем із резервних копій не гарантує уникнення репутаційних або юридичних ризиків, пов'язаних із витоком даних.

Особливої уваги заслуговує поява бізнес-моделі Ransomware-as-a-Service (RaaS), яка призвела до своєрідної "демократизації" кіберзлочинності. Ця модель передбачає комерціалізацію шкідливого ПЗ, коли розробники ransomware надають готові інструменти та інфраструктуру для проведення атак у вигляді платних підписок або партнерських програм. Унаслідок цього навіть особи без спеціальної технічної підготовки отримують змогу здійснювати ефективні атаки, що значно підвищує загальний рівень кіберзагроз для малого бізнесу, який часто не має достатніх ресурсів для комплексного захисту.

Сучасні тенденції розвитку ransomware також вказують на гібридизацію атак, коли різні техніки компрометації — фішинг, експлуатація вразливостей у програмному забезпеченні, використання викрадених або довірених облікових записів, а також lateral movement у внутрішніх мережах — поєднуються у багаторівневі сценарії вторгнення. Такий підхід забезпечує зловмисникам глибше проникнення в корпоративне середовище, ускладнюючи виявлення та нейтралізацію інцидентів традиційними засобами кіберзахисту. У результаті, сучасні програми-вимагачі трансформувалися з ізольованих шкідливих компонентів у складні кібероперації з чітко структурованою логістикою, фінансуванням та розподілом ролей, що становить особливо серйозну загрозу для кіберстійкості малого бізнесу в умовах еволюції цифрових загроз.

Деструктивний вплив ransomware на малий бізнес проявляється у трьох вимірах: економічному, операційному та репутаційному. Прямі економічні втрати включають сплату викупу, відновлення даних і втрату доходів унаслідок простою. Операційні наслідки виявляються у втраті досту-

пу до інформаційних ресурсів і зупинці бізнес-процесів, тоді як репутаційні ризики загрожують втратою клієнтської довіри. Людський фактор залишається визначальним у більшості випадків компрометації — понад 80% інфекцій починаються з фішингових листів або шкідливих вкладень.

Для підвищення кіберстійкості малого бізнесу доцільним є впровадження багаторівневої стратегії захисту, що базується на принципах Zero Trust і проактивного моніторингу. Серед найефективніших заходів — ізольоване резервне копіювання, багатофакторна автентифікація, застосування EDR/XDR-рішень для поведінкового аналізу, регулярне оновлення програмного забезпечення, контроль привілеїв користувачів, сегментація мережі та навчання персоналу методам розпізнавання соціоінженерних атак. Впровадження таких практик дає змогу мінімізувати ризики компрометації, скоротити час виявлення інцидентів і забезпечити швидке відновлення після атак.

Отже, сучасні атаки програм-вимагачів є одним із головних викликів для кіберстійкості малого бізнесу, який потребує не лише технічних, а й організаційних рішень. Перехід до моделі проактивної кібербезпеки та впровадження стратегічного управління ризиками є необхідною умовою стабільності підприємницької діяльності в умовах зростання цифрових загроз.

Література

1. Symantec. Ransomware and Business 2024 Report. – Symantec, 2024.

2. Verizon. Data Breach Investigations Report (DBIR) 2024. – Verizon Enterprise, 2024.

3. IBM X-Force. Cost of a Data Breach Report 2024. – IBM Security, 2024.

4. Ящук В.І. Методика забезпечення безпеки інформаційних систем та реагування на кіберінциденти кібербезпековими центрами / Ящук В.І. // Scientific Collection «InterConf+», 45(201): with the Proceedings of the 8thInternational Scientific and Practical Conference «International Scientific Discussion: Problems, Tasks and Prospects» (May19-20, 2024; Brighton, United Kingdom)/ comp. by LLC SPC «InterConf».Brighton: A.C.M. Webb Publishing Co Ltd., 2024. P.632-641 ISSN 2709-4685 DOI10.51582/interconf.19-20.05.2024

5. Microsoft Security Intelligence. Ransomware Trends and Data Breach Report 2025. – Redmond, 2025.

6. ENISA. Threat Landscape 2024: The Ransomware Dimension. – European Union Agency for Cybersecurity, 2024.

УДК 004.056.5:004.8:621.391

СУЧАСНІ ПІДХОДИ ДО RF-FINGERPRINTING: МОДЕЛІ ТА МЕТОДИ ІДЕНТИФІКАЦІЇ БЕЗДРОТОВИХ ПРИСТРОЇВ ЗА РАДІОЧАСТОТНИМИ ПАРАМЕТРАМИ

Георгій ЛОБАН, Тарас ЛУКОВСЬКИЙ
Національний Університет «Львівська Політехніка»

У дослідженні представлені сучасні моделі та методи RF-fingerprinting у контексті ідентифікації бездротових пристроїв. Проаналізовано основні джерела унікальності радіосигналів, сучасні методи обробки та класифікації сигналів, вплив факторів середовища. Окреслено ключові методологічні обмеження та перспективні напрями розвитку технології.

Ключові слова: *RF-fingerprinting, кібербезпека, виявлення загроз, радіочастотна ідентифікація, обробка сигналів, бездротова безпека, класифікація пристроїв.*

The study presents a comprehensive analysis of state-of-the-art models and methods of RF-fingerprinting in the context of wireless device identification. It analyzes the primary sources of signal uniqueness, modern signal processing and classification methods, and environmental influences. Key methodological limitations and prospective directions for advancing the technology are outlined.

Keywords: *RF-fingerprinting, cybersecurity, threat detection, radio-frequency identification, signal processing, wireless security, device classification.*

Стрімкий розвиток бездротових технологій та експоненційне зростання кількості підключених пристроїв формують нові виклики у галузі кібербезпеки та управління мережевими інфраструктурами. За таких умов особливої актуальності набуває створення ефективних механізмів ідентифікації й автентифікації бездротових пристроїв, здатних гарантувати захищеність комунікацій і запобігати несанкціонованому доступу. Хоча криптографічні протоколи та цифрові сертифікати залишаються основою більшості систем безпеки, вони не забезпечують повної стійкості до загроз. З огляду на це, технологія RF-fingerprinting, що базується на використанні унікальних радіочастотних параметрів апаратних компонентів передавачів, постає як перспективний інструмент посилення безпеки на фізичному рівні мережевої моделі OSI.

Концепція RF-fingerprinting полягає у тому, що кожен радіопередавач має індивідуальний «радіочастотний відбиток», що виникає унаслідок виробничих неточностей та відмінностей у параметрах електронних компонентів [1]. Зазначені особливості проявляються як характерні спотворення сигналу, що передається і який піддається вимірюванню та можуть бути основою для формування індивідуального «радіочастотного відбит-

ка» пристрою. На відміну від програмних методів автентифікації, які можуть бути скомпрометовані, фізичні ознаки сигналу значно складніше підробити або клонувати, що робить RF-fingerprinting ефективним засобом виявлення підроблених, клонованих або несанкціонованих пристроїв [2].

У роботі було розглянуто джерела формування RF-відбитків та їх вплив на характеристики переданого сигналу задля здійснення комплексного аналізу фізичних основ унікальних радіочастотних характеристик бездротових передавачів. Було досліджено кварцові осцилятори, підсилювачі потужності, модулятори IQ та антенні системи, а також їх особливості.

У межах проведеного аналізу систематизовано сучасні методи вилучення ознак із радіосигналів, що використовуються для побудови моделей ідентифікації. У часовій області ключовими ознаками є вивчення перехідних процесів (transients) при вмиканні передавача, динаміки наростання та спаду сигналу, а також статистичних характеристик амплітуди, які дозволяють виокремлювати індивідуальні особливості передавача [3]. У частотній області параметрами є зсув несучої частоти та спектральна щільність фазового шуму [4]. У часово-частотному підході основними методами є вейвлет-перетворення, що забезпечує адаптивну роздільну здатність а також віконне перетворення (STFT), яке дозволяє відстежувати зміни спектральних характеристик під час передачі пакету даних [5].

Особлива увага в роботі була приділена сучасним підходам класифікації радіочастотних відбитків на основі машинного та глибокого навчання, які станом на сьогодні займають важливе місце у системах RF-fingerprinting. Традиційні моделі, такі як SVM, k-NN та Random Forest залишаються актуальними для задач з невеликою кількістю пристроїв та високим співвідношенням сигнал/шум. Вони забезпечують прийнятний рівень точності і мають нижчі обчислювальні вимоги, проте їх масштабованість обмежена через збільшення розмірності ознакових просторів [6]. Натомість методи глибокого навчання, включно зі згортковими нейронними мережами (CNN), рекурентними моделями (LSTM) і трансформерами, демонструють високу точність при роботі з великими масивами необроблених IQ-даних [7]. Їхня здатність автоматично формувати багаторівневі ознаки робить ці підходи найбільш ефективними для ідентифікації пристроїв у складних радіочастотних середовищах. Проте такі моделі є чутливими до зміни каналу, старіння компонентів та атак, спрямованих на порушення роботи алгоритмів машинного навчання. Систематизація існуючих підходів виявила чітку тенденцію переходу від традиційних методів обробки сигналів до складних архітектур глибокого навчання. Згорткові нейронні мережі та трансформери демонструють найкращі результати з точністю 97-99.8% [8] в контрольованих умовах, проте традиційні методи машинного навчання, такі як SVM та Random Forest, залишаються актуальними завдяки кращій інтерпретованості та меншим обчислювальним вимогам.

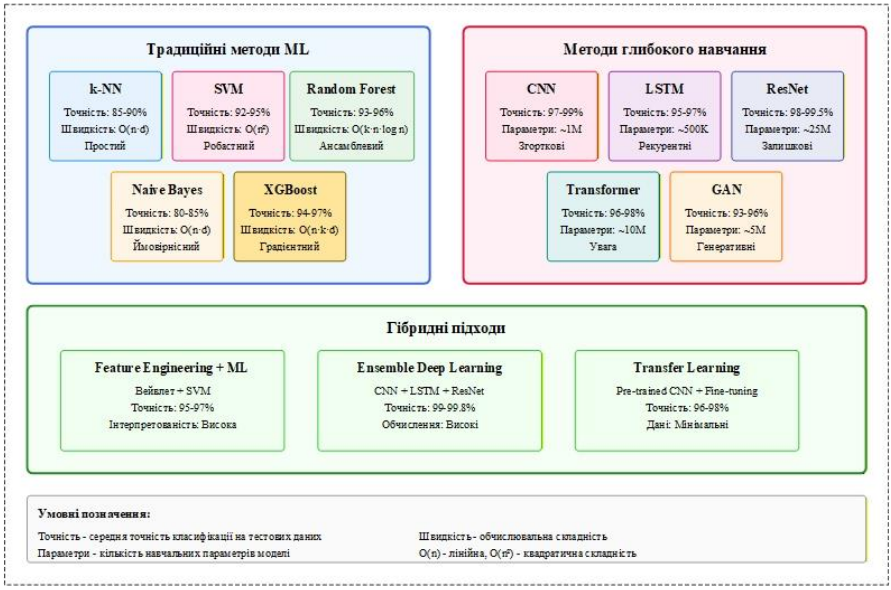

Рисунок 1 – Класифікація алгоритмів машинного навчання для RF-fingerprinting

Проблематика впливу радіочастотного середовища на достовірність ідентифікації є одним з ключових викликів для широкого впровадження методу RF-fingerprinting. Багатопроменеве поширення, температурні коливання та динамічні зміни каналу здатні суттєво спотворювати інформативні ознаки сигналів, що вимагає розробку і використання методів адаптивної компенсації. Важливим також є питання довготривалої стабільності RF-відбитка: деградація параметрів апаратних компонентів може спричиняти дрейф частоти та нелінійних характеристик, що знижує точність ідентифікації в довгостроковій перспективі [9]. Запропоновані у сучасних дослідженнях методи регулярного перенавчання моделей та використання автоенкодерів для відстеження зміни ознак демонструють перспективність, але потребують подальшої оптимізації.

Говорячи про обмеження та виклики технології, варто також зазначити проблему масштабованості та навмисних атак. При збільшенні кількості пристроїв спостерігається квадратичне зростання складності класифікації для методів на основі попарних порівнянь. База даних для 10,000 пристроїв з 1000 зразків на пристрій при 1024 комплексних відліках займає близько 80 ГБ пам'яті. Час пошуку в такій базі становить 50-200 мс навіть з оптимізованими індексами [10]. Навмисні атаки (adversarial attacks), які спеціально розроблені для обману систем машинного навчання, становлять

серйозну загрозу для даної технології. Додавання carefully crafted perturbations з потужністю всього -30 дБ відносно сигналу може знизити точність класифікації з 98% до 15%.

Аналіз прикладних аспектів RF-fingerprinting підтверджує широкий спектр його застосування. У промислових IoT-системах технологія дозволяє виявляти підроблені датчики й протидіяти атакам спуфінгу без модифікації протоколів зв'язку. У військових системах вона може забезпечувати розпізнавання «свій–чужий» на фізичному рівні, а в телекомунікаційних мережах — запобігати появі клонованих SIM-карт або несанкціонованих точок доступу Wi-Fi. Автомобільні системи безключового доступу — один із найбільш показових прикладів, де RF-fingerprinting здатний підвищити стійкість до relay- та replay-атак, забезпечуючи додатковий рівень автентифікації пристроїв.

Проведений аналіз дає змогу стверджувати, що RF-fingerprinting є перспективною технологією посилення кібербезпеки бездротових систем. Подальший розвиток цього напрямку пов'язаний із впровадженням квантових методів обробки сигналів, використанням федеративного навчання для побудови розподілених моделей без централізованого збору даних [11], а також інтеграцією з технологією 6G, що відкривають можливості для аналізу сигналів терагерцового діапазону та використання масивних MIMO-антенних решіток. Сукупність цих технологічних трендів формує підґрунтя для створення робастних та масштабованих систем ідентифікації, здатних функціонувати в умовах складного та динамічного радіочастотного середовища.

Таким чином, технологія RF-fingerprinting не замінює наявні механізми безпеки, а виступає їхнім доповненням, забезпечуючи додатковий фізичний рівень захисту, що функціонує незалежно від програмних вразливостей. Це визначає її як ключовий елемент майбутніх систем кібербезпеки в умовах глобальної цифровізації та розвитку Інтернету речей.

Література

1. Danev, B., Zanetti, D., & Capkun, S. (2012). On physical-layer identification of wireless devices. ACM Computing Surveys, 45(1), 1-29. DOI: 10.1145/2379776.2379782

2. Rehman, S. U., Sowerby, K. W., & Coghill, C. (2014). Analysis of impersonation attacks on systems using RF fingerprinting and low-end receivers. Journal of Computer and System Sciences, 80(3), 591-601. DOI: 10.1016/j.jcss.2013.06.013

3. Ureten, O., & Serinken, N. (1999). Wireless security through RF fingerprinting. Canadian Journal of Electrical and Computer Engineering, 32(1), 27-33. DOI: 10.1109/CJECE.2007.364330

4. Vo-Huu, T. D., Vo-Huu, T. D., & Noubir, G. (2016). Fingerprinting Wi-Fi devices using software defined radios. Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks, 3-14. https://doi.org/10.1145/2939918.2939936

5. Klein, R. W., Temple, M. A., & Mendenhall, M. J. (2009). Application of wavelet-based RF fingerprinting to enhance wireless network security. Journal of Communications and Networks, 11(6), 544-555. DOI: 10.1109/JCN.2009.6388408

6. Reising, D. R., Temple, M. A., & Mendenhall, M. J. (2010). Improved wireless security for GMSK-based devices using RF fingerprinting. International Journal of Electronic Security and Digital Forensics, 3(1), 41-59. https://doi.org/10.1504/IJESDF.2010.032330

7. A. Al-Shawabka et al., "Exposing the Fingerprint: Dissecting the Impact of the Wireless Channel on Radio Fingerprinting," IEEE INFOCOM 2020 - IEEE Conference on Computer Communications, Toronto, ON, Canada, 2020, pp. 646-655, doi: 10.1109/INFOCOM41043.2020.9155259.

8. S. Hanna, S. Karunaratne and D. Cabric, "Open Set Wireless Transmitter Authorization: Deep Learning Approaches and Dataset Considerations," in IEEE Transactions on Cognitive Communications and Networking, vol. 7, no. 1, pp. 59-72, March 2021, doi: 10.1109/TCCN.2020.3043332

9. Xie, Ning & Zhang, Shengli. (2018). Blind Authentication at the Physical Layer Under Time-Varying Fading Channels. IEEE Journal on Selected Areas in Communications. PP. 1-1. 10.1109/JSAC.2018.2824583.

10. Wang, W., Sun, Z., Piao, S., Zhu, B., & Ren, K. (2016). Wireless physical-layer identification: Modeling and validation. IEEE Transactions on Information Forensics and Security, 11(9), 2091-2106. DOI: 10.1109/TIFS.2016.2552146

11. McMahan, B., Moore, E., Ramage, D., Hampson, S., & y Arcas, B. A. (2017). Communication-efficient learning of deep networks from decentralized data. Proceedings of the 20th International Conference on Artificial Intelligence and Statistics, 1273-1282. https://doi.org/10.48550/arXiv.1602.05629

УДК 004.056.53:004.8

АНАЛІЗ ОБМЕЖЕНЬ ТРАДИЦІЙНИХ NIDS ТА ПЕРСПЕКТИВИ ЇХ РОЗШИРЕННЯ МЕТОДАМИ МАШИННОГО НАВЧАННЯ

Софія ЛУКАШ
Сумський державний університет

У роботі розглянуто традиційні та інтелектуальні підходи до виявлення аномалій у мережевому трафіку. Проаналізовано обмеження класичних NIDS та переваги використання методів машинного навчання. Обґрунтовано доцільність інтеграції ML-модулів у сучасні системи для підвищення точності та адаптивності виявлення загроз.

Ключові слова: *мережевий трафік, аномалії, NIDS, сигнатурний аналіз, поведінковий аналіз, машинне навчання, кіберзагрози.*

The paper examines traditional and intelligent approaches to network anomaly detection. It analyzes the limitations of classical NIDS and the benefits of applying machine learning methods. The study justifies the integration of ML modules to enhance the accuracy, adaptability, and effectiveness of modern intrusion detection systems.

Keywords: *network traffic, anomalies, NIDS, signature analysis, behavioral analysis, machine learning, cyber threats.*

Вступ. В умовах стрімкого розвитку мережевих технологій своєчасне виявлення загроз залишається одним із фундаментальних аспектів кібербезпеки. Постійне зростання обсягів трафіку, ускладнення сценаріїв атак та поява нових, малопомітних технік вимагають переосмислення підходів до аналізу даних.

Серед найпоширеніших загроз, що проявляються у вигляді аномалій, виділяють DDoS-атаки, сканування портів і вразливостей, спроби несанкціонованого доступу, Brute-force, мережеві вторгнення, DNS-спуфінг, а також різні види шкідливого трафіку, націленого на порушення конфіденційності та цілісності даних. Основою захисту інфраструктури залишаються традиційні системи виявлення мережевих вторгнень (NIDS), і саме на їхній базі сформувалися класичні методи аналізу [1].

Аналіз традиційних підходів. Традиційні NIDS, як правило, спираються на сигнатурні або поведінкові методи. Сигнатурний підхід працює за принципом порівняння трафіку з базою відомих шаблонів атак – саме так функціонують Snort, Suricata та інші популярні рішення.

Поведінковий аналіз, у свою чергу, формує профіль «нормальної» активності та фіксує будь-які відхилення від нього. Ці підходи стали стандартом індустрії, оскільки гарантують швидку реакцію, простоту впровадження та високу точність виявлення вже відомих загроз.

З технічної точки зору, основою роботи традиційних систем є детерміновані алгоритми, що спираються на чітко визначені правила. Вони здійснюють порівняння мережевих пакетів із базами відомих сигнатур або використовують прості евристики та базові статистичні порогові моделі для

виявлення відхилень. Завдяки низькій обчислювальній складності та прозорості логіки такі методи забезпечують ефективне виявлення більшості відомих типів атак у режимі реального часу, майже не навантажуючи системні ресурси.

Водночас традиційні підходи мають низку обмежень, які стають критичними на тлі сучасного ландшафту кіберзагроз. До ключових недоліків належать [2]:

- нездатність виявляти Zero-Day атаки, для яких ще не існує сигнатур;
- висока залежність від ручного оновлення баз та правил;
- вразливість до обхідних технік, що маскують шкідливу активність під легітимну;
- значна кількість хибнопозитивних спрацювань, особливо при використанні поведінкового аналізу;
- відсутність адаптивності, оскільки ці методи не здатні навчатися на нових даних;
- неефективність при роботі зі складними високовимірними залежностями, характерними для сучасного трафіку.

Варто зазначити, що значна кількість хибнопозитивних спрацювань у таких системах часто призводить до явища «втоми від сповіщень», коли адміністратори безпеки можуть пропустити реальну загрозу через великий потік фонового шуму.

Попри це, традиційні підходи не можна назвати застарілими. Вони мають очевидні переваги, зокрема високу швидкість, прогнозованість, прозорість роботи та ефективність проти масових типових атак. Саме тому вони залишаються актуальними для базового рівня мережевого моніторингу.

Впровадження машинного навчання. Розвиток машинного навчання (ML) відкриває можливості для компенсації згаданих недоліків. Методи з учителем (наприклад, Random Forest, Support Vector Machine) дозволяють класифікувати типи атак, використовуючи попередньо розмічені дані. Методи без учителя (Unsupervised Learning, зокрема автоенкодери) допомагають виявляти невідомі аномалії шляхом групування схожих патернів. Глибоке навчання дає змогу аналізувати високовимірні структури трафіку, знаходячи приховані закономірності, які недоступні традиційним алгоритмам [3]. Завдяки здатності до самонавчання та адаптивності ці моделі значно розширюють можливості NIDS там, де класичні методи демонструють обмежену ефективність.

Алгоритми ML дозволяють детектувати нові або модифіковані атаки, зменшувати кількість помилкових тривог, обробляти великі масиви даних та адаптуватися до змін у поведінці мережі. Це робить машинне навчання перспективним доповненням до існуючих систем. На практиці мова йде не про відмову від традиційних NIDS, а про створення комбінованих рішень, де сигнатурний, поведінковий та ML-аналіз доповнюють один одного, забезпечуючи багаторівневий захист [4].

Окремою вагомою перевагою використання ML є можливість аналізу зашифрованого трафіку без необхідності його дешифрування. У

той час як традиційні системи втрачають ефективність при роботі з протоколами TLS/SSL, моделі машинного навчання здатні виявляти шкідливу активність, аналізуючи лише метадані потоку: довжину пакетів, інтервали між ними та специфіку рукостискань.

Таким чином, виникає нагальна потреба у створенні та інтеграції модулів машинного навчання в архітектуру існуючих NIDS. Розробка таких модулів є технічно реалістичною завдяки наявності широкого спектра бібліотек і фреймворків, таких як Scikit-learn, TensorFlow та PyTorch, що забезпечують ефективне тренування моделей на мережевому трафіку Водночас низка питань залишається відкритою: окрім ефективності навчання, точності та здатності до узагальнення, критичним викликом є вразливість самих ML-моделей до змагальних атак, спрямованих на маніпуляцію вхідними даними для обходу захисту [5].

Тематика застосування ML для виявлення аномалій активно розглядається в наукових колах, де досліджуються питання функціональності, доцільності впровадження та перспективи подальшого вдосконалення таких систем.

Висновки. Отже, сучасний підхід до виявлення аномалій має базуватися не на заміні класичних методів, а на їхньому розширенні за допомогою інтелектуальних технологій. Інтеграція машинного навчання у традиційні NIDS є необхідним кроком для підвищення адаптивності, масштабованості та здатності виявляти нові типи загроз. Це дозволить побудувати надійну систему безпеки, яка зможе ефективно захистити мережу.

Література

1. Khraisat A., Gondal I., Vamplew P., Kamruzzaman J. Survey of intrusion detection systems: techniques, datasets and challenges. Cybersecurity, 2019, 2(1). – P. 1–22. URL: https://doi.org/10.1186/s42400-019-0038-7.

2. Hindy H., Brosset D., Bayne E. et al. A Taxonomy of Network Threats and the Effect of Current Datasets on Intrusion Detection Systems. IEEE Access, 2020, Vol. 8. – P. URL: https://doi.org/10.1109/ACCESS.2020.3000179.

3. Charles E., Iseal S., Olabiyi W. Comparative Study of Traditional vs. AI-Based Techniques in Network Intrusion Detection Systems. ResearchGate. (2025). URL: https://www.researchgate.net/publication/389717078_Comparative_Study_of_Traditional_vs_AI-Based_Techniques_in_Network_Intrusion_Detection_Systems.

4. Ferrag M. A., Maglaras L., Moschoyiannis S., Janicke H. Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. Journal of Information Security and Applications, 2020, Vol. 50. – и 102419. URL: https://doi.org/10.1016/j.jisa.2019.102419.

5. Ibitoye O., Abou-Khamis R., Matrawy A. The Threat of Adversarial Attacks against Machine Learning in Network Security: A Survey. IEEE Communications Surveys & Tutorials, 2019, 21(4). – P. 3543–3572. URL: https://doi.org/10.37256/jeee.4120255738.

УДК 004.056:004.85

ЗАСТОСУВАННЯ МЕХАНІЗМІВ ЗАХИСТУ ПЕРСОНАЛІЗОВАНИХ ТЕКСТОВИХ ДАНИХ У СЕРВІСАХ МАШИННОГО ПЕРЕКЛАДУ

Ігор МАЛЕЦЬ
Національний університет «Львівська політехніка»

Описано підхід до захисту персоналізованих текстових даних у сервісах машинного перекладу, інтегрованих з e-mail-розсилками. Запропоновано сегментацію контенту за чутливістю, введено шар контролю безпеки між CRM та хмарними рушіями МП, окреслено вимоги до журналювання, анонімізації та обмеження доступу до пам'яті перекладів.

***Ключові слова**: машинний переклад, e-mail-розсилки, персональні дані, інформаційна безпека, хмарні сервіси.*

An approach to protecting personalized text data in machine translation services integrated with email newsletters is described. Content segmentation by sensitivity is proposed, a layer of security control is introduced between CRM and cloud-based MT engines, and requirements for logging, anonymization, and access restrictions to translation memories are outlined.

***Keywords**: machine translation, e-mail newsletters, personal data, information security, cloud services.*

Персоналізовані e-mail-розсилки та друк зі змінними даними (VDP) широко застосовуються у маркетингових сервісах. У таких сценаріях текстові шаблони листів поєднуються з даними CRM-системи, що містять ім'я одержувача, адресу електронної пошти, мовні уподобання та інші атрибути [1]. Для багатомовної підтримки цих кампаній дедалі частіше використовуються сервісні рішення машинного перекладу, які взаємодіють із хмарними рушіями та зовнішніми API. У результаті виникає задача забезпечення конфіденційності персоналізованого тексту на всьому шляху його проходження від CRM до каналу доставки.

У реалізованій архітектурі сервісу машинного перекладу документи та шаблони розглядаються як сукупність сегментів: звертання з маркерами [[NAME]], реквізити автора, основний текст пропозиції, службові елементи. Такий підхід дає змогу присвоювати кожному сегменту тип і набір атрибутів, зокрема ознаку чутливості. Виділяються принаймні три класи: сегменти з явними персональними даними (ПІБ, адреса, контактні дані), нейтральний зміст шаблону без ідентифікаторів особи та службові маркери й технічні коди.

На основі цієї класифікації сформовано політику оброблення тексту в сервісі машинного перекладу. Сегменти з високою чутливістю не передаються до хмарних рушіїв МП, а обробляються локально за допомогою внутрішніх моделей або пам'яті перекладів. Для нейтральних сегментів дозволяється виклик зовнішніх сервісів, але перед відправкою виконується нормалізація та фільтрація маркерів, що можуть розкривати персональні дані. Службові маркери [[NAME]], [[DISCOUNT]], [[GROUP_ID]] тощо замінюються

на анонімізовані ідентифікатори, а підстановка реальних значень виконується лише на локальному етапі формування електронних листів.

У сервісну архітектуру [2] додано шар контролю безпеки, який функціонує між інтерфейсами CRM/VDP та модулем виклику хмарних рушіїв [3]. Цей шар виконує перевірку належного маркування сегментів, анонімізацію персональних маркерів, обмеження обсягу журналювання та застосування політик доступу до пам'яті перекладів. Записи ТМ, що містять або потенційно можуть містити ідентифікаційні дані, зберігаються у зашифрованому вигляді або взагалі виключаються з повторного використання [4]. Доступ до ТМ і журналів API дозволяється лише автентифікованим користувачам за ролями [5].

REST-інтерфейси /api/translate та /api/bulk-translate, реалізовані в прототипі [2], доповнено параметрами автентифікації та обмеженням швидкості запитів. Логування результатів обмежується технічною інформацією (ідентифікатори сегментів, тривалість запиту, тип джерела перекладу), без збереження повних текстів персоналізованого змісту. У веб-інтерфейсі сегментного редагування передбачено візуальне позначення сегментів, для яких заборонена відправка в хмарні сервіси: такі сегменти перекладаються локально або тільки через пам'ять перекладів (рис. 1).

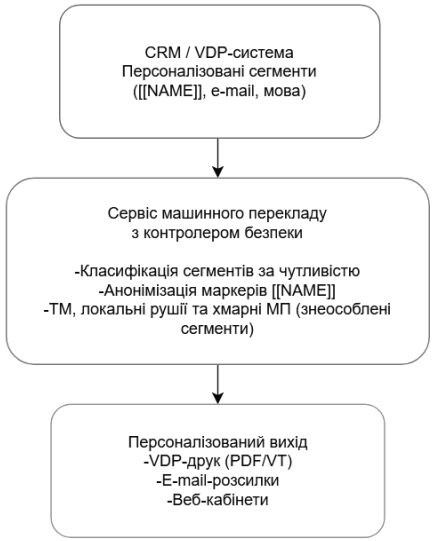

Рисунок 1 – Потік персоналізованих текстових даних
у сервісі машинного перекладу з шаром контролю безпеки

Таким чином, запропонований підхід демонструє, що сервіс машинного перекладу може використовуватися як проміжний мовний шар у email-розсилках та інших персоналізованих даних за умови формалізації політики оброблення сегментів за чутливістю, обмеження передачі конфіденційних даних у хмарні рушії та впровадження механізмів контролю доступу до пам'яті перекладів. При розгортанні моделі обробки сегментів із використанням пам'яті перекладів та маршрутизації між рушіями це створює передумови для безпечної інтеграції технологій машинного перекладу в системи персоналізованих комунікацій.

Література

1. Малець І. Сценарії використання сервісу машинного перекладу в цифрових каналах. Сучасні методи, інформаційне, програмне та технічне забезпечення систем керування організаційно-технічними та технологічними комплексами, №12, 2025.

2. Малець І. Централізована мовна інфраструктура для каналів контент-маркетингу у системах підготовки персоналізованих матеріалів. Електронні інформаційні ресурси, №1, 2025.

3. Romano F. J. The Handbook for Digital Printing and Variable-Data Printing. Pittsburgh : PIA/GATF Press, 2004. 204 p.

4. Koehn P. Statistical Machine Translation. Cambridge : Cambridge University Press, 2010. 433 p.

5. Моісєєва Н., Дзикович О., Штанько А. Машинний переклад: порівняння результатів та аналіз помилок DeepL та Google Translate. Advanced Linguistics, Т. 11, 2023.

УДК 004.8:004.42:004.9

ПОЄДНАННЯ БІОМЕТРИЧНОЇ АВТЕНТИФІКАЦІЇ ТА ГІБРИДНОГО ШИФРУВАННЯ ДЛЯ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Роман МАСЛЯК[1], Ростислав ТКАЧУК[1,2], Наталія МАСЛОВА[2]
[1]Львівський державний університет безпеки життєдіяльності
[2]Національний університет «Львівська політехніка»

Анотація. *У роботі розглянуто розробку десктопної системи FaceLock для захисту файлів і папок, що поєднує біометричну автентифікацію на основі розпізнавання облич та гібридне шифрування (AES-256 + RSA-2048). Система реалізована з модульною архітектурою, яка охоплює компоненти відеоаналізу, розпізнавання облич, криптографії та графічного інтерфейсу, забезпечуючи масштабованість і надійність. Запропоноване рішення демонструє ефективне поєднання криптографічних і біометричних технологій, що відповідає сучасним вимогам до безпечного та зручного управління конфіденційною інформацією.*

Ключові слова: *FaceLock, біометрична автентифікація, розпізнавання облич, гібридне шифрування, AES-256, RSA-2048, захист даних, модульна архітектура, інформаційна безпека, десктопна система.*

Abstract*. The paper discusses the development of a desktop FaceLock system for protecting files and folders, combining biometric authentication based on facial recognition and hybrid encryption (AES-256 + RSA-2048). The system is implemented with a modular architecture that includes components of video analysis, facial recognition, cryptography and a graphical interface, ensuring scalability and reliability. The proposed solution demonstrates an effective combination of cryptographic and biometric technologies that meets modern requirements for secure and convenient management of confidential information.*

Keywords: *FaceLock, biometric authentication, facial recognition, hybrid encryption, AES-256, RSA-2048, data protection, modular architecture, information security, desktop system.*

Актуальність дослідження зумовлена стрімким зростанням обсягів цифрових даних та підвищенням ризиків їх несанкціонованого доступу, що робить традиційні паролі дедалі менш надійними через вразливість до підбору, фішингу та компрометації. Біометричні технології, зокрема розпізнавання обличчя, пропонують значно вищий рівень автентифікації. За сучасними даними, понад 60 % користувачів смартфонів застосовують біометричну автентифікацію, а серед молоді цей показник сягає 75 %. У практичних сферах — від банків до прикордонного контролю — біометричні системи показали високу ефективність, зменшуючи час перевірки та ризики шахрайства. Поєднання таких методів з криптографічним шифруванням файлів і папок, як у системі FaceLock, відповідає глобальній тенденції переходу до безпарольних, зручних і водночас стійких механізмів захисту даних [1, 2].

Пропонована система FaceLock, спрямована на підвищення рівня захисту конфіденційної інформації шляхом інтеграції гібридного шифрування

(AES-256 + RSA) та біометричної ідентифікації на основі розпізнавання облич, значно підвищить рівень безпеки даних, зменшить ризики несанкціонованого доступу та компрометації інформації, забезпечить персоналізований доступ для користувачів і дозволить ефективно застосовувати сучасні методи автентифікації у персональних та корпоративних IT-системах. Передбачається, що такий підхід забезпечить доступ до даних лише після успішної автентифікації користувача, що суттєво знизить ймовірність їхньої компрометації. Використання високоточних алгоритмів розпізнавання облич із середньою точністю понад 99 % на стандартних датасетах у поєднанні з надійним криптографічним захистом дозволить сформувати комплексну модель безпеки, ефективну як у персональних, так і в корпоративних сценаріях використання. Крім того, система забезпечить зручність користування, масштабованість і відповідність сучасним вимогам до захисту даних у різних IT-інфраструктурах, що робить її перспективним рішенням для підвищення надійності інформаційної безпеки в умовах зростання кіберзагроз [3].

Система реалізується з використанням сучасних бібліотек та інструментів: OpenCV і face_recognition для обробки зображень, SQLAlchemy і PostgreSQL для роботи з базою даних, PyQt5 для створення графічного інтерфейсу, а також багатопотокового механізму для паралельного виконання операцій розпізнавання та шифрування. Контейнеризація за допомогою Docker Compose забезпечує відтворюваність, ізоляцію та масштабованість середовища. Біометричні шаблони зберігаються у хешованому або зашифрованому вигляді у PostgreSQL, що відповідає сучасним вимогам кібербезпеки.

Порівняння з існуючими рішеннями — VeraCrypt, TrueCrypt та BitLocker — показало, що ці системи не підтримують інтегровану біометричну автентифікацію. FaceLock усуває це обмеження, об’єднуючи шифрування, розпізнавання облич, обробку відеопотоків у реальному часі та багаторівневий контроль доступу, що підкреслює інноваційність підходу та відповідає сучасним вимогам до комплексного захисту даних [4].

Архітектура системи має модульну будову та включає компоненти для захоплення і обробки відеопотоку, генерації й порівняння біометричних ознак, керування користувачами та виконання криптографічних операцій (рис. 1). Модулі працюють незалежно один від одного, що забезпечує масштабованість, можливість модифікації окремих елементів і стійкість системи до навантажень. Взаємодія між ними реалізована через стандартизовані запити, що спрощує інтеграцію нових функцій.

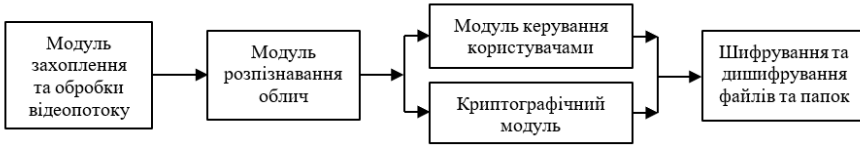

Рисунок 1 – Блок схема алгоритму архітектури системи

Гібридна схема шифрування даних передбачає використання алгоритму AES-256 для симетричного шифрування файлів, а симетричний ключ додатково кодується відкритим ключем RSA-2048 [5, 6]. Така комбінація забезпечує високу швидкодію при обробці великих обсягів даних і надійний захист ключової інформації навіть у разі часткової компрометації системи.

Реалізація системи передбачає графічний інтерфейс FaceLockApp, модуль обробки відеопотоку VideoStreamWorker, систему розпізнавання облич SimpleFaceRec та криптографічний модуль. Процес розпізнавання включає поетапне виявлення обличчя, обчислення дескрипторів і порівняння з базою даних. Реєстрація користувача включає зчитування біометричних ознак, генерацію криптографічних ключів і збереження публічного ключа разом із дескриптором обличчя. Доступ до шифрованих файлів можливий лише після успішної автентифікації користувача.

Отже FaceLock поєднує біометричну автентифікацію та гібридне шифрування, що забезпечує комплексний захист даних, модульну архітектуру для масштабованості та стабільну роботу системи. Інтеграція відеопотоків, розпізнавання облич і багаторівневий контроль доступу робить її інноваційним і практично придатним рішенням для безпечного управління конфіденційною інформацією.

Література

1. Yang, W., Wang, S., Cui, H., Tang, Z., & Li, Y. (2023). *A Review of Homomorphic Encryption for Privacy-Preserving Biometrics. Sensors,* 23(7), 3566. https://doi.org/10.3390/s23073566 MDPI

2. Пановик У. П., Ткачук Р. Л. Кібербезпека через призму системного аналізу. Комп'ютерні технології друкарства : зб. наук. пр. Львів : УАД, 2023. № 1 (49). С. 197–208. URL: https://doi.org/10.32403/2411-9210-2023-1-49-197-208 (index Copernicus International)

3. Боднар О., Лагун А. Е., Ткачук Р. Л. Виявлення небезпечних входжень у комп'ютерну мережу за допомогою систем виявлення вторгнень. Інформаційна безпека та інформаційні технології : зб. тез доповідей V Всеукраїнської науково-практичної конференції молодих учених, студентів і курсантів. (Львів, 26 листопада 2021 р.). Львів : ЛДУБЖД, 2021. С. 9–12.

4. Моравський В., Ткачук Р. Л., Колос Н. М. Криптологія: сучасні тенденції та перспективи. Інформаційна безпека та інформаційні технології : зб. тез доповідей VI Всеукраїнської науково-практичної конференції молодих учених, студентів і курсантів. (Львів, 30 листопада 2023 р.). Львів : ЛДУБЖД, 2023. С. 130–133.

5. Singh, S., Igene, L., & Schuckers, S. (2024). *Securing Biometric Data: Fully Homomorphic Encryption in Multimodal Iris and Face Recognition*. arXiv. https://arxiv.org/abs/2408.14609

6. Qin, Y., & Zhang, B. (2023). *Privacy-Preserving Biometrics Image Encryption and Digital Signature Technique Using Arnold and ElGamal*. *Applied Sciences,* 13(14), 8117. https://doi.org/10.3390/app13148117 MDPI

УДК 004.492.3+ 378.147

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ У ПУБЛІКАЦІЙНИХ ПЛАТФОРМАХ

Роман МОРОЗ
Національний університет «Львівська політехніка»

Виконано аналіз сучасних підходів до реалізації безпеки персональних даних у контексті публікаційних платформ. Розглянуто сценарії витоку даних на публікаційних платформах.Здійснено оцінку ефективності застосовуваних технічних та організаційних заходів щодо підвищення рівня захисту даних.
***Ключові слова**: персональні дані, публікаційні платформи, захист інформації, GDPR, інформаційна безпека, конфіденційність.*

An analysis of modern approaches to implementing personal data security in the context of publishing platforms was performed. Data leakage scenarios on publishing platforms were considered. The effectiveness of the applied technical and organizational measures to increase the level of data protection was assessed.
***Keywords**: personal data, publishing platforms, information protection, GDPR, information security, privacy.*

Захист персональних даних у сучасних публікаційних платформах є одним з найважливіших аспектів забезпечення довіри користувачів та гарантії дотримання нормативно-правових вимог. Публікаційні платформи, включно з електронними журналами, репозиторіями та системами управління науковими конференціями, обробляють широкий спектр персональних даних, включаючи ідентифікаційні дані користувачів, контактну інформацію, історію публікацій та аналітичні відомості про активність [1]. Актуальність проблеми обумовлена не тільки підвищеним ризиком несанкціонованого доступу до даних, але й потенційними наслідками для репутації платформ, авторів та установ, що їх підтримують. Незважаючи на наявність міжнародних стандартів, таких як Загальний регламент захисту даних ЄС (GDPR), а також національних законів про персональні дані, практика їх реалізації у контексті публікаційних платформ є неоднорідною і часто недостатньо ефективною [2].

Проблема захисту персональних даних у цифрових публікаційних системах привертає увагу дослідників у різних аспектах. З одного боку, акцент робиться на технічних механізмах безпеки, таких як шифрування даних, двофакторна автентифікація, контроль доступу та регулярні аудити активності користувачів. З іншого боку, увага приділяється організаційним заходам, включаючи розробку політик конфіденційності, інструкцій для користувачів та персоналу, а також впровадження процедур реагування на інциденти безпеки. У наукових публікаціях підкреслюється, що ефективний захист персональних даних можливий лише за умови комплексного підходу, який поєднує технічні засоби, організаційні процедури та нормативно-правове забезпечення. Окремі дослідження зосереджені на аналізі реальних випадків витоків даних

на платформених ресурсах, що дозволяє визначити слабкі місця в існуючих механізмах захисту та пропонувати удосконалення.

Найефективнішими підходами до захисту персональних даних є комплексні методи, які поєднують технічні, організаційні та нормативні засоби. Використання сучасних алгоритмів шифрування, зокрема AES та RSA, забезпечує високий рівень конфіденційності збережених даних. Двофакторна автентифікація та диференційовані права доступу дозволяють обмежити можливості несанкціонованого входу до системи. Організаційні заходи, такі як розробка чітких політик конфіденційності, інструкцій для персоналу та користувачів, навчання щодо безпечного поводження з даними, підвищують рівень обізнаності та відповідальності учасників платформи. Важливою складовою є регулярний аудит та моніторинг активності користувачів, що дозволяє виявляти підозрілі дії та реагувати на потенційні інциденти безпеки.

Головним викликом у сфері захисту персональних даних є баланс між доступністю інформації та її конфіденційністю. Публікаційні платформи прагнуть забезпечити зручність користування та відкритий доступ до наукових матеріалів, що ускладнює впровадження суворих механізмів контролю доступу. Крім того, постійне оновлення технологій та методів атак вимагає безперервного вдосконалення захисних заходів (рисунок).

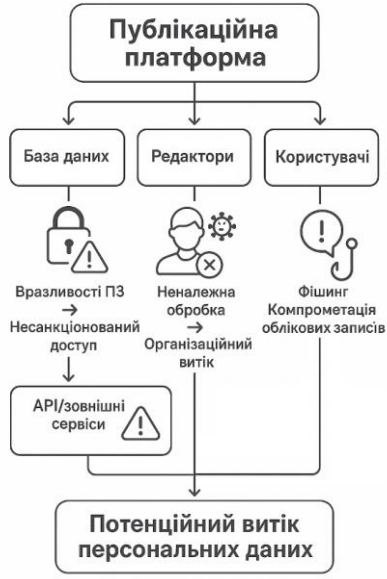

Рисунок 1 – Виклики у сфері захисту персональних даних користувачів публікаційних платформ

Аналіз міжнародного досвіду показує, що інтеграція правових вимог, таких як GDPR, у політики платформ, а також застосування сучасних технічних рішень дозволяє значно знизити ризики витоку даних. Водночас організаційні заходи, включно з навчанням персоналу та підвищенням обізнаності користувачів, є важливими для створення культури безпеки на платформі.

В умовах сучасних публікаційних платформ ризики витоку персональних даних проявляються у різних сценаріях, які можна класифікувати за типами загроз і каналами витоку. Таким чином, ефективний захист персональних даних у публікаційних платформах можливий лише за умови інтегрованого підходу, який включає регулярне тестування систем, шифрування даних, диференційовані права доступу, навчання персоналу, моніторинг активності користувачів та підвищення обізнаності користувачів щодо кіберзагроз. Така системна стратегія дозволяє мінімізувати ризики витоку та підтримувати довіру всіх учасників публікаційного процесу. Важливим напрямом для подальших робіт є розробка адаптивних механізмів безпеки, що враховують специфіку різних типів платформ та поведінку користувачів, а також інтеграція аналітичних інструментів для прогнозування та запобігання потенційним загрозам.

Література

1. Мороз Р. Обґрунтування доцільності розгортання автоматизованих видавничо-редакційних веб-платформ. Друкарство молоде, №25. С. 91-96.

2. Регламент Європейського Союзу 2016/679 (GDPR) про захист фізичних осіб у зв'язку з обробкою персональних даних та про вільний рух таких даних.

3. Moroz R. Enhancement of Security Mechanisms for an Open Information Platform Supporting the Publication of Scientific Research. Security of modern information and communication systems. С. 230-235.

УДК 004.056:628.19

ІНСТРУМЕНТАРІЙ СУЧАСНИХ МЕТОДИК ТА ТЕХНОЛОГІЙ ДЛЯ ПОБУДОВИ ЗАХИЩЕНИХ IOT СИСТЕМ

Валерій НЕДІЛЕНКО
Національний Університет "Львівська Політехніка"

Анотація: *Розроблено промисловий IoT-пристрій для моніторингу та запобігання витокам води з інтеграцією в AWS IoT Core, що підвищує безпеку зберігання та передачі даних завдяки сучасним методам шифрування та захисту від кіберзагроз. Реалізовано метод безпечного зберігання даних у Flash ESP32, авторизацію клієнтів у відкритому протоколі BLE, а також потокобезпечну реалізацію протоколу MQTT у середовищі FreeRTOS із підтримкою Over-the-Air (OTA) оновлень.*

Ключові слова: *Безпека даних, AWS IoT Core, Методи шифрування, Кібербезпека IoT-пристроїв, Апаратні та програмні рішення, ESP32, FreeRTOS.*

Abstract: *An industrial IoT device has been developed for water leak monitoring and prevention with integration into AWS IoT Core, which enhances the security of data storage and transmission through modern encryption methods and protection against cyber threats. Secure data storage in the ESP32 Flash memory has been implemented, along with client authorization in the open BLE protocol, as well as a thread-safe implementation of the MQTT protocol in the FreeRTOS environment with support for Over-the-Air (OTA) updates.*

Keywords: *Data Security, AWS IoT Core, Encryption Methods, IoT Device Cybersecurity, Hardware and Software Solutions, ESP32, FreeRTOS.*

В умовах постійного розвитку сучасних технологій та зростання попиту на інноваційні рішення захист від непередбачуваних ситуацій та небезпек стає критично важливим завданням [1]. Спостерігається різке зростання популярності розумних пристроїв та інтернету речей (IoT), які забезпечують зручність та ефективність в управлінні різноманітними пристроями та системами. У цьому контексті дослідницька робота присвячена розробці пристрою для захисту від протікання води, який використовує інфраструктуру Amazon Web Services (AWS) IoT Core.

Мета роботи полягає у вивченні доступних рішень та методик для розробки захищеної інформаційної системи для розумного будинку та розробці одного з елементів такої системи на прикладі приладу для контролю за витоком води.

Дослідження включає в себе не лише розробку апаратно-програмного комплексу, але й вивчення та аналіз відповідних аспектів кібербезпеки, зокрема у сфері захисту IoT-пристроїв від потенційних загроз та атак. Подальше вдосконалення та розширення можливостей захисту та взаємодії з AWS IoT Core є ключовими аспектами цього дослідження.

Проект поділений на 5 основних частин, рис. 1, де:

1) Основна програма – тут виконується керування моторизованими кранами, зчитування сигналів з давачів протікання, з лічильників, відбувається ініціалізація та об'єднання всіх модулів, запуск FreeRTOS завдань, також тут відбуваються усі операції пов'язані з пам'яттю.

2) Взаємодія з BLE – у цій частині проекту виконуються всі функції пов'язані з обміном даними по протоколу BLE, тут описано всі сервіси, дескриптори та характеристики GATT сервера, відбувається опрацювання вхідних даних з мобільного застосунку та генерація відповідей.

3) AWS IoT Core – тут описані всі функції які використовуються для підключення та взаємодії з MQTTS брокером AWS, тут же відбуваються операції по роботі з сертифікатам, ключами, авторизаційними даними, також читання та генерація JSON об'єктів відбувається тут.

4) OTA Updates – у цій частині проекту описана вся взаємодія з сервером оновлень OTA, відбувається опитування на наявність нових версій, завантаження бінарного коду, тимчасовий запис у розділ пам'яті OTA1 чи OTA2, перевірка цілісності коду, та переписуються дані завантажувача, для того щоб він запускав програму з новішою версією, якщо все пройшло вдало.

5) Взаємодія з радіопередавачем – тут знаходяться функції для керування радіопередачачем NRF 868MHz, який приймає команди по SPI, тут відбувається ініціалізація даного модуля, запис та зчитування даних у буфери FIFO, керування режимами передачі, також тут описаний власний протокол обміну даними, що забезпечує перевірку цілісності отриманих пакетів, RSSI (у разі завантаженості каналу, виконується автопідбір), опрацювання помилок та аварій.

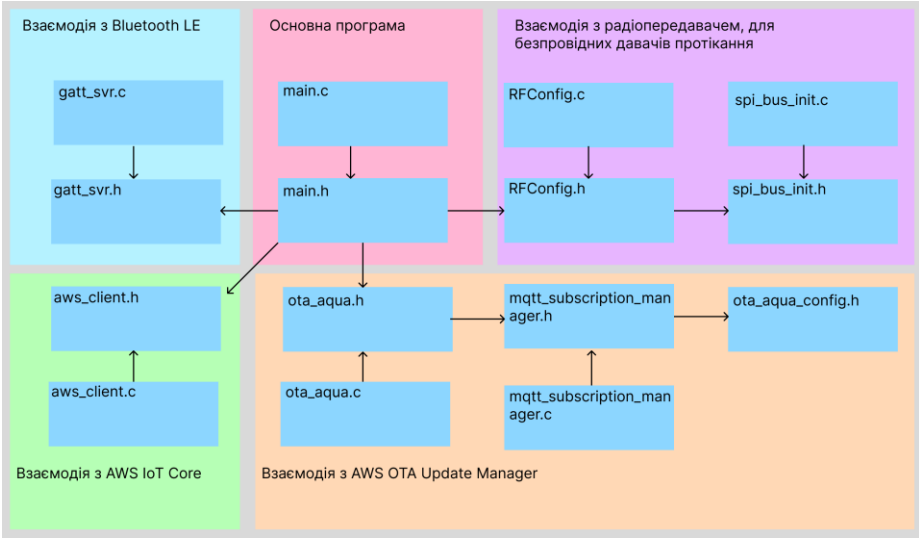

Рисунок 1 – Програмні компоненти реалізованого проєкту

В проєкті був використаний мікроконтролер ESP32, який має інтегровані контролери Wi-Fi і Bluetooth, низьке енергоспоживання і невисоку ціну. Для розробки додатків була застосована ESP-IDF офіційна опенсорсна платформа розробки IoT Espressif для серій SoC ESP32, ESP32-S, ESP32-C і ESP32-H. Зв'язок з роутером відбувався за протоколом Bluetooth Low Energy (BLE).

Проект враховує високі стандарти кібербезпеки, використовуючи сучасні методи шифрування та захисту від зламу. Практична реалізація системи підтверджує її ефективність та надійність в реальних умовах експлуатації, що підтверджено успішним впровадженням на базі двох приватних підприємств.

Література

1. Yang Zhang, Pengxiao Duan, Chaoyang Li, Hua Zhang Haseeb Ahmad. Preserving Privacy of Internet of Things Network with Certificateless Ring Signature Sensors 2025, 25(5), 1321; https://doi.org/10.3390/s25051321

УДК 004.75

ПІДХОДИ ДО МАСШТАБУВАННЯ ВЕБ-ДОДАТКІВ У ХМАРНИХ СЕРЕДОВИЩАХ AWS, AZURE ТА GOOGLE CLOUD

Миколай НЕДІЛЬСЬКИЙ
Львівський національний університет ветеринарної медицини та біотехнологій імені С.З. Ґжицького

Розглянуто сучасні підходи до масштабування веб-додатків у хмарних середовищах Amazon Web Services, Microsoft Azure та Google Cloud Platform. Проаналізовано моделі автоматичного масштабування, балансування навантаження, контейнеризації та безсерверних рішень. Визначено переваги та відмінності механізмів масштабування у провідних хмарних платформах.

***Ключові слова**: хмарні обчислення, масштабування, веб-додатки, AWS, Azure, GCP.*

The paper examines modern approaches to scaling web applications in cloud environments such as Amazon Web Services, Microsoft Azure, and Google Cloud Platform. It analyzes autoscaling models, load balancing mechanisms, containerization, and serverless solutions. The advantages and differences of scaling mechanisms in leading cloud platforms are identified.

***Keywords**: cloud computing, scaling, web applications, AWS, Azure, GCP.*

Стрімкий розвиток хмарних технологій формує нові підходи до проєктування та експлуатації веб-додатків, які повинні забезпечувати високу доступність, продуктивність та здатність динамічно реагувати на зміну навантаження. Масштабування є одним із ключових механізмів, що визначає надійність та ефективність сучасних інформаційних систем. Провідні хмарні платформи AWS, Azure та Google Cloud пропонують широкий спектр інструментів, які забезпечують автоматизацію, відмовостійкість та оптимізацію витрат.

Горизонтальне масштабування (scale-out) є найбільш гнучким і передбачає збільшення кількості екземплярів застосунку. У AWS цей процес реалізується за допомогою Auto Scaling Groups[1], в Azure — через Virtual Machine Scale Sets[2], а у GCP — Managed Instance Groups. Ці сервіси працюють на основі політик, що враховують метрики навантаження (CPU, RAM, кількість запитів), забезпечуючи своєчасну реакцію на пікові навантаження та оптимальне використання ресурсів.

Важливою складовою масштабованих систем є балансування навантаження. AWS Elastic Load Balancer, Azure Application Gateway та Google Cloud Load Balancer дозволяють рівномірно розподіляти запити між серверами, зменшувати затримки та підвищувати відмовостійкість. GCP відрізняється глобальним балансувальником, який працює на рівні всієї інфра-

структури Google і забезпечує маршрутизацію запитів у найближчий регіон без додаткових налаштувань.

Контейнеризація та оркестрація стали стандартом у розробці масштабованих застосунків. Kubernetes-платформи — Amazon EKS, Azure Kubernetes Service та Google Kubernetes Engine [3] — забезпечують автоматичне масштабування контейнерів, відновлення подів, оновлення без простоїв та розподіл навантаження. Google GKE є однією з найоптимізованіших платформ завдяки високому рівню інтеграції з інфраструктурою Google.[4]

Безсерверні обчислення (serverless) розширюють можливості масштабування, усуваючи необхідність керувати серверами. AWS Lambda, Azure Functions та Google Cloud Functions запускують код лише у відповідь на події, автоматично масштабуються та дозволяють зменшувати витрати завдяки моделі оплати за фактичне виконання. Для контейнеризованих serverless-рішень застосовуються Google Cloud Run, AWS Fargate та Azure Container Apps.

Порівняння платформ показує, що AWS має найбільшу кількість сервісів та гнучкість у виборі архітектурних рішень; Azure є оптимальною платформою для корпоративного сектору та інтеграції з екосистемою Microsoft; GCP забезпечує найефективніші рішення для контейнерних навантажень та глобальних розподілених систем. Вибір платформи залежить від вимог до продуктивності, географії користувачів та бюджету.

Таким чином, підходи до масштабування у хмарних середовищах базуються на поєднанні інструментів автоматичного масштабування, балансування навантаження, контейнеризації та serverless-архітектур. Їхнє раціональне використання дозволяє забезпечити високу доступність вебдодатків та оптимізувати витрати на інфраструктуру, що є критично важливим для сучасних інформаційних систем будь-якого масштабу.

Література

1. Amazon Web Services. Auto Scaling Documentation. [Електронний ресурс] – Режим доступу: https://docs.aws.amazon.com/autoscaling/

2. Microsoft Azure Architecture Center. Scalability Patterns. [Електронний ресурс] – Режим доступу: https://learn.microsoft.com/en-us/azure/architecture/patterns/category/scalability

3. Google Cloud Platform. Compute and Scaling Services Overview. [Електронний ресурс] – Режим доступу: https://cloud.google.com/compute/docs; https://cloud.google.com/solutions/scaling-your-applications

4. Hightower K., Burns B., Beda J. Kubernetes: Up and Running. URL: https://www.oreilly.com/library/view/kubernetes-up-and/9781492046523/

НЕБЕЗПЕКИ ІНФОРМАЦІЇ У ХМАРНИХ СХОВИЩАХ: ПРИЧИНИ ВИНИКНЕННЯ ТА СПОСОБИ ЗАХИСТУ

ОБРОЦЬКА Н.М, ВІНТЮК Ю.В
Львівський державний університет безпеки життєдіяльності

Анотація. У роботі розглянуто основні небезпеки використання хмарних сховищ, такі як шкідливе програмне забезпечення, несанкціонований доступ та витоки даних. Проаналізовано технічні, людські та організаційні чинники виникнення загроз. Запропоновано ключові методи захисту: багаторівнева автентифікація, шифрування, контроль доступу та резервування даних.

Ключові слова: *хмарні сховища, безпека даних, витік інформації, ransomware, автентифікація, шифрування.*

Abstract. This paper examines the main risks associated with the use of cloud storage, such as malicious software, unauthorized access, and data breaches. Technical, human, and organizational factors contributing to these threats are analyzed. Key protection methods are proposed, including multi-factor authentication, encryption, access control, and data backup.

Keywords: *cloud storage, data security, information leakage, ransomware, authentication, encryption*

Вступ

Хмарні сховища стали невід'ємним інструментом у роботі приватних користувачів, бізнесу та державних установ. Завдяки простоті доступу, можливості синхронізації та масштабованості вони забезпечують швидкий обмін даними та централізоване зберігання великих масивів інформації. Проте зростання популярності таких сервісів супроводжується збільшенням випадків втрати даних та кібератак.

Актуальність теми підтверджується статистикою: за даними аналітичних досліджень 2024 року понад 450 млн записів було викрадено або скомпрометовано саме у хмарних середовищах, а збитки від атак ransomware перевищили 11 млрд доларів США. Хмарні сервіси дедалі частіше стають мішенню кіберзлочинців через високу концентрацію персональних і корпоративних даних, що створює потребу у поглибленому дослідженні вразливостей та ефективних методів захисту.

Мета роботи

Метою роботи є аналіз основних небезпек, характерних для хмарних сховищ, визначення причин їх виникнення та опис практичних способів забезпечення безпеки даних.

Основний зміст

Однією з найнебезпечніших загроз є шкідливе програмне забезпечення, зокрема ransomware. Після зараження зловмисники шифрують дані та вимагають викуп за відновлення доступу. Хмарні системи часто стають

мішенню через концентрацію великої кількості важливої та конфіденційної інформації.

Другою поширеною проблемою є несанкціонований доступ. Він виникає через використання слабких паролів, повторення одного пароля на різних сервісах, помилки у налаштуваннях спільного доступу або викрадення облікових даних. Навіть один некоректно налаштований файл може призвести до масштабного витоку інформації.

До основних причин виникнення загроз належать:

Технічні вразливості — програмні помилки, недостатньо захищені системи автентифікації, часткове шифрування даних.

Людський фактор — нехтування базовими правилами безпеки, відкриття доступу стороннім особам, завантаження підозрілих файлів.

Недостатній рівень захисту облікових записів — відсутність двофакторної автентифікації, рідкісна зміна паролів, ігнорування системних повідомлень про підозрілу активність.

Зменшення ризиків можливе лише за умови комплексного підходу до безпеки. До основних заходів належать:

- багаторівнева (двох- чи трьохфакторна) автентифікація;
- регулярний перегляд дозволів і контроль доступу до файлів;
- шифрування даних перед завантаженням у хмару;
- резервне копіювання на окремих носіях;
- оновлення програмного забезпечення та перевірка журналів активності.

Результати власного дослідження

З метою аналізу практик користувачів щодо захисту інформації у хмарних сховищах було проведено соціологічне опитування серед мешканців Рясного. Усього опитано 57 людей віком 18–35 років.

Учасникам запропонували відповісти на запитання щодо досвіду використання хмарних сервісів, випадків втрати даних та застосування засобів захисту.

Основні результати опитування:

- 59% респондентів хоча б раз втрачали файли або доступ до них у хмарних сервісах;
- 38% отримували повідомлення про спроби входу з невідомих пристроїв;
- Лише 26% користуються двофакторною автентифікацією;
- Лише 17% регулярно (раз на пів року або частіше) перевіряють налаштування доступу до своїх документів;
- 72% зазначили, що потребують додаткових знань у сфері кібергігієни.

Отримані дані свідчать, що більшість користувачів недооцінюють ризики, пов’язані з використанням хмарних сховищ, та недостатньо застосо-

вують ефективні засоби захисту. Це підвищує ймовірність витоків інформації та несанкціонованого доступу.

Висновок

Хмарні сховища є зручним інструментом зберігання інформації, проте їх використання пов'язане з низкою небезпек: шкідливими програмами, витоками даних та несанкціонованим доступом. Основними чинниками ризику є технічні вразливості та помилки користувачів. Проведене дослідження підтверджує, що серед молоді рівень цифрової безпеки залишається недостатнім. Для забезпечення захисту даних у хмарних сховищах необхідно застосовувати багаторівневу автентифікацію, шифрування та контроль прав доступу.

Література

1. Скоринович, Б. В., Лах, Ю. В. *Аналіз методів моніторингу стану безпеки в хмарному середовищі*. — Сучасний захист інформації, 2025, № 1, с. 12–25.

2. Дакова, Л. В., Даков, С. Ю., Блаженний, Н. В. *Механізми безпеки в хмарному середовищі на базі міжнародних стандартів*. — Зв'язок, 2022, с. 45–56.

3. Дейнека, О. Р. *Аналіз сучасних тенденцій та підходів до надійного і захищеного зберігання великих даних*. — CSN (Наукові журнали та конференції), 2025, Вип. 7, № 1, с. 106–118.

УДК 004.056.5:004.77:66.013-027.22

ДЕЦЕНТРАЛІЗОВАНИЙ КОНТРОЛЬ ДОСТУПУ ДЛЯ ЦИФРОВИХ ДВІЙНИКІВ НА ОСНОВІ СМАРТ-КОНТРАКТІВ

Дмитро ОВСЯНКО
Національний Університет "Львівська Політехніка"

Анотація: *Розглянуто проблеми безпеки розподілених екосистем цифрових двійників, зокрема обмеження традиційних централізованих моделей контролю доступу. Розглянуто потенціал блокчейн-технологій і смарт-контрактів як децентралізованої альтернативи, проаналізовано їхні переваги, обмеження та перспективи застосування гібридних архітектур у критично важливих галузях.*

Ключові слова: *цифрові двійники, блокчейн, смарт-контракти, контроль доступу, децентралізація, RBAC, ABAC, інформаційна безпека, конфіденційність даних, розподілені системи, Ethereum, Hyperledger Fabric, гібридні архітектури*

Abstract: *The paper considers the security issues of distributed digital twin ecosystems, in particular the limitations of traditional centralized access control models. The potential of blockchain technologies and smart contracts as a decentralized alternative is considered, and their advantages, limitations, and prospects for the application of hybrid architectures in critical industries are analyzed.*

Keywords: *digital twins, blockchain, smart contracts, access control, decentralization, RBAC, ABAC, information security, data privacy, distributed systems, Ethereum, Hyperledger Fabric, hybrid architectures*

Цифрові двійники – це віртуальні моделі фізичних об'єктів і процесів, що відтворюють їхній стан та динаміку в режимі реального часу, та на сьогоднішній день широко застосовуються у критично важливих сферах. Зі зростанням ступеня розподіленості та взаємозв'язку таких систем посилюються загрози, пов'язані з безпекою даних, керуванням доступом і захистом приватності користувачів. Наявні централізовані рішення вже не забезпечують належного рівня конфіденційності, довіри та можливості аудиту в динамічних, децентралізованих середовищах. Традиційні розподілені системи використовують механізми контролю доступу RBAC (Role-Based Access Control) та ABAC (Attribute-Based Access Control). RBAC визначає права доступу на основі організаційних ролей, тоді як ABAC враховує атрибути користувача, ресурсу та умови середовища. Незважаючи на широке застосування в корпоративних системах і хмарних платформах, обидві моделі виявляють обмежену придатність для динамічних децентралізованих середовищ, зокрема IoT та екосистем цифрових двійників. Автентифікація в таких системах традиційно реалізується через централізовані сервери із застосуванням протоколів OAuth 2.0 або JSON Web Token (JWT). Проте ця архітектура формує єдину точку відмови та розширює поверхню атаки, особливо у сценаріях із множинними незалежними джерелами даних і учасниками.

Блокчейн-технології пропонують децентралізовану альтернативу традиційним моделям безпеки, забезпечуючи незмінність реєстрів і децен-

тралізований консенсус без потреби в центральних системах керування. Смарт-контракти на платформах Ethereum, Hyperledger Fabric та Polkadot функціонують як автономні агенти, що виконують код за визначених умов, дедалі частіше застосовуючись для децентралізованого контролю доступу та управління цифровими активами [1]. Проте блокчейн-системи мають суттєві обмеження: відкритість транзакцій у публічних мережах суперечить вимогам конфіденційності; високі витрати на газ для складних операцій; незмінність смарт-контрактів обмежує їхню адаптивність після розгортання. Для вирішення цих проблем застосовують гібридні моделі, що поєднують мережеві смарт-контракти з позамережевим сховищем (IPFS, Filecoin), хоча це підвищує архітектурну складність [2]. Перспективність інтеграції блокчейн з цифровими двійниками демонструє дослідження "Blockchain-enabled digital twin system for brain stroke prediction" [3]. Запропонована модель поєднує машинне навчання з консорціумною блокчейн-технологією для прогнозування ризику інсульту, забезпечуючи незмінність даних, виявлення спроб фальсифікації та автоматичне відновлення оригінальних значень. Масштабована архітектура дозволяє адаптувати систему до інших патологій без зміни коду та підтримує інтеграцію носимих медичних пристроїв, що критично важливо для впровадження цифрових двійників у охороні здоров'я.

Традиційні централізовані моделі контролю доступу виявляють критичні обмеження у забезпеченні безпеки розподілених екосистем цифрових двійників, формуючи єдину точку відмови та розширюючи поверхню атаки. Блокчейн-технології та смарт-контракти пропонують перспективну децентралізовану альтернативу, забезпечуючи незмінність реєстрів і автономне виконання політик безпеки, проте їхнє впровадження супроводжується викликами масштабованості, конфіденційності та адаптивності. Подальші дослідження мають зосередитись на розробці гібридних архітектур, що балансують вимоги безпеки, конфіденційності та продуктивності у критично важливих галузях.

Література

1. A Digital Twin Approach for Blockchain Smart Contracts / F. Corradini et al. *2024 IEEE International Conference on Software Analysis, Evolution and Reengineering - Companion (SANER-C)*, Rovaniemi, Finland, 12 March 2024. 2024. P. 1–7. URL: https://doi.org/10.1109/saner-c62648.2024.00007.

2. Овсянко Д., Нємкова. О. СМАРТ-КОНТРАКТИ ЯК МЕХАНІЗМИ ЗАБЕЗПЕЧЕННЯ ПРИВАТНОСТІ В РОЗПОДІЛЕНИХ СИСТЕМАХ ЦИФРОВИХ ДВІЙНИКІВ. *Кібербезпека: освіта, наука, техніка*. 2025. Т. 1, № 29. С. 107–123. URL: https://doi.org/10.28925/2663-4023.2025.29.867.

3. Upadrista V., Nazir S., Tianfield H. Blockchain-enabled digital twin system for brain stroke prediction. *Brain Informatics*. 2025. Vol. 12, no. 1. URL: https://doi.org/10.1186/s40708-024-00247-6.

УДК 004.738.5:004.056.55

ІНТЕГРАЦІЯ БЛОКЧЕЙН-ТЕХНОЛОГІЙ ДЛЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ IoT-МЕРЕЖ

Роман ПАДЮКА, Богдан ДУДКО, Роман ШАПОВАЛ
Львівський національний університет ветеринарної медицини та біотехнологій імені С.З. Гжицького

Анотація. *У роботі досліджено можливості інтеграції блокчейн-технологій у системи Інтернету речей (IoT) з метою забезпечення безпеки, цілісності та стійкості даних. Описано архітектуру блокчейну, особливості Merkle-дерев, моделі дозволених і недозволених реєстрів, а також перспективні технології на кшталт IOTA.*
Ключові слова: *блокчейн, IoT, безпека, Merkle-дерево, IOTA, децентралізація.*

Abstract. *The paper examines the integration of blockchain technologies into Internet of Things (IoT) systems to enhance security, data integrity and resilience. It outlines blockchain architecture, Merkle trees, permissioned and permissionless models, and discusses future technologies such as IOTA for resource-constrained IoT devices.*
Keywords: *blockchain, IoT security, Merkle tree, distributed ledger, IOTA.*

Стрімке зростання Інтернету речей (IoT) супроводжується збільшенням обсягів чутливих даних, передаваних між пристроями, що підсилює актуальність проблеми безпеки. IoT-мережі складаються з великої кількості гетерогенних пристроїв, які отримують, обробляють та передають дані в реальному часі. Однак традиційні централізовані моделі зберігання й обробки інформації, переважно засновані на хмарних серверах, мають низку істотних недоліків: наявність єдиної точки відмови, підвищену вразливість до кібератак, загрозу спуфінгу та підробки даних, а також обмежені можливості масштабування.

У цьому контексті блокчейн виступає перспективним підходом для забезпечення прозорості, стійкості та недоторканності даних IoT. Блокчейн є розподіленим децентралізованим реєстром, записи якого пов'язані між собою криптографічними хешами та впорядковані хронологічно. Основою структури даних є Merkle-дерево, у якому кожна транзакція хешується, а отримані значення рекурсивно об'єднуються у кореневий хеш. Зміна хоча б одного запису спричиняє модифікацію всіх пов'язаних хешів, що робить фальсифікацію даних практично неможливою.

Механізм додавання нових блоків здійснюється за участю майнерів або валідаторів, які перевіряють транзакції й формують новий блок за допомогою консенсусних алгоритмів (Proof-of-Work, Proof-of-Stake, Practical Byzantine Fault Tolerance тощо). Майнер не має доступу до персональних даних користувача, оскільки працює виключно з криптографічними представленнями транзакцій, що підвищує конфіденційність мережі.

Залежно від моделі доступу блокчейни поділяють на дозволені (permissioned) та недозволені (permissionless). Недозволені блокчейни, такі як Bitcoin чи Ethereum, допускають участь будь-якого вузла. Це забезпечує високу децентралізацію, але водночас знижує пропускну здатність. Дозволені блокчейни, представлені Hyperledger Fabric або Ripple, працюють із попередньо визначеним набором учасників, забезпечуючи вищу продуктивність, чіткий контроль доступу та відповідність вимогам корпоративних IoT-систем.

У системах IoT блокчейн вирішує низку критичних проблем безпеки. По-перше, він дозволяє зберігати дані в розподіленому реєстрі, мінімізуючи ризик централізованих атак та втрати інформації. По-друге, механізм хешування унеможливлює модифікацію даних непомітним чином, а перевірка валідаторами гарантує правильність записів. По-третє, автентифікація між пристроями може здійснюватися без центрального сервера сертифікації, що істотно знижує загрозу спуфінгу. Такий підхід забезпечує довіру між вузлами мережі та підсилює загальний рівень захищеності.

Особливої уваги заслуговує проблема обмежених обчислювальних ресурсів IoT-пристроїв. Зберігання повної копії блокчейну є ресурсомістким, тому досліджуються архітектури із застосуванням проксі-вузлів, що виконують функції зберігання й обробки даних, тоді як IoT-пристрої працюють лише з легкими хеш-значеннями. Це дозволяє інтегрувати блокчейн-технології навіть у малопотужні сенсорні мережі.

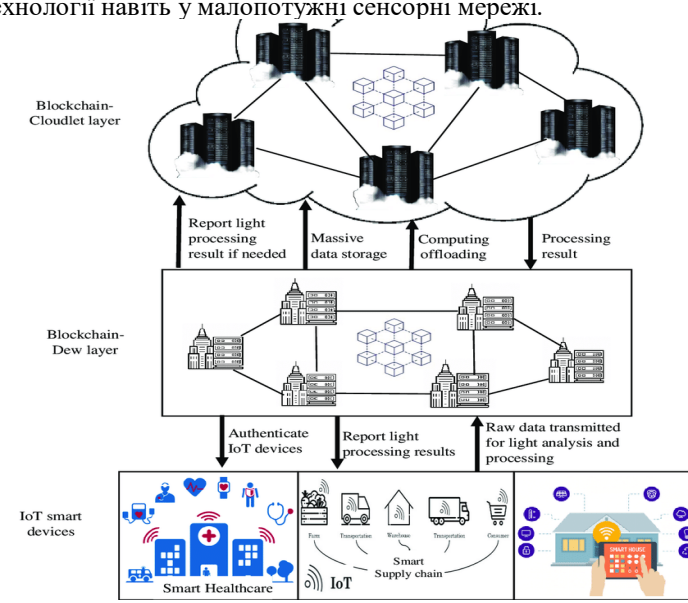

Рисунок 1 – Узагальнена архітектура інтеграції блокчейну у IoT-мережі

Іншим перспективним напрямом є використання розподілених реєстрів нового покоління, зокрема технології IOTA. На відміну від класичного блокчейну, IOTA використовує Directed Acyclic Graph (DAG), відомий як Tangle. Кожен новий запит у мережі підтверджує два попередні, що усуває необхідність у майнерах та забезпечує надзвичайно низьку комісію за транзакції. Це робить IOTA максимально придатною для великих IoT-мереж із високою частотою дрібних транзакцій.

Узагальнену концептуальну архітектуру інтеграції блокчейну в IoT-системи наведено на рисунку. У ній відображено взаємодію пристроїв IoT із розподіленим реєстром, участь проксі-вузлів, хмарних компонентів та сервісів аналізу даних.

Отже, інтеграція блокчейн-технологій у сферу IoT є ефективним шляхом до створення стійких, безпечних і прозорих мереж, що здатні протистояти широкому спектру сучасних кіберзагроз. Поєднання криптографічного захисту, децентралізації та можливостей розподілених реєстрів відкриває можливості для формування нових архітектур інтелектуальних систем, які не залежать від централізованої інфраструктури та здатні забезпечити високий рівень довіри між пристроями.

УДК 004.056:681.518:531.787

ЗАБЕЗПЕЧЕННЯ КІБЕРЗАХИСТУ ТА ДОСТОВІРНОСТІ ВИМІРЮВАЛЬНОЇ ІНФОРМАЦІЇ В АВТОМАТИЗОВАНИХ СИСТЕМАХ МОНІТОРИНГУ ВИРОБНИЧИХ ПРОЦЕСІВ

Уляна ПАНОВИК[1,2], Роман ГІДЕЙ[2], Валерія БАЛАЦЬКА[1]
[1] Львівський державний університет безпеки життєдіяльності
[2] Національний університет «Львівська політехніка»

Анотація. *Запропоновано інформаційно-алгоритмічну модель кіберзахисту та достовірності вимірювальної інформації в автоматизованих системах моніторингу виробничих процесів. Розроблено модуль довіри для перевірки автентичності, цілісності й метрологічної узгодженості даних. Моделювання підтвердило підвищення індексу цілісності до 0,98 і скорочення часу виявлення спотворень. Результати можуть бути впроваджені в автоматизованих системах моніторингу для підвищення надійності контролю.*

Ключові слова: *кіберзахист, достовірність даних, модуль довіри, метрологічна узгодженість.*

Abstract. *An information and algorithmic model for cybersecurity and measurement data reliability in automated production monitoring systems has been proposed. A trust module was developed to verify data authenticity, integrity, and metrological consistency. Simulation confirmed an increase in the integrity index to 0.98 and a reduction in distortion detection time. The results can be implemented in automated monitoring systems to improve control reliability.*

Keywords: *cybersecurity, data reliability, trust module, metrological consistency.*

Зі збільшенням кількості сенсорів у промислових мережах зростає обсяг вимірювальної інформації, від якої залежить якість управлінських рішень. Відкритість мережевих протоколів і відсутність комплексного метрологічно-кіберзахисного підходу створюють ризики спотворення даних — як навмисного (кібератаки, фальсифікація), так і випадкового (похибки, шуми). Традиційні засоби кіберзахисту не враховують метрологічні параметри, а класичний метрологічний контроль — автентичність джерел і цілісність потоку. Тому необхідна інтеграція метрологічного та кібернетичного підходів для забезпечення точності, автентичності й довіри до даних. У сучасних дослідженнях ця проблема розглядається в межах концепції *trusted sensing*, що поєднує метрологічну достовірність із криптографічною перевіркою даних (хешування, цифрові підписи, блокчейн). Попри наявність стандартів ISO/IEC 27019, IEC 62443 і NIST SP 800-82, поки не існує інтегрованої моделі, яка одночасно враховувала б точність вимірювань, стійкість каналів і автентичність сенсорів [1, 2].

Метою дослідження є розроблення інформаційно-алгоритмічної моделі, що поєднує метрологічні показники точності (похибка, стабільність,

повторюваність) із параметрами кіберзахисту (цілісність, автентичність, стійкість каналу), формуючи єдиний критерій довіри до даних. У моделі використано узагальнений показник достовірності вимірювальної інформації, який відображає взаємозв'язок метрологічної точності, автентичності джерела, цілісності потоку та стійкості каналу до атак. Для його практичного обчислення застосовується індекс довіри Td, що визначає рівень надійності кожного пакета даних. Отже, поставлене завдання полягає у розробленні алгоритму функціонування модуля довіри, який забезпечує автоматичну оцінку *Td* у реальному часі та прийняття рішення щодо достовірності кожного вимірювального пакета (рис. 1).

Рисунок 1 – Алгоритм функціонування модуля довіри до сенсорних даних

Розроблена інформаційно-алгоритмічна модель підвищує достовірність вимірювальної інформації шляхом інтеграції метрологічних і кіберзахисних механізмів у структурі автоматизованої системи моніторингу. Система реалізована як багаторівнева архітектура, де дані сенсорів проходять етапи фільтрації, перевірки автентичності, контролю цілісності та оцінювання довіри. Основний контур даних має вигляд: сенсори → контролер → агент шифрування → агрегатор → модуль довіри → база даних → інтерфейс користувача. Сенсори зчитують фізичні параметри, контролер оцифровує сигнали та передає їх до каналу зв'язку. Агент шифрування захищає інформацію за допомогою AES-256 або RSA, агрегатор об'єднує потоки з різних сенсорів і надсилає їх у модуль довіри. Центральний елемент — модуль довіри (Trust Module) — виконує перевірку автентичності, цілісності та метрологічної узгодженості даних. База даних зберігає первинні та перевірені значення разом із журналом подій, забезпечуючи контроль змін і рівня достовірності. Модуль довіри виконує п'ять основних функцій: перевірку автентичності сенсорів, контроль метрологічної узгодженості, перевірку цілісності, оцінку рівня довіри та прийняття рішення. Для кожного сенсора використовується криптографічний ідентифікатор, що запобігає підміні. Цілісність даних контролюється через хешування (SHA-256), а метрологічна узгодженість перевіряється за статистичними критеріями. На основі цих параметрів формується індекс довіри Td: високі значення свідчать про достовірність даних, нижчі — про необхідність повторної перевірки. Модуль забезпечує оперативну оцінку достовірності вимірювань у реальному часі.

Для перевірки ефективності запропонованої моделі проведено імітаційне моделювання у середовищі Python. Дослідження охоплювало два сценарії: нормальний режим роботи — передавання достовірних сенсорних даних без спотворення; атака на сенсорну мережу — випадки підміни даних та змін хеш-кодів пакетів. На вхід подавався масив із 10 000 вимірювальних точок, кожна з яких мала власні параметри похибки, контрольної суми та позначку автентичності. Для кожного пакета обчислювався індекс довіри Td за формулою: $Td = w_1(1 - /E_m/) + w_2 I_c + w_3 A_s + w_4 S_t$, де вагові коефіцієнти w_i приймали значення 0,25 для рівномірного впливу чинників. Порівняльні результати подано у таблиці.

Таблиця – Результати моделювання ефективності модуля довіри

Показник	**Без модуля довіри**	**З модулем довіри**	**Поліпшення**
Частка спотворених даних, E_m %	12 %	2 %	−10 %
Середній час виявлення спотворень, S_t с	7,4	2,3	в 3 рази швидше
Індекс цілісності *Ic*	0,87	0,98	+12,6 %
Коефіцієнт довіри *Td*	0,82	0,96	+17,1 %
Кількість відхилених пакетів A_s (із 10 000)	1180	210	−82 %

Результати свідчать, що використання модуля довіри суттєво підвищує достовірність сенсорних даних та знижує ризик прийняття некоректних рішень у виробничій системі. У нормальному режимі коефіцієнт довіри перевищує 0,95, а при моделюванні атаки система коректно відхиляє більшість спотворених пакетів. Застосування алгоритму на рівні агрегатора дозволяє проводити валідацію у реальному часі без впливу на швидкодію моніторингу.

У ході дослідження розроблено інформаційно-алгоритмічну модель кіберзахисту та достовірності вимірювальної інформації, що поєднує метрологічні критерії з механізмами безпеки. Центральним елементом є модуль довіри, який перевіряє автентичність, цілісність і метрологічну узгодженість даних у реальному часі. Моделювання показало підвищення індексу цілісності до 0,98 і скорочення часу виявлення спотворень, що підтверджує ефективність підходу та його придатність для IoT- і CPS-систем моніторингу виробництва.

Література

1. Janakiraman S. CYBER SECURITY FOR INDUSTRIAL AUTOMATION & CONTROL SYSTEMS. *Oil and Gas Business*. 2024. No. 1. P. 176–194. URL: https://doi.org/10.17122/ogbus-2024-1-176-194

2. Пановик У., Гідей Р. Математичне моделювання процесу агрегації та обробки вимірювальної інформації в автоматизованих метрологічних системах моніторингу. Вимірювальна та обчислювальна техніка в технологічних процесах, 2025. 82(2), с. 37–44. URL: https://doi.org/10.31891/2219-9365-2025-82-6

УДК 004.056.5:378.1

ІМІТАЦІЙНЕ МОДЕЛЮВАННЯ КІБЕРЗАХИЩЕНОСТІ МОДЕЛІ НАВЧАЛЬНО-МЕТОДИЧНОГО КОМПЛЕКСУ ОСВІТНЬОГО ПРОЦЕСУ

Уляна ПАНОВИК[1,2], Богдана ФЕДИНА[1,2], Роман ПАНОВИК[2]
[1]Львівський державний університет безпеки життєдіяльності,
[2]Національний університет «Львівська політехніка»

Анотація. *Подано методику імітаційного моделювання кіберзахищеності навчально-методичного комплексу (НМК) у середовищі Python + SimPy. Модель відтворює сценарії атак і відмов, оцінює стійкість системи та ефективність заходів безпеки. Результати моделювання і розрахунку ключових метрик підтвердили ефективність моніторингу, двофакторної автентифікації та резервування бази даних, що дає змогу оптимізувати архітектуру освітніх інформаційних систем.*

Ключові слова: *імітаційне моделювання, кіберзахищеність, навчально-методичний комплекс.*

Abstract. *A methodology for simulation modeling of the cybersecurity of the educational-methodical complex (EMC) in the Python + SimPy environment is presented. The model reproduces attack and failure scenarios, assesses system resilience and the effectiveness of security measures. The obtained results and calculated key metrics confirmed the efficiency of monitoring, two-factor authentication, and database backup, allowing optimization of the architecture of educational information systems.*

Keywords: *simulation modeling, cybersecurity, educational-methodical complex.*

Освіта активно переходить у цифровий формат, де більшість процесів здійснюється через автоматизовані платформи. Зростання кіберзагроз робить захищеність даних ключовим аспектом цифрової трансформації вищої освіти. Навчально-методичні комплекси (НМК) містять значні обсяги чутливої інформації, тому рівень їхньої безпеки варто оцінювати ще на етапі проєктування. Метою дослідження є створення імітаційної моделі подій безпеки та аналіз стійкості НМК до типових кіберзагроз. Практика показує, що безпеку освітніх систем часто враховують уже після запуску, тому необхідні інструменти для попередньої оцінки їхньої кіберстійкості. Попередні дослідження авторів стали основою запропонованого підходу. У [2] розглянуто імітаційне моделювання процесів управління освітнім середовищем, що підтвердило ефективність симуляційного аналізу потоків даних у ВНЗ, а міжнародні роботи [3] демонструють доцільність використання моделювання для оцінки ризиків кібербезпеки освітніх платформ. Водночас не проводилась оцінка захищеності архітектури НМК і не розглядалися сценарії атак чи відмов. Тому імітаційне моделювання є доціль-

ним інструментом для оцінювання кіберстійкості освітніх систем, оскільки дає змогу виявляти вразливості ще на етапі проєктування.

Навчально-методичний комплекс (НМК) є основою управління освітнім процесом, поєднуючи навчальні програми, методичні матеріали та цифрові інструменти моніторингу. Він складається з трьох підсистем — нормативно-методологічної, методологічної та інфраструктурно-організаційної, які взаємодіють у межах єдиної архітектури. Ключові точки контролю безпеки охоплюють модуль автентифікації, API-з'єднання, базу даних і канали обміну, що є потенційно вразливими до атак типу brute-force, SQL-ін'єкцій, несанкціонованого доступу та перехоплення даних. Для аналізу взаємодії компонентів НМК створено Data Flow Diagram, що відображає рух даних між підсистемами та визначає потенційно вразливі точки. На її основі побудовано карту ризиків (рис. 1), яка охоплює спроби несанкціонованого доступу, перевантаження серверів, втрату чи підміну даних і відмови сервісів.

Для оцінювання кіберзахищеності навчально-методичного комплексу (НМК) створено імітаційну модель, що відтворює взаємодію користувачів, серверів і бази даних за умов навантаження та кіберзагроз. Моделювання виконано у Python з використанням бібліотеки SimPy, яка забезпечує подійне середовище для опису паралельних процесів, управління ресурсами та вимірювання часових параметрів. Такий підхід дозволяє дослідити не лише роботу системи в нормальному режимі, а і її поведінку під час атак або відмов компонентів. Модель охоплює п'ять сценаріїв: нормальну роботу, несанкціонований доступ (brute force, SQL-injection), перевантаження серверів (DoS), відмову бази даних та відновлення після інциденту із залученням резервних механізмів і поверненням системи до стабільного стану.

Імітаційний алгоритм моделі (рис. 2) реалізує подійний цикл, у якому після ініціалізації середовища SimPy створюються основні ресурси — пул серверів (server_pool) та база даних (db). Запускаються два генератори: користувачів і атак, що формують потоки подій різної інтенсивності. Усі події надходять до блоку Dispatcher, який визначає їх тип — звичайний запит чи атака. Якщо сервер вільний, запит обробляється; за перевантаження — потрапляє в чергу або тайм-аут. Для атак визначається тип загрози (brute, SQLi, DoS, DB-fail); при виявленні інциденту виконується блокування і відновлення, а якщо він не виявлений — подія фіксується як компрометація. Усі події реєструються в журналі логів, що є основою для подальшого аналізу. Моделювання триває до досягнення встановленого часу T, після чого система переходить до етапу оцінки результатів.

Рисунок 1 – Концептуальна модель НМК та критичні точки безпеки

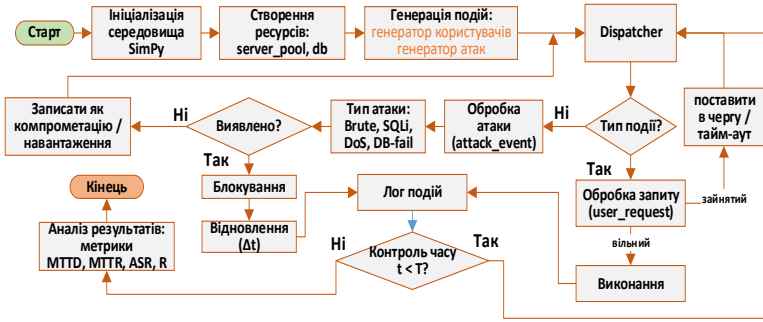

Рисунок 2 – Алгоритм імітаційного моделювання кіберзахищеності інформаційної системи

На завершальному етапі проведено аналіз журналів подій і розраховано ключові метрики кіберстійкості, що дало можливість оцінити ефективність політик безпеки та оптимізувати архітектуру НМК. Імітаційне моделювання підтвердило здатність системи ефективно реагувати на кіберінциденти в п'яти сценаріях, зокрема, під час пікових навантажень, коли різко зростає частота brute force та SQL-injection атак (рис. 3). Аналіз результатів (табл. 1) засвідчив, що впровадження моніторингу, 2FA та резервування бази даних суттєво підвищило кіберстійкість системи, скоротивши час виявлення та відновлення після інцидентів.

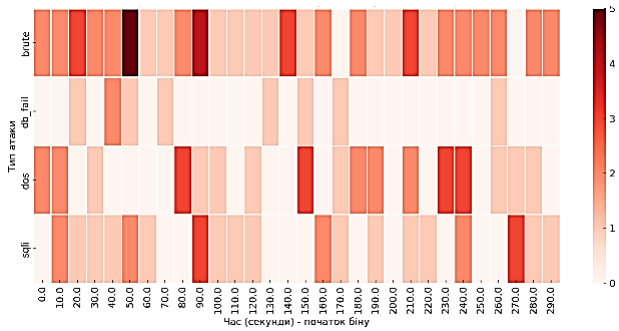

Рисунок 3 – Heatmap частоти атак

Таблиця 1. Порівняльні показники ефективності кіберзахищеності для різних сценаріїв

Сценарій	**MTTD (с)**	**MTTR (с)**	**ASR**
Базовий	9,6	7,2	0,64
Моніторинг	3,4	7,2	0,64
2FA	3,4	7,2	0,87
Резервування БД	3,4	3,4	0,87

MTTD (с) – час виявлення, MTTR (с) – час відновлення, ASR – частка заблокованих атак

У результаті дослідження розроблено методику імітаційного моделювання кіберзахищеності навчально-методичного комплексу (НМК) у середовищі Python + SimPy, що дозволяє відтворювати сценарії атак і відмов без ризику для реальної інфраструктури. Отримані метрики підтвердили ефективність моніторингу, двофакторної автентифікації та резервування бази даних. Імітаційний підхід довів свою придатність для виявлення вразливостей, порівняння конфігурацій безпеки та підвищення кіберстійкості освітніх систем.

Література

1. Пановик Р., Пановик У., Федина Б. Імітаційне моделювання для цифрової трансформації підсистеми управління освітнім процесом ВНЗ. *Вимірювальна та обчислювальна техніка в технологічних процесах,* 2025. 82(2), с. 159–166

2. Palko D. et al. Cyber Security Risk Modeling in Distributed Information Systems. *Applied Sciences*. 2023. Vol. 13, no. 4. P. 2393. URL: https://doi.org/10.3390/app13042393

УДК 004.056.5:004.738.5

КІБЕРЗАХИСТ МІКРОСЕРВІСНОЇ IIOT-АРХІТЕКТУРИ ВИРОБНИЧИХ ІНФОРМАЦІЙНИХ СИСТЕМ

Уляна ПАНОВИК[1,2], Богдана ФЕДИНА[1,2], Діана РІВНЯК[1]
[1]Львівський державний університет безпеки життєдіяльності,
[2]Національний університет «Львівська політехніка»

Анотація. *Розглянуто підхід до кіберзахисту виробничих інформаційних систем на основі мікросервісної архітектури IIoT. Запропоновано багаторівневу модель, що поєднує VPN, TLS, Zero Trust Policy Engine, контейнерну ізоляцію та моніторинг з аудитом. Такий підхід забезпечує захищене передавання даних, автентифікацію сервісів і контроль поведінки компонентів. Модель формує єдиний захисний контур від сенсорів до хмарних сервісів, підвищуючи стійкість і довіру до промислових даних.*

Ключові слова: *кіберзахист, IIoT, мікросервісна архітектура, Zero Trust, TLS, VPN, контейнерна безпека.*

Abstract. *The approach to cybersecurity of industrial information systems based on a microservice IIoT architecture is considered. A multilayer model is proposed that combines VPN, TLS, Zero Trust Policy Engine, container isolation, and monitoring with auditing. This approach ensures secure data transmission, service authentication, and component behavior control. The model forms a unified security contour from sensors to cloud services, increasing resilience and trust in industrial data.*

Keywords: *cybersecurity, IIoT, microservice architecture, Zero Trust, TLS, VPN, container security*

Сучасні виробничі системи переходять до архітектури IIoT, де сенсори, контролери та аналітичні модулі взаємодіють через мікросервісні інтерфейси. Така децентралізація підвищує гнучкість, але й збільшує ризики — від доступу до даних сенсорів до атак на контейнери. Традиційні засоби, як VPN чи TLS, захищають лише канали зв'язку, не контролюючи довіру між сервісами. Тому актуальним стає багаторівневий підхід до кіберзахисту з урахуванням контексту взаємодії елементів. Використання принципу security-by-design дозволяє вбудовувати захист у мікросервіси, API-шлюзи та політики доступу, поєднуючи шифрування, контроль ресурсів і виявлення аномалій.

У промислових системах IIoT безпека охоплює всі рівні — від сенсорів до хмарних сервісів. Висока взаємопов'язаність компонентів, динамічне масштабування контейнерів і використання відкритих протоколів (MQTT, REST API) створюють нові вектори атак, недоступні для класичних методів захисту. Оскільки кожен мікросервіс має власні політики доступу та автономне розгортання, ефективний кіберзахист потребує комплексного підходу, що поєднує мережеві, прикладні та поведінкові технології [1].

Базовими механізмами захисту в IIoT-системах залишаються VPN і TLS технології. VPN забезпечує створення захищених тунелів між вузлами, ізоляцію від публічних мереж і захист управлінських команд. Сучасні рішення (WireGuard, OpenVPN) відзначаються високою швидкодією, однак не усувають ризик внутрішніх атак, тому використовуються як частина багаторівневого захисту. TLS гарантує конфіденційність і автентичність даних у мікросервісних обмінах, зокрема через сертифікати X.509. Його реалізація у брокерах MQTT чи API-шлюзах потребує належного керування ключами та ротації сертифікатів, інакше можливе створення лише ілюзії безпеки без фактичного контролю ідентичності [2].

Концепція Zero Trust Architecture (ZTA) усуває довіру за замовчуванням: кожен запит автентифікується й авторизується незалежно від джерела. У IIoT це означає цифрову ідентичність для кожного сенсора, шлюзу чи сервісу, а рішення про доступ приймає Policy Engine, що знижує ризик внутрішніх атак. Контейнерна безпека (Docker, Kubernetes, AppArmor, SELinux, Falco) ізолює мікросервіси й контролює їхню поведінку, запобігаючи поширенню компрометацій. IDS/IPS аналізують трафік і виявляють аномалії на рівні edge-пристроїв. Таким чином, поєднання VPN, TLS, Zero Trust, контейнерної ізоляції та IDS/IPS формує проактивну, багаторівневу систему кіберзахисту IIoT.

Виробнича система на базі IIoT — це багаторівнева структура, де апаратні, комунікаційні й аналітичні компоненти взаємодіють через мікросервіси. Така архітектура підвищує гнучкість, але створює нові вразливості, тому захист має охоплювати всі рівні. Зазвичай виокремлюють три: польовий, edge/gateway і центральний. Польовий рівень охоплює сенсори й контролери, що потребують локального шифрування та автентифікації. Edge-рівень — шлюзи, брокери MQTT/AMQP і мікросервіси, де використовуються VPN, TLS, контейнерна ізоляція й Zero Trust. Центральний рівень включає аналітику, бази даних і SCADA/HMI з реалізацією RBAC, IDS/IPS та аудиту. Ефективний кіберзахист досягається лише інтеграцією цих рівнів — від достовірності даних до захищеного управління.

Побудова кіберзахисту виробничої IIoT-системи повинна розпочинатися ще на етапі її проєктування, коли визначаються логіка взаємодії сервісів, канали обміну даними та механізми автентифікації. Концепція security-by-design передбачає інтеграцію безпеки не як додаткового модуля, а як невід'ємної частини архітектури — із закладеними політиками шифрування, контролю доступу та моніторингу. У межах запропонованої моделі кіберзахисту мікросервісної IIoT-архітектури використовуються взаємопов'язані рівні безпеки, які формують єдину захисну оболонку системи: VPN, TLS, Zero Trust Policy Engine, контейнерна ізоляція та моніторинг і аудит (рис.1).

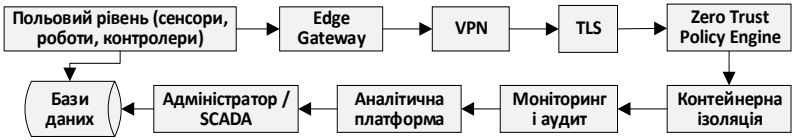

Рисунок 1 – Модель кіберзахисту мікросервісної IIoT-архітектури

Перший рівень VPN формує захищений тунель між вузлами та серверами, запобігає перехопленню трафіку й гарантує безпечний доступ через публічні мережі. Для промислових систем ефективними є легковагові протоколи WireGuard або OpenVPN. Другий рівень TLS забезпечує шифрування даних і взаємну автентифікацію мікросервісів, а централізована система PKI з ротацією сертифікатів гарантує цілісність як зовнішнього, так і внутрішнього трафіку. Третій рівень Zero Trust Policy Engine контролює доступ, перевіряючи кожен запит за контекстом і станом пристроїв, що запобігає внутрішнім загрозам. Четвертий рівень контейнерна ізоляція забезпечує безпечне виконання мікросервісів через обмеження привілеїв, контроль ресурсів і перевірку образів, запобігаючи поширенню атак між контейнерами. П’ятий рівень моніторинг і аудит здійснює постійний аналіз поведінки системи за допомогою IDS/IPS і SIEM, формуючи зворотний зв’язок із Policy Engine для адаптації політик безпеки в реальному часі.

Представлена модель кіберзахисту мікросервісної IIoT-архітектури забезпечує безпечну взаємодію польових пристроїв, шлюзів і аналітичних сервісів. Вона об’єднує п’ять рівнів — VPN, TLS, Zero Trust Policy Engine, контейнерну ізоляцію та моніторинг — у єдиний захисний контур від збору даних до управління процесами. VPN і TLS гарантують захищене передавання даних, Zero Trust контролює динамічний доступ, контейнерна ізоляція запобігає поширенню атак, а моніторинг і аудит забезпечують постійний контроль. Така інтегрована структура підвищує стійкість, керованість і довіру до промислових даних без потреби складної централізованої перевірки

Література

1. Пановик У. Захист інформації в автоматизованих системах на основі концептуальної моделі з формалізованою оцінкою ефективності. *Кібербезпека: освіта, наука, техніка»*, 2025. 4(28), с. 307–320. URL: https://doi.org/10.28925/2663-4023.2025.28.798

2. Zhukabayeva T. et al. Cybersecurity Solutions for Industrial Internet of Things–Edge Computing Integration: Challenges, Threats, and Future Directions. *Sensors*. 2025. Vol. 25, no. 1. P. 213. URL: https://doi.org/10.3390/s25010213

УДК 004.056.5

ZERO-KNOWLEDGE-МЕХАНІЗМ ПІДТВЕРДЖЕННЯ ПРАВ ДОСТУПУ У ХМАРНИХ СЕРВІСАХ

Петро ПЕТРІВ, Іван ОПІРСЬКИЙ
Національний університет «Львівська політехніка»

Досліджено передові механізми контролю доступу в хмарних середовищах на основі протоколів з нульовим розголошенням (ZKP). Проаналізовано гібридні архітектури, що інтегрують ZKP з блокчейном, гомоморфним шифруванням та Merkle-деревами для забезпечення конфіденційності, цілісності даних та ефективної автентифікації, спираючись на актуальні дослідження 2024-2025 років.

Ключові слова: *хмарні сервіси, безпека, контроль доступу, Zero-Knowledge Proof, ZKP, блокчейн, гомоморфне шифрування*

Advanced access control mechanisms in cloud environments based on Zero-Knowledge Proofs (ZKP) are investigated. Hybrid architectures integrating ZKP with blockchain, homomorphic encryption, and Merkle trees are analyzed to ensure confidentiality, data integrity, and efficient authentication, drawing on current research from 2024-2025.

Keywords: *cloud services, security, access control, Zero-Knowledge Proof, ZKP, blockchain, homomorphic encryption*

Метою цього дослідження є аналіз та систематизація сучасних підходів до реалізації механізмів підтвердження прав доступу у хмарних сервісах з використанням протоколів нульового розголошення (ZKP), з акцентом на переваги та виклики гібридних архітектур.

У сучасному світі хмарні обчислення стали основою цифрової інфраструктури, проте вони несуть значні ризики, пов'язані з централізованим зберіганням даних та автентифікацією. Традиційні методи, що вимагають передачі паролів або ключів, є вразливими до атак типу «людина посередині», фішингу та атак на основі скомпрометованих облікових даних (credential stuffing). Технологія доведення з нульовим розголошенням (Zero-Knowledge Proof, ZKP) – криптографічний протокол, що дозволяє одній стороні (доводжувачу) переконати іншу сторону (верифікатора) в істинності твердження, не розкриваючи жодної додаткової інформації, окрім самого факту істинності – пропонує кардинально новий підхід до цієї проблеми. Актуальність теми підкреслюється прогнозами аналітиків, згідно з якими до 2025 року 30% великих підприємств почнуть впровадження ZKP для автентифікації.

Застосування ZKP у хмарних сервісах дозволяє користувачам підтверджувати свої права доступу, не розкриваючи при цьому самих облікових даних. Це створює надійну систему, де верифікація відбувається на основі математичного доказу, а не на довірі до централізованого

провайдера. Сучасні дослідження [1-5] зосереджені на розробці гібридних архітектур, які поєднують ZKP з іншими передовими технологіями, такими як блокчейн, гомоморфне шифрування та Merkle-дерева, для створення комплексних, багатошарових систем безпеки. Такі інтеграції дозволяють нівелювати недоліки окремих технологій та посилити їхні переваги, створюючи синергетичний ефект.

У рамках дослідження розглянуто декілька ключових гібридних моделей. Інтеграція ZKP з блокчейном, як показано в системі ZKBAR-V [1], дозволяє створювати децентралізовані та незмінні системи управління ідентифікацією за допомогою zkEVM смарт-контрактів. Поєднання ZKP з Pedersen Commitments [2], які є адитивно гомоморфними, забезпечує ефективну верифікацію цілісності великих обсягів даних сторонніми аудиторами без доступу до самої інформації. Комбінація ZKP з гомоморфним шифруванням [3] відкриває можливості для безпечних обчислень над зашифрованими даними, наприклад, для конфіденційної дедуплікації, що зменшує навантаження на сховище провайдера. Для підвищення ефективності пропонується інтеграція автентифікації та контролю доступу в єдиний модуль з використанням Merkle-дерев [4], що дозволяє ефективно доводити наявність певних прав доступу, не розкриваючи весь їх перелік. Для надійності в розподілених системах, що включають туманні обчислення, модель [5] використовує поєднання блокчейну та гібридних алгоритмів шифрування (ECDH та SHA-512), що зменшує затримки при обробці даних.

Ключові характеристики ZKP-систем у хмарних сервісах базуються на трьох фундаментальних властивостях. По-перше, конфіденційність доказу гарантує, що система дозволяє верифікувати права доступу без розкриття будь-якої конфіденційної інформації, наприклад, доводити досягнення повноліття, не розкриваючи дати народження. По-друге, цілісність верифікації забезпечується криптографічною природою доказів, що унеможливлює їх підробку або модифікацію, гарантуючи, що тільки легітимний користувач може пройти автентифікацію. По-третє, децентралізована довіра, особливо при інтеграції з блокчейном, усуває необхідність у централізованому органі, що керує довірою, розподіляючи її між учасниками мережі та усуваючи єдину точку відмови.

Переваги використання ZKP для контролю доступу є значними. Найважливішою є надійний захист від крадіжки облікових даних, оскільки секретні дані ніколи не передаються через мережу, ризик їх перехоплення зводиться до мінімуму, на відміну від систем, що зберігають навіть хешовані паролі. Це також забезпечує відповідність стандартам конфіденційності, таким як GDPR та HIPAA, оскільки ZKP-механізми реалізують принцип мінімізації даних, обробляючи лише доказ, а не самі персональні дані. Нарешті, такий підхід веде до зменшення поверхні атаки:

оскільки на сервері не зберігаються секрети користувачів, його компрометація не призведе до масового витоку облікових даних.

Отже, впровадження ZKP-механізмів є стратегічно важливим кроком для підвищення безпеки хмарних сервісів. Гібридні архітектури, що поєднують ZKP з блокчейном, гомоморфним шифруванням та іншими криптографічними інструментами, створюють надійну, багатошарову систему захисту, яка відповідає сучасним вимогам до конфіденційності та цілісності даних. Незважаючи на такі виклики, як обчислювальна складність та розмір доказів, особливо для неінтерактивних протоколів типу zk-SNARKs, що вимагають довіреної початкової установки (trusted setup), переваги ZKP роблять їх ключовою технологією для побудови довірених цифрових екосистем. Подальші дослідження повинні бути спрямовані на оптимізацію продуктивності, зокрема через розвиток прозорих та масштабованих протоколів, таких як zk-STARKs, стандартизацію API для інтеграції та розробку квантово-стійких ZKP-алгоритмів для протидії майбутнім загрозам. Це відкриє шлях до їх широкого застосування не тільки в хмарних сервісах, але й у сферах Інтернету речей (IoT), цифрових фінансів та електронного голосування, створюючи нові бізнес-моделі, засновані на довірі та перевірці даних.

Література

1. Блокчейн як технологія децентралізованих баз даних / О. М. Сидоренко // Вісник Київського національного університету імені Тараса Шевченка. Серія "Комп'ютерні науки та інформаційні технології". – 2020. – Вип. 3(59). – С. 13-20.

2. Блокчейн-технологія в децентралізованих базах даних / В. В. Кісь, М. В. Піщак, І. О. Філіпчук // Вісник Національного університету "Львівська політехніка". Серія "Комп'ютерні науки". – 2022. – № 235. – С. 133-140.

3. Децентралізовані бази даних на основі блокчейн-технології / О. В. Мельник, О. В. Руденко // Вісник Одеського національного університету імені І. І. Мечникова. Серія "Математика. Комп'ютерні науки. Інформаційні технології". – 2021. – Вип. 35(2). – С. 103-110.

4. Блокчейн у децентралізованих базах даних: перспективи та виклики / О. І. Полотай, О. О. Тлумак // Вісник Національного університету "Львівська політехніка". Серія "Комп'ютерні науки". – 2023. – № 237. – С. 119-128.

5. Блокчейн у системах управління даними: особливості та перспективи / В. В. Кісь, М. В. Піщак // Вісник Національного університету "Львівська політехніка". Серія "Комп'ютерні науки". – 2023. – № 238. – С. 137-146.

УДК 004.056

КОНЦЕПЦІЯ ПОКРАЩЕННЯ ЗАХИСТУ АНОНІМНОСТІ КОРИСТУВАЧІВ МЕРЕЖІ TOR ЧЕРЕЗ ЗАСТОСУВАНЯН ДОДАТКОВОГО ШАРУ ЗАХИСТУ ТА ТЕХНОЛОГІЇ БЛОКЧЕЙН

**Василь ПОБЕРЕЖНИК[1], Іван ОПІРСЬКИЙ[1],
Валерія БАЛАЦЬКА[2]**

1. Національний університет «Львівська політехніка»
2. Львівський державний університет безпеки життєдіяльності

Анотація. *Розглянуто концепцію методу покращення захисту анонімності користувачів мережі Tor, через застосування додаткових шарів захисту та транзитної точки, яка повинна розривати можливі зловмисні маршрути. Запропоновано застосування технології блокчейн для забезпечення збереження прозорої та стійкої до підробок інформації про вузли захисту, які застосовуються у системі*

Ключові слова: *блокчейн, Tor, анонімність, приватність, багатошарова маршрутизація.*

Abstract*. The concept of a method for improving the protection of the anonymity of the Tor network users is considered, using additional layers of protection and a transit point that should break possible malicious routes. The use of blockchain is proposed to preserve the transparent and tamper-resistant information about the protection nodes used in the system*

Keywords: *blockchain, Tor, anonymity, privacy, onion routing*.

Приватність та анонімність користувачів є важливим атрибутом користувачів різних сервісів у мережі. За допомогою різних сервісів забезпечення анонімності та приватності, користувачів намагаються захистити свою приватність в мережі, обійти різного роду обмеження чи захистити власні персональні дані, від надмірного збору чи несанкціонованого використання зі сторони провайдерів різних сервісів.

Одним із способі захисту власної приватності є використання мережі Tor. Ця технологія дозволяє забезпечувати захист анонімності користувачів, через встановлення багатошарової маршрутизації між вузлами мережі. Найменшою кількістю вузлів, для встановлення захищеного з'єднання із застосуванням мережі Tor є три вузли: вхідний, проміжний і вихідний.

Однак, застосування такого підходу не є гарантією збереження анонімності, оскільки існує ряд атак на користувачів мережі, який дозволяє деанонімізувати користувача мережі. Наприклад, дозволяє встановлювати особу користувача шляхом застосування різних деанонімізуючих засобів, наприклад аналіз вхідного і вихідного трафіку, використання зловмисних вузлів тощо [1]. Також нещодавно було продемонстровано техніку, яка дозволяла не тільки визначити користувача, який користується мережею, але й із допомогою зловмисних вузлів розривати захищене з'єднання і спрямовувати трафік на маршрут, який є контрольованим зловмисником [2].

Одним із принципів Tor є збереження інформації про вихідні вузли у відкритому доступі, що дозволяє зловмиснику без будь-яких перешкод, що спрощує атаки на ці вузли, їхнє цензурування тощо. Хоча сам підхід до відкритості є одним із ключових аспектів мережі Tor, який з одного боку покликаний підвищити довіру до мережі, а з іншого – є важливим функціональним аспектом, оскільки ця відкритість вузлів є необхідною для забезпечення встановлення маршруту між вузлами, користувачем та точкою призначення [3]. Проте така відкритість може стати своєрідним “modus operandi”, що може призвести до компрометації з’єднання та подальшої атаки на користувача, цензурування, деанонімізації тощо.

Зважаючи на це, можна вважати, що критичними точками у такій системі є вузол входу та виходу, оскільки перший знає інформацію про користувача, а останній – про точку призначення. Опираючись на це, можна розробити концепцію захисту від зловмисних вузлів, яка б могла протидіяти згаданій вразливості. Основна ідея пропонованого методу полягає в тому, що для захисту з’єднання і самого користувача необхідно встановити додатковий шар захисту та точку розриву маршруту, що схематично зображено на рисунку 1.

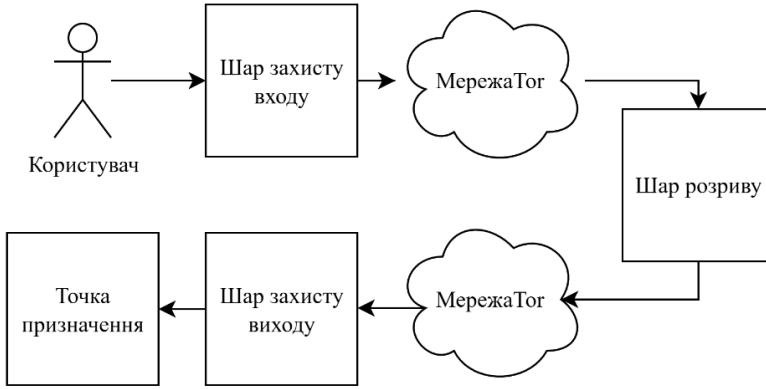

Рисунок 1 – Схематичне зображення методу із застосуванням розриву та додаткових шарів захисту

Безпека шарів захисту повинна забезпечуватися через застосування технології блокчейн як реєстру довірених вузлів: вузли вхідного і вихідного шару зберігають інформацію про себе у мережі блокчейн, що дозволить точно впевнитися в автентичності вузла, а вузол розриву слугує для захисту від зловмисної вихідної точки, оскільки він виконує роль транзитної точки, яка є одночасно кінцевою точкою для одного маршруту і початком нового, який буде вести до за шару виходу з мережі Tor. Отже суть підходу полягає в тому, щоб анонімізувати користувача ще до входу в мережу Tor, а також розірвати

можливе зловмисне з'єднання через створення двох маршрутів, де вхідна і вихідна точки є надійними. Застосування блокчейну в такому підході є важливим, оскільки сам він дозволить забезпечити надійне збереження даних про вузли, через свої властивості збереження інформації у незмінному вигляді та прозорість [4]. Також пропонується застосування гібридного підходу, де вузли обробляють інформацію підходом off-chain, оскільки обробка інформації великих обсягів або чутливої до затримок є недоцільною у самому блокчейні [5].

Аргументом для застосування такої концепції є те, що вона може використовувати уже готову інфраструктуру, як от публічний блокчейн, наприклад Ethereum, Solana тощо, та мережу Tor, яка є розвинутою дозволяє обробляти відносно великі об'єми трафіку даних.

Також ця концепція має і свої недоліки, які можуть стати на заваді реалізації системи, одним з них є необхідність підтримки роботи вузлів пропонованої системи, оскільки вона потребуватиме для своєї роботи постійного оновлення даних в мережі блокчейн та обслуговування самих вузлів.

Зважаючи на переваги та недоліки, можна зробити висновок, що застосування запропонованого підходу може дозволити покращити захищеність анонімності та приватності користувачів, а застосування гібридних технологій дозволяє застосовувати сильні сторони технологій, як от стійкість до змін та прозорість даних у блокчейні, та нівелювати їхні обмеження, як от низька толерантність до обробки великих масивів даних чи відносно низька швидкодія. Також концепція потребує подальшого дослідження, щоб дослідити доцільність застосування такого підходу та можливі шляхи застосування.

Література

1. Tor project | network attackers on the tor network. Tor Project | Join the Tor Community. URL: https://community.torproject.org/threat-model/threat-positioning/network/ (дата звернення: 21.11.2025).

2. An anonymity vulnerability in tor / Q. Tan та ін. IEEE/ACM transactions on networking. 2022. С. 1–14. URL: https://doi.org/10.1109/tnet.2022.3174003

3. You should hide the list of tor relays, so people can't block the exits. Support. URL: https://support.torproject.org/about-tor/alt-design/hide-list-of-exits/ (дата звернення: 21.11.2025).

4. Балацька В. С., Побережник В. О., Стефанків А. В., Шевчук Ю. А. Розробка методу забезпечення достовірності та безпеки персональних даних у блокчейн-системах державних реєстрів. Комп'ютерні системи та мережі. 2025. Т. 7, № 1. С. 1–16. DOI: https://doi.org/10.23939/csn2025.01.001

5. Дослідження швидкодії методу передачі повідомленнь із застосуванням off-chain обробки даних для забезпечення цілісності та незмінності даних. Сучасний захист інформації. 2025. Т. 63, № 3. С. 230–242. URL: https://doi.org/10.31673/2409-7292.2025.032280 (дата звернення: 21.11.2025).

УДК 004.056.5:004.942

ВИКОРИСТАННЯ СЛАБКИХ ЛАНЦЮЖКІВ МЕРЕЖЕВИХ ІГОР ЯК ТОЧКИ ВХОДУ В КОРПОРАТИВНІ МЕРЕЖІ

[1]Полотай О.І., [2]Дітковський М.М., [1]Гуменюк М.Р.
[1]Львівський державний університет безпеки життєдіяльності
[2]Національний університет Львівська політехніка

Анотація. *Розглядається малодосліджений вектор кіберзагроз — використання слабких елементів мережевих ігор як потенційних точок проникнення у корпоративні мережі. Окреслено типові сценарії атак, способи маскування шкідливої активності під ігровий трафік, а також наведено рекомендації щодо мінімізації ризиків і підвищення кіберстійкості.*

Ключові слова : *мережеві ігри; кіберзагрози; корпоративна мережа; уразливості; P2P-з'єднання; ігрові модифікації; шкідливе програмне забезпечення; соціальна інженерія; інформаційна безпека; кіберстійкість; вектори атак; контроль програмного середовища.*

Сучасні корпоративні мережі дедалі частіше зазнають атак не через класичні вектори проникнення, а через малопомітні побічні канали, пов'язані з цифровою поведінкою працівників. Однією з таких недооцінених загроз є використання мережевих ігор, які встановлюються на робочих станціях або запускаються через браузер. Оскільки більшість компаній не розглядають геймінг як серйозний фактор кіберризику, ігрові клієнти, сторонні лаунчери та внутрішньоігрові сервіси часто залишаються поза увагою систем технічного захисту інформації. Це створює можливість для атакувальників використовувати слабкі компоненти ігор як точку входу в корпоративне середовище.

Мережеві ігри використовують складну інфраструктуру: центральні сервери, peer-to-peer-механізми, голосові чати, моди, плагіни та сторонні лаунчери. Більшість із цих компонентів не проходять комплексної перевірки безпеки на рівні корпоративного ІТ. На відміну від бізнес-ПЗ, ігрові програми часто мають нерегулярні оновлення, невідомі залежності, слабко захищені протоколи передачі даних та високий рівень довіри з боку користувача, що відкриває можливості для інжекції шкідливого коду.

В таблиці 1 показано найбільш популярні онлайн-ігри.

Таблиця 1 – Сучасні онлайн-ігри

Назва гри	Платформи	Особливості
World of Tanks	ПК, консолі, мобільні	Класика MMO-танків
World of Tanks Blitz / Modern	Мобільні / консолі	Мобільні/консольні версії WoT

Armor		
World of Tanks: Heat	ПК, консолі (PS5, XSX/S), Steam Deck	Hero-shooter у танковому сеттингу
War Thunder	ПК, консолі	Реалістичний симулятор
Armored Warfare	ПК	Сучасні танки + PvE
Enlisted	ПК	Історичні кампанії WWII
Call of War: WWII	Браузер	Глобальна стратегія/MMO
Diep.io	Браузер / мобільні	Легка .io-гра
BZFlag	ПК	Open-source 3D FPS-танки
Tanki Online	Браузер	Кастомізація, PvP, івенти
Modern Tanks (Steam)	ПК (Steam)	Аркадний топ-down танковий шутер

В сучасних комп'ютерних топологіях існують такі типові місця потенційного проникнення в корпоративну мережу через мережеві ігри:

1. P2P-з'єднання між гравцями, які можуть бути використані для сканування відкритих портів або впровадження експлойтів на робочі станції.
2. Ігрові моди й плагіни, що часто розробляються сторонніми програмістами без аудитів безпеки; поширення модів може стати інструментом масового зараження.
3. Голосові чати та VoIP-інтеграції, уразливі до атак типу buffer overflow або компрометації протоколів передавання голосу.
4. Фішингові внутрішньоігрові повідомлення, що імітують офіційні нотифікації від ігрових сервісів, стимулюючи працівника переходити за шкідливими посиланнями.
5. Сторонні лаунчери, які збирають телеметрію, мають привілейований доступ до файлової системи та оновлюються через незашифровані канали.
6. Потрапивши на робочу станцію, шкідливе ПЗ може використати ігровий процес як маскування для аномального трафіку або lateral movement усередині мережі.

Для мінімізації таких загроз необхідно дотримуватися таких рекомендацій:

1. Заборонити запуск ігор на робочих станціях або ізолювати їх у віртуальних контейнерах.
2. Застосовувати контроль додатків з чітким переліком дозволених програм.
3. Використовувати мережеву сегментацію, щоб робочі місця з низьким рівнем довіри не мали прямого доступу до внутрішніх сервісів.
4. Активувати поведінковий моніторинг трафіку, що дозволить виявляти аномальні P2P-з'єднання.

5. Проводити корпоративні тренінги, де працівників навчають ризикам встановлення модів та сторонніх патчів.

6. Аналізувати журнали дій на робочих станціях через системи SIEM для виявлення специфічних патернів, типових для ігрового ПЗ.

Висновки. Мережеві ігри становлять малопомітний, але потенційно високоризиковий вектор проникнення в корпоративні мережі. Незахищені компоненти ігрової інфраструктури, багатокомпонентні лаунчери, моди та P2P-механізми можуть стати "слабкими ланцюжками", через які зловмисники отримують доступ до внутрішніх систем підприємства. Поєднання технічних уразливостей і ризикованої поведінки користувачів створює сприятливе середовище для проведення атак нового типу. Усвідомлення цієї проблеми та впровадження комплексних заходів контролю дозволить суттєво підвищити рівень кіберстійкості корпоративної інфраструктури та мінімізувати ризики, пов'язані з використанням розважального ПЗ у робочому середовищі

Література

1. Поширені загрози для геймерів: як суперники можуть впливати на хід гри. URL: https://www.eset.com/ua/about/newsroom/blog/home-security/osnovnyye-ugrozy-dlya-geymerov-kak-protivniki-mogut-vliyat-na-khod-igry/?srsltid=AfmBOoqmU3ieMyMCr7agDWUVKzO0Y7Z033LeULHz-5bTZgTok0_hqjz0

2. Полотай О.І., Брич Т.Б., Ткаченко А.М., Дітковський М.М., Гуменюк М.Р. Інформаційні загрози та методи забезпечення безпеки в сучасних мережевих іграх. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка». 2025. Том 2 № 30: С. 50-64.

3. 10 порад щодо безпеки в іграх онлайн. URL: https://lemon.school/blog/10-porad-shhodo-bezpeky-v-igrah-onlajn

УДК 004.056.5:004.9:004.738.5

ПРОГНОЗУВАННЯ КІБЕРЗАГРОЗ ЧЕРЕЗ АНАЛІЗ “ЕМОЦІЙНИХ ПАТЕРНІВ” СОЦІАЛЬНИХ МЕРЕЖ

Полотай О.І.
Львівський державний університет безпеки життєдіяльності

Анотація. *У роботі розглянуто підхід до прогнозування кіберзагроз на основі аналізу емоційних патернів, що формуються у соціальних мережах під впливом суспільних подій та інформаційних хвиль. Показано, що різкі зміни емоційного фону, зокрема зростання негативу, паніки чи агресії, можуть передувати масштабним фішинговим, DDoS-атакам або інформаційним операціям.*

Ключові слова*: емоційні патерни; соціальні мережі; кіберзагрози; прогнозування; інформаційна безпека; машинне навчання; аналіз тональності; поведінкова аналітика; аномалії; кіберстійкість.*

Вступ. У сучасному цифровому середовищі соціальні мережі формують великий масив непрямої інформації, що відображає суспільні настрої, реакції на події, конфлікти та інформаційні коливання. Ці дані можуть бути не лише індикатором соціальної активності, але й потужним інструментом прогнозування кіберзагроз. Емоційні патерни – тобто зміни емоційного забарвлення контенту, реакцій, коментарів та поведінки користувачів – часто передують активізації кібератак, кампаній дезінформації та хвиль фішингових дій. Вивчення таких патернів дозволяє створити новий підхід до раннього попередження про можливі інциденти, особливо в умовах гібридних загроз.

Основні частина. Емоційний фон у соціальних мережах змінюється під впливом політичних криз, економічних новин, техногенних подій чи інформаційних кампаній. Для кіберзахисту важливо те, що різке зростання емоційної напруженості, агресивних повідомлень або одноманітності реакцій часто корелює з підготовкою цілеспрямованих цифрових атак. Наприклад:

- перед масовими DDoS-атаками спостерігається різкий сплеск токсичності в публічних коментарях;
- перед фішинговими розсилками – активне обговорення певної теми, яку зловмисники збираються використати як приманку;
- перед кібератаками на державні органи – збільшення кількості негативних емоційних хвиль у згадках про ці органи..

Для формування системи прогнозування необхідно аналізувати:

- семантику текстів (ключові слова, контекст, настрій);
- тональність (рівень негативу, агресії, паніки, ентузіазму);
- динаміку реакцій (раптові піки лайків, репостів, згадок);
- ритм комунікацій (частота постів у короткі проміжки часу);
- емоційні кластери (групи повідомлень з однотипним настроєм).

Дослідження показують, що інформаційні операції часто використовують три стадії:

1. Підготовка емоційного фону – невеликі вкиди інформації створюють напруження.

2. Ескалація емоцій – масові обговорення підсилюють увагу до теми.

3. Кіберудар – використання створеного емоційного стану для маскування атаки або підвищення її ефективності.

На основі аналізу емоційних патернів можна створити:

Модель короткострокового прогнозування (1–3 дні) – реагує на раптові зміни в негативі, сплески агресії чи масові обговорення новин.

Модель середньострокового прогнозування (1–2 тижні) – виявляє поступову ескалацію напруги та формування «інформаційних хвиль».

Модель подієвого прогнозування – передбачає кібератаку під час значимих подій (вибори, свята, кризи), якщо спостерігається аномальна концентрація емоційних реакцій.

Такі моделі можуть інтегруватися у SOC або системи моніторингу ризиків.

Підприємства та державні структури можуть використовувати аналіз емоційних патернів для:

- підсилення кіберстійкості перед кризами;
- передбачення хвиль фішингу, пов'язаних з резонансними новинами;
- ідентифікації інформаційних операцій, що супроводжують кібератаки;
- виявлення цілеспрямованої дискредитації, яка є частиною гібридних дій;
- коригування кіберзахисних сценаріїв відповідно до суспільних настроїв.

Інтеграція таких підходів у системи безпеки дозволяє не лише реагувати на інциденти, а й передбачати їх до фактичного прояву.

В якості прикладу можна навести таку ситуацію: під час загострення політичної ситуації в країні одна з великих фінансових установ помічає різке збільшення кількості негативних і панічних згадок у соціальних мережах. У короткий період стрімко зростає емоційна напруженість: користувачі поширюють повідомлення про нібито "масове блокування карток", активно коментують чутки про можливі технічні збої й висловлюють недовіру до банківської системи. Алгоритми аналізу емоційних патернів фіксують аномальну концентрацію негативного контенту, а тематика цих повідомлень збігається з популярними методами фішингових атак. Система попередження ризиків формує прогноз про ймовірну хвилю шахрайських розсилок, спрямованих на клієнтів та співробітників підприємства.

За кілька годин після піку емоційної хвилі зловмисники дійсно запускають масштабну фішингову кампанію, маскуючи свої повідомлення під офіційні попередження банку. Користувачі, які вже перебувають у стані підвищеної тривожності та очікують проблем, значно частіше переходять за шкідливими посиланнями, що збільшує ефективність атаки. Завдяки ранньому аналі-

зу емоційного фону організація отримує змогу швидко попередити клієнтів, посилити моніторинг транзакцій і внести корективи у політику кіберзахисту до того, як атака набула критичного масштабу. Такий приклад демонструє, як вчасне виявлення деструктивних емоційних патернів може стати дієвим інструментом прогнозування кіберзагроз.

Висновки. Аналіз емоційних патернів соціальних мереж відкриває новий напрям у прогнозуванні кіберзагроз. Емоційні хвилі часто передують активним фазам цифрових атак, а їх раннє виявлення дозволяє підприємствам і державним структурам підготуватися до можливих інцидентів. Застосування машинного навчання та моніторингу соціальних платформ дає можливість формувати динамічні моделі ризику, що відображають реальний емоційний стан суспільства. Це підвищує ефективність кіберзахисту, забезпечує перевагу у часі та зменшує ймовірність успішної реалізації атак.

Література

1. Полотай О.І., Кухарська Н.П. Прогнозування індексу захищеності комп'ютерних мереж за допомогою економетричних моделей. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка». 2025. Том 4 № 28: С. 365-374.

2. Сус В. Аналіз моделі прогнозування кіберзагроз "Cyber Kill Chain". Modeling, Control and Information Technologies: Proceedings of International Scientific and Practical Conference, (7), 2025, С. 210–211.

3. Яковів І. Модель чотирьох інформаційних середовищ кібератаки. Information Technology and Security. July-December 2023. Vol. 11. Iss. 2 (21). С.175-192.

УДК 004.056.5:004.421.2:004.415.2

МІКРОПРОЦЕСОРНА КРИМІНАЛІСТИКА: АНАЛІЗ АТАК ЧЕРЕЗ ПАРАЗИТНІ ЕНЕРГЕТИЧНІ КОЛИВАННЯ

Полотай О.І.
Львівський державний університет безпеки життєдіяльності

Анотація. *У роботі розглядається сучасний напрям кібербезпеки — мікропроцесорна криміналістика, що базується на аналізі паразитних енергетичних коливань мікропроцесорів для виявлення кіберзагроз. Показано, що навіть незначні зміни у споживанні енергії, коливання тактової частоти чи теплові аномалії можуть сигналізувати про присутність шкідливого програмного забезпечення, апаратних бекдорів або атак через side-channel. Проаналізовано основні методи криміналістики на мікропроцесорному рівні, включаючи аналіз енергоспоживання, електромагнітного випромінювання, кеш-патернів та тимчасових характеристик, а також їх застосування для розслідування і прогнозування кіберінцидентів. Результати підкреслюють ефективність апаратного моніторингу як додаткового інструменту кіберзахисту і цифрової криміналістики.*

Ключові слова: *мікропроцесорна криміналістика; паразитні енергетичні коливання; side-channel атаки; апаратна безпека; аналіз кеш-пам'яті; електромагнітний аналіз; тимчасові аномалії; цифрова криміналістика; кіберзагрози; апаратні бекдори..*

Вступ. Зростання складності сучасних комп'ютерних систем та процесорних архітектур створює нові виклики для кібербезпеки. Одним із перспективних і водночас маловивчених напрямів є мікропроцесорна криміналістика, яка дозволяє виявляти атаки та аномальні дії через аналіз паразитних енергетичних коливань, що виникають під час роботи електронних компонентів. Навіть незначні зміни у споживанні електроенергії або напрузі можуть сигналізувати про стороннє втручання, спроби експлуатації вразливостей або приховану діяльність шкідливого програмного забезпечення. Тема стає особливо актуальною в умовах росту кількості апаратних атак, коли класичні засоби виявлення шкідливого ПЗ або вторгнень можуть бути неефективними.

Основна частина. Мікропроцесорна криміналістика ґрунтується на тому, що будь-який електронний пристрій під час роботи генерує специфічні енергетичні сигнали, що залежать від виконуваних інструкцій, навантаження на ядра та взаємодії з периферією. Паразитні коливання, тобто мікроскопічні відхилення напруги або струму, можуть виникати через апаратні збої, а також бути наслідком впровадження шкідливого коду або сторонніх процесів, що намагаються використовувати уразливості мікропроцесора. Аналіз цих коливань дозволяє відстежувати навіть приховані дії, що не залишають слідів у традиційних журналах подій або операційних системах.

За допомогою спеціалізованих датчиків та високочастотного моніторингу енергетичних характеристик можна виявити аномалії, які корелюють з потенційними атаками. Наприклад, спроби здійснення side-channel

атак, таких як атаки на кеш або через коливання тактової частоти, створюють закономірні, хоч і мінімальні, відхилення у споживанні енергії. Виявлення цих відхилень дозволяє проводити ретроспективний аналіз дій на мікропроцесорному рівні, відтворювати сценарії атаки та ідентифікувати вектор вторгнення. Це відкриває нові можливості для цифрової криміналістики, особливо в умовах складних гібридних систем, де традиційні методи безпеки виявляються недостатньо чутливими.

В таблиці 1 наведено опис методів мікропроцесорної криміналістики, які є популярними на даний час.

Таблиця 1 – перелік методів мікропроцесорної криміналістики

Метод	Суть методу	Що дозволяє виявити	Типові сценарії застосування
Аналіз паразитних енергетичних коливань (Power Analysis)	Вимірювання коливань напруги та струму під час роботи мікропроцесора.	Приховані процеси, шкідливий код, side-channel атаки, аномальні інструкції.	Виявлення атак на криптографічні модулі, зчитування активності під час експлуатації вразливостей.
Електромагнітний аналіз (EM Analysis)	Реєстрація електромагнітного випромінювання, яке генерується процесором під час виконання інструкцій.	Стороннє втручання, шпигунські закладки, витік даних через ЕМ-канали.	Дослідження апаратних бекдорів, аналіз шкідливого ПЗ, що працює на низькому рівні.
Темпоральний аналіз (Timing Analysis)	Вимірювання часу виконання інструкцій і затримок.	Атаки на кеш, експлуатація вразливостей спекулятивного виконання, приховані інструкції.	Розслідування атак Spectre/Meltdown-типу, аналіз аномальних часових патернів.
Аналіз коливань тактової частоти (Clock Skew Analysis)	Відстеження змін стабільності та частоти тактового генератора.	Спроби зламати систему через зміну clock skew, приховане навантаження, несправності.	Виявлення прихованих обчислювальних процесів або шкідливих модифікацій мікропрограми.
Аналіз теплового профілю (Thermal Forensics)	Вимір температурних змін на корпусі або всередині чипа.	Перегрів через шкідливий код, нехарактерне навантаження, виконання прихованих інструкцій.	Діагностика майнерів, rootkit-ів, мікрофірмового шкідливого ПЗ.
Аналіз кеш-патернів (Cache Behaviour Analysis)	Відстеження поведінки кеш-пам'яті та її заповнення.	Side-channel атаки, атаки на кеш-лінії, приховані обчислення.	Розслідування атак типу Flush+Reload, Prime+Probe, Evict+Time.
Аналіз роботи шин (Bus Traffic Forensics)	Моніторинг даних, що передаються внутрішніми шинами процесора та пам'яті.	Несанкціоновані звернення, приховані DMA-операції, доступ до заборонених областей пам'яті.	Розслідування атак на периферію, firmware-бекдорів, апаратних троянів.

Інтеграція методів мікропроцесорної криміналістики у системи кіберзахисту підприємств або критичних об'єктів дозволяє підвищити точність моніторингу та скоротити час реагування на атаки. Аналіз паразитних енергетичних коливань може стати частиною багаторівневої стратегії безпеки, поєднуючи апаратний контроль із поведінковим моніторингом програмного забезпечення. Це забезпечує можливість виявлення атак, які приховані від традиційних засобів логування та мережевого аналізу, і сприяє формуванню більш ефективних методів захисту високотехнологічних систем.

Висновки. Мікропроцесорна криміналістика відкриває новий підхід до аналізу кіберзагроз, концентруючись на паразитних енергетичних коливаннях, що супроводжують роботу апаратних компонентів. Виявлення таких сигналів дозволяє ідентифікувати приховані атаки, які не фіксуються традиційними засобами безпеки, та формувати більш точні моделі кіберзахисту. Метод демонструє потенціал для інтеграції у сучасні багаторівневі системи моніторингу, що поєднують апаратний контроль, аналіз поведінки програмного забезпечення та прогнозування ризиків. Впровадження цього підходу здатне значно підвищити стійкість критичних об'єктів та корпоративних мереж до нових видів атак на апаратному рівні

Література

1. Гора І.В., Колесник В.А, Попович І.І. Цифрова криміналістика в забезпеченні діяльності з протидії злочинності. Науковий вісник Ужгородського Національного Університету, 2024. С. 63-70.

2. Інноваційні методи та цифрові технології в криміналістиці й судовій експертизі : монографія / [В. Ю. Шепітько, Г. К. Авдєєва, В. М. Шевчук та ін.] ; за заг. ред. В. Ю. Шепітька ; НДІ вивч. проблем злочинності ім. акад. В. В. Сташиса Нац. акад. прав. наук України. – Харків : Право, 2024. – 208 с.

3. Полотай О.І. Використання комп'ютерної криміналістики для забезпечення ефективного розслідування інцидентів інформаційної та кібербезпеки. Вісник ЛДУБЖД : зб. наук. праць. Львів : ЛДУБЖД, 2023. № 28. С. 73–80.

УДК 004

ПРОЄКТУВАННЯ СИСТЕМИ ВІДДАЛЕНОГО ДОСТУПУ НА БАЗІ WINDOWS SERVER ДЛЯ ОРГАНІЗАЦІЇ БЕЗПЕЧНОЇ РОБОТИ ПЕР-СОНАЛУ

Проданик Б.Б., Борзов Ю.О.
Львівський державний університет безпеки життєдіяльності

Анотація. *Розглянуто особливості розгортання захищеного середовища для віддаленої роботи співробітників на базі Windows Server. Проаналізовано переваги використання технології Remote Desktop Services (RDS) у поєднанні з Active Directory для централізованого обліку користувачів та захисту корпоративних даних..*

Ключові слова: *Windows Server, RDS, віддалений доступ, інформаційна безпека, Active Directory.*

Abstract. *The features of deploying a secure environment for remote work of employees based on Windows Server are considered. The advantages of using Remote Desktop Services (RDS) technology in combination with Active Directory for centralized user accounting and corporate data protection are analyzed*.

Key words: *Windows Server, RDS, remote access, information security, Active Directory.*

В умовах сучасних викликів, таких як воєнний стан та глобалізація бізнес-процесів, організація безпечного віддаленого доступу до робочих місць стає критично важливою задачею для будь-якого підприємства. Використання незахищених каналів зв'язку або неконтрольованих домашніх пристроїв працівників створює значні загрози для цілісності та конфіденційності корпоративних даних.

Метою даної роботи є проєктування системи віддаленого доступу на базі операційної системи Windows Server, що дозволяє забезпечити баланс між зручністю для користувача та високим рівнем інформаційної безпеки. Основним інструментом реалізації обрано роль Remote Desktop Services (RDS).

На відміну від класичних VPN-рішень, які надають доступ до мережі, але залишають дані на кінцевому пристрої користувача, технологія RDS дозволяє виконувати всі обчислювальні процеси безпосередньо на сервері підприємства. Користувач отримує лише зображення екрану, а реальні дані не покидають захищений периметр [1].

Процес розгортання системи включає наступні етапи:

1. Налаштування Active Directory (AD DS). Це фундаментальний етап для обліку користувачів. Створення домену дозволяє централізовано керувати правами доступу, політиками паролів та групами безпеки. Кожен працівник отримує унікальний ідентифікатор, що дозволяє чітко розмежувати доступ до ресурсів.

2. Конфігурація ролей RDS. Для повноцінної роботи системи розгортаються ключові компоненти: RD Session Host (сервер, де працюють користувачі), RD Connection Broker (балансування навантаження) та RD Gateway (шлюз для безпечного підключення з зовнішньої мережі через HTTPS).

3. Створення клієнтського доступу. Для кінцевого користувача процес входу максимально спрощений. Адміністратор генерує спеціальний .rdp файл (ярлик), який налаштований на з'єднання з RD Gateway. При запуску ярлика відбувається автентифікація через Active Directory. Після успішного входу користувач потрапляє на свій робочий стіл або отримує доступ до опублікованих додатків (RemoteApp), які виглядають так, ніби запущені локально.

Особливу увагу в проєкті приділено безпеці. Використання протоколу RDP поверх HTTPS шифрує трафік, захищаючи його від перехоплення (Man-in-the-Middle attacks). Крім того, на рівні політик GPO (Group Policy Object) налаштовується заборона на копіювання файлів між віддаленим сервером та локальним комп'ютером користувача, що унеможливлює витік інформації. Також обов'язковим є налаштування Network Level Authentication (NLA), що вимагає підтвердження особи користувача ще до встановлення повної сесії з сервером [2].

Висновки. Реалізація системи на базі Windows Server та RDS дозволяє створити єдину точку входу для працівників, забезпечити централізований облік через Active Directory та гарантувати, що всі робочі інструменти використовуються виключно у захищеному мережевому середовищі підприємства. Крім того, такий підхід мінімізує ризики інсайдерських загроз та зовнішніх атак.

Література

1. Таненбаум Е., Везерал Д. Комп’ютерні мережі. 5-те вид. Київ: Видавнича група BHV, 2016. 960 с.

2. Microsoft Learn. Remote Desktop Services architecture. URL: https://learn.microsoft.com/en-us/windows-server/remote/remote-desktop-services/rds-architecture

УДК 004.934:004.056.5

МОНОКУЛЯРНА ОЦІНКА ГЛИБИНИ ЯК ЗАСІБ ПІДВИЩЕННЯ НАДІЙНОСТІ БІОМЕТРИЧНОЇ АВТЕНТИФІКАЦІЇ

Ростислав РОПНІЦКИЙ[1], Ростислав ТКАЧУК[1,2], Андрій ІВАНУСА[2]
[1]Національний університет «Львівська політехніка
[2]Львівський державний університет безпеки життєдіяльності

Анотація. *Біометрична автентифікація за зображенням обличчя широко використовується у цифрових сервісах, однак залишається вразливою до презентаційних атак через друковані фото, відеоповтори з екрана або прості маски. Наявність глибинних ознак суттєво підсилює перевірку живості, але у реальних системах спеціалізовані RGB-D або ІЧ сенсори доступні не завжди. Робота пропонує застосування монокулярної оцінки глибини з однієї RGB камери для формування додаткової 3D ознаки у каналі автентифікації. Ключова ідея полягає у прогнозуванні відносної карти глибини обличчя та інтеграції її у модуль прийняття рішення як просторового критерію живості і відповідності шаблону. Очікуваний ефект полягає у підвищенні стійкості до 2D атак без зміни апаратної платформи, зберігаючи вимоги реального часу і сумісність з наявними моделями розпізнавання.*

Ключові слова *біометрична автентифікація, перевірка живості, монокулярна глибина, карти глибини обличчя, презентаційні атаки, комп'ютерний зір.*

Abstract. *Face based biometric authentication is widely adopted in digital services, yet it remains vulnerable to presentation attacks such as printed photos, screen replays, or simple masks. Depth cues significantly strengthen liveness detection, but dedicated RGB-D or infrared sensors are not always available in practical deployments. This paper considers the use of monocular depth estimation from a single RGB camera to obtain an additional 3D cue within the authentication pipeline. The core idea is to predict a relative facial depth map and fuse it with the decision module as a spatial liveness and template consistency criterion. The anticipated outcome is improved resistance to 2D spoofing without changing the hardware platform, while preserving real time constraints and compatibility with existing face recognition models..*

Key words*: biometric authentication, liveness detection, monocular depth estimation, facial depth maps, presentation attacks, computer vision*.

Основний канал ризику у біометричній автентифікації за обличчям пов'язаний із тим, що класичні RGB-ознаки відображають переважно текстурні та фотометричні характеристики, які можуть відтворюватися на двовимірних носіях із високою точністю. Біометрична автентифікація в цілому базується на стабільних фізіологічних або поведінкових характеристиках людини, тоді як розпізнавання обличчя стало найбільш поширеним методом завдяки безконтактності та доступності стандартних камер як сенсорів. У типовому конвеєрі роботи таких систем виконуються етапи детекції та вирівнювання обличчя, формування ембеддингу та його порівняння з еталонними представленнями за метричними критеріями. Ця процедура забезпечує високу точність на контрольованих наборах даних, проте одночасно підвищує чутливість системи до реальних спотворень і атак на біометричні ознаки.

Сучасні методи перевірки живості базуються на аналізі мікротекстур, природних мікрорухів та оптичних артефактів, проте їх ефективність знижується при зміні освітлення, ракурсу та якості зображення. Додаткові фактори, такі як макіяж, аксесуари або висока зовнішня подібність між особами, ускладнюють класифікацію та підвищують ризик помилкових допусків і відмов. Найбільш критичними залишаються презентаційні атаки з використанням фотографій і відео, оскільки вони експлуатують плоску природу RGB-зображень. Застосування просторових ознак, зокрема глибини або альтернативних каналів, підвищує надійність автентифікації, дозволяючи відрізняти реальну тривимірну геометрію обличчя від плоских підробок та формувати незалежний від текстури критерій живості [1].

Інструменти прогнозування глибини з одиночного кадру останніми роками еволюціонували від задач загального сценного аналізу до прикладних сценаріїв, де необхідно відновлювати відносні карти глибини локальних об'єктів. У контексті біометричної автентифікації, така карта для обличчя відтворює його просторовий профіль і надає додаткову, комплементарну інформацію про форму, яка є більш стійкою до змін освітлення, макіяжу, аксесуарів або текстури шкіри, оскільки базується на геометрії, а не на фотометричних характеристиках. У практичних реалізаціях використовуються моделі на кшталт MiDaS, здатні формувати відносні глибинні поля з RGB кадру та адаптувати їх під обличчя як окремий сценний підоб'єкт. Результати попередніх досліджень і прикладних експериментів демонструють, що перехід у простір глибини відкриває нові дискримінативні ознаки, які не можуть бути повністю виловлені традиційним RGB описом. Спільне використання фотометричних та глибинних сигналів підвищує надійність і робастність біометричної автентифікації, забезпечуючи додатковий рівень захисту від презентаційних атак та інших спроб компрометації системи.

Роботи у сфері підвищення презентаційної стійкості демонструють, що комбінування RGB та глибинних ознак у двогілкових або багатозадачних нейронних мережах значно покращує розділення справжніх зразків від атак [1]. Дослідження, присвячені відновленню та уточненню глибинних даних обличчя, підтверджують придатність однокадрових глибинних реконструкцій як джерела 3D-критерію у біометричних та захисних модулях [2].

Запропонований підхід передбачає інтеграцію монокулярної глибини як додаткового рівня ознак у стандартній системі автентифікації. На вхід подається RGB кадр обличчя, з якого одночасно формуються 2D ембеддинги та прогнозується відносна карта глибини. Через масштабну неоднозначність монокулярної оцінки використовується відносний профіль, який зберігає стабільні просторові співвідношення між ключовими зонами обличчя, забезпечуючи перевірку живості. Глибинний опис нормалізується та узгоджується з 2D областю інтересу, формуючи спільний просторово-фотометричний вектор. Новизна підходу полягає у використанні відносної геометричної ознаки як критерію живості в умовах відсутності апаратних глибинних сенсорів, коли канал RGB є єдиним джерелом спостереження.

Модель прийняття рішення одночасно оцінює ідентичність за ембеддингом та узгодженість 3D профілю, суттєво знижуючи ймовірність проходу більшості 2D підробок навіть при наближенні фотометричних характеристик до реальних (рис. 1).

Рисунок 1 – Схема інтеграції монокулярної карти глибини у конвеєр біометричної автентифікації

Ключовим прикладним результатом запропонованого підходу є істотне підвищення стійкості біометричної автентифікації до презентаційних атак, зокрема друкованих фотографій і відеоповторів, завдяки інтеграції просторового контролю на основі монокулярної оцінки глибини без потреби додаткового апаратного обладнання. Практична реалізація підходу передбачає використання компактних моделей прогнозування відносної глибини та оптимізованого злиття 2D і 3D ознак, що забезпечує збереження швидкодії та відповідності вимогам реального часу. Така архітектура є придатною для мобільних і вбудованих платформ із обмеженими обчислювальними ресурсами та не потребує модифікацій існуючих конвеєрів розпізнавання. Отже, запропоноване рішення забезпечує ефективне поєднання доступності апаратних засобів, високої надійності перевірки живості та практичної придатності для сучасних систем біометричної автентифікації.

Література

1. SA-UNet for face anti-spoofing with depth estimation / J. Chen et al. Proceedings of the conference on face anti-spoofing. 2022. P. 9. DOI: https://doi.org/10.1117/12.2623137.

2. Schlett T., Rathgeb C., Busch C. Deep learning-based single image face depth data enhancement. Computer vision and image understanding. 2021. Vol. 210. P. 103247. DOI: https://doi.org/10.1016/j.cviu.2021.103247.

3. Мних М., Ткачук Р. Л., Федина Б. І. Організація оперативного управління кібербезпекою компанії. Інформаційна безпека та інформаційні технології : зб. тез доповідей IV Міжнародної науково-практичної конференції, ІБІТ 2022. (Львів, 30 листопада 2022 р.). Львів : ЛДУБЖД, 2022. С. 30–32.

УДК 004.932.7

АЛГОРИТМІЧНА ПРОПАГАНДА: ЯК ШІ ВИКОРИСТОВУЄТЬСЯ У СТВОРЕННІ ФЕЙКОВИХ ВІДЕО ПРО ВІЙНУ

Христина СЕРЕДНИЦЬКА, Діана РАЙТА
Львівський державний університет безпеки життєдіяльності

Анотація. *У цій роботі розглядається використання технологій штучного інтелекту для створення фейкових відео у воєнному контексті. Показано, як модифікуються обличчя, голос і контекст відео для маніпуляції громадською думкою, деморалізації військових та підриву довіри до інформаційних джерел. Розглянуто психологічні наслідки таких технологій та шляхи протидії, включно з медіаграмотністю, технічними засобами виявлення фейків і маркуванням штучного контенту.*

Ключові слова*: алгоритмічна пропаганда, штучний інтелект, діпфейки, війна, психологічний вплив, дезінформація, медіаграмотність.*

Abstract*. This paper examines the use of artificial intelligence technologies to create fake videos in a military context. It shows how the face, voice, and context of the video are modified to manipulate public opinion, demoralize the military, and undermine trust in information sources. It examines the psychological consequences of such technologies and ways to counter them, including media literacy, technical means of detecting fakes, and labeling artificial content.*

Keywords*: algorithmic propaganda, artificial intelligence, deepfakes, war, psychological impact, disinformation, media literacy.*

У сучасному інформаційному середовищі, коли війна й збройні конфлікти стають не лише ареною фізичних дій, а й інформаційних війн, з'являються нові потужні інструменти маніпуляції. Одним із таких інструментів є застосування технологій штучного інтелекту у створенні фейкових відео та аудіо, що імітують реальні події, промови, інтерв'ю або заяви лідерів держав. Ці технології відкривають новий рівень алгоритмічної пропаганди коли не просто публікується підроблений текст чи зображення, а створюється відеоматеріал із рухомим зображенням, звуком, часто із залученням відомих осіб, що значно підвищує правдоподібність.

Метою цього матеріалу є розкрити механізми створення таких фейків; описати специфічно - для воєнного контексту загрози у тому числі психологічні, а також запропонувати напрямки реагування та протидії.

Діпфейки з'явилися майже одразу після повномасштабного вторгнення, дозволивши Росії використовувати штучний інтелект для маніпулювання вже існуючими відео. 16 березня 2022 року проросійські актори зламали веб-сайт українського ЗМІ та завантажили неякісно зроблений діпфейк президента України Володимира Зеленського. У відео підроблена версія Зеленського стверджувала, що він пішов у відставку, втік з Києва та

закликав Збройні Сили України здатися та врятувати свої життя. Відео отримало значне поширення через Telegram; наратив також поширився в ефірі після злому російською версією новинного каналу телеканалу «Україна 24», який був змінений, щоб повторити те саме повідомлення. Надзвичайно низька якість відео чітко дала зрозуміти, що це діпфейк, тому прокремлівські джерела в Telegram почали називати його фейком, одночасно вихваляючись, що йому все ж вдалося змусити деяких українських військових здатися.

Не завжди необхідно повністю генерувати відео «з нуля». Частіше використовують реальні кадри, які підмінюють за аудіо або змінюють підписи, видаляють або додають контекст, змінюють дату чи місце події.

Ще однією важливою аудіотактикою є ліпсинкінґ, під час якого справжнє відео покращується, щоб змінити вираз обличчя та вимову людини. Один із таких випадків стався після теракту в Крокус-Сіті-Холі в Москві 22 березня 2024 року. Прокремлівські джерела, намагаючись знайти докази «причетності України» до нападу, представили численні неправдиві історії та докази. Одна з них містила нібито інтерв'ю з Олексієм Даніловим, колишнім секретарем Ради національної оборони та безпеки України, в якому він заявив під час українського національного телемарафону, що Москва «дуже розважається» з приводу нападу. Російський канал НТВ, що належить державній енергетичній компанії «Газпром», транслював нібито інтерв'ю Данілового. Однак Данілов не з'являвся на українському телебаченні під час телемарафону. Саме відео було поєднанням двох різних інтерв'ю, накладених на фальшивий голос; навіть Шаян Сардарізде з BBC Verify підтвердив , що його голос був згенерований штучним інтелектом.

У конфліктній ситуації технології таких фейків отримують додаткову силу: висока емоційність, невизначеність, швидкий темп подій. Відео, що показує «зраду», «капітуляцію», «загибель багатьох» – легко викликає паніку або деморалізацію. Зокрема, у доповіді Center for Countering Disinformation (Україна) наведено випадки відео, які виявились глибокими фейками, але були націлені на українське військово-територіальне угруповання.

Проблема проникнення пропаганди в штучний інтелект є складною, але не безнадійною. Експерти і технологічні компанії вже обговорюють шляхи її вирішення.Насамперед пропонується контролювати дані, на яких навчаються моделі. Компанії мають ретельніше перевіряти джерела, виключати відомі пропагандистські сайти або ж не робити їх настільки важливими для ботів. На жаль, блокування декількох доменів не вирішить проблему. Потрібно використовувати алгоритми, що автоматично виявляють мережі дезінформації і відсіюють їх. Ба більше, в статті “How AI Can Help Stop the Spread of Misinformation” повідомляється, що алгоритми машинного навчання можуть значно перевершувати людську здатність у виявленні брехні. Крім того, має бути прозорість і маркування. Якщо чат-бот

посилається на джерело, користувач має одразу ж бачити, що це за джерело і звідки воно. І не можна забувати про заповнення інформаційних прогалин правдивим та якісним контентом. Найкращим інструментом для боротьби з пропагандою буде наповнення мережі правдивою та перевіреною інформацією. Наостанок — регулювання та співпраця з владою. Крім технічних рішень, потрібні й політичні ухвали. Варто пам'ятати, що інтернет не має кордонів, а інформаційна війна навколо ШІ масштабується по всьому світу

Література

1. Пропаганда атакує фейками з ШТУЧНИМ ІНТЕЛЕКТОМ |Хроніки інформаційної війни [Електронний ресурс] / Еспресо.TV. — Електрон. пов. текст. — Режим доступу: https://www.youtube.com/watch?v=rIgbZnShejU. — Дата звернення: 04.11.2025.

2. Нестерова М. Сучасні технології в арсеналі пропаганди: як Кремль використовує ШІ в інформаційній війні [Електронний ресурс] // UATV / FREEДОМ. — 2025. — 19 вер. — Режим доступу: https://uatv.ua/uk/suchasni-tehnologiyi-v-arsenali-propagandy-yak-kreml-vykorystovuye-shi-v-informatsijnij-vijni/. — Дата звернення: 04.11.2025.

3. Marushchak A. Countering AI-Powered Disinformation through National Strategies / A. Marushchak, S. Petrov, A. Khoperiya // Frontiers in Artificial Intelligence. — 2025. — Vol. 7. — Режим доступу: https://www.frontiersin.org/journals/artificial-intelligence/articles/10.3389/frai.2024.1474034/full. — DOI: 10.3389/frai.2024.1474034. — Дата звернення: 04.11.2025.

4. AI tools usage for disinformation in the war in Ukraine [Електронний ресурс] / Roman Osadchuk ; Digital Forensic Research Lab (DFRLab). — 2024. — 9 лип. — Режим доступу: https://dfrlab.org/2024/07/09/ai-tools-usage-for-disinformation-in-the-war-in-ukraine/. — Дата звернення: 04.11.2025

УДК 159.9:004.738

ПСИХОЛОГІЧНА СТІЙКІСТЬ СУСПІЛЬСТВА ЯК ЧИННИК ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

Володимир СИДОРЕНКО, Олександр ДОЦЕНКО
Інститут наукових досліджень з цивільного захисту
Національного університету цивільного захисту України, м. Київ

Анотація. *Розглядається психологічна стійкість суспільства як складова інформаційного захисту в умовах війни. Проаналізовано загрози інформаційних атак, роль критичного мислення, медіаграмотності, державної комунікації та соціальної згуртованості у формуванні психологічної стійкості населення та протидії дезінформації.* *Ключові слова: психологічна стійкість, інформаційний захист, війна, медіаграмотність, дезінформація, критичне мислення, суспільство, соціальна згуртованість, психологічна безпека*

В умовах гібридної війни та масштабних інформаційних атак психологічна стійкість суспільства набуває стратегічного значення. Сучасні інформаційно-психологічні операції (ІПсО) спрямовані не лише на підрив обороноздатності, а й на руйнування внутрішньої єдності, довіри до державних інституцій і морального духу населення. Тому формування психологічної стійкості громадян є ключовим елементом системи інформаційного захисту держави [1].

Психологічна стійкість суспільства – це здатність колективної свідомості зберігати емоційну рівновагу, критичне мислення та соціальну згуртованість під тиском інформаційних загроз. На індивідуальному рівні вона проявляється у вмінні не піддаватися паніці, адекватно реагувати на стрес і зберігати конструктивну поведінку. На колективному рівні – у підтримці соціальної довіри, взаємопідтримки та впевненості в спільній меті. Психологічна стійкість є основою інформаційного «імунітету» суспільства [2]. Під час війни інформаційний простір насичується величезною кількістю суперечливих повідомлень, що несуть наступні загрози:

- дезінформація та фейки, що викликають паніку або розчарування;
- маніпуляції через соціальні мережі, спрямовані на емоційний тиск;
- психологічна втома та інформаційне перевантаження, що знижують увагу й критичність сприйняття;
- цілеспрямовані ІПсО, що експлуатують страх, горе чи апатію населення [3].

Такі атаки можуть призвести до деморалізації, зниження довіри до влади та розколу суспільства.

Інформаційна безпека включає не лише технічний, а й соціально-психологічний компонент. Психологічна стійкість створює бар'єр, що зменшує ефективність ворожих інформаційних впливів. Її ключовими складовими є:

- критичне мислення (здатність розпізнавати маніпуляції та перевіряти факти);
- довіра до офіційних джерел та обережність у поширенні інформації;
- соціальна згуртованість (почуття єдності, що нейтралізує спроби посіяти розбрат);
- психологічна грамотність (уміння керувати власними емоціями й підтримувати інших).

Стійке суспільство є менш уразливим до фейків і панічних настроїв, отже більш захищеним інформаційно.

Формування психологічної стійкості є комплексним процесом, що включає освітні, інформаційні, соціальні та психологічні заходи за наступними напрямами:

1) освітня діяльність і медіаграмотність. Формування критичного мислення починається з освіти. Впровадження програм медіаграмотності у школах та університетах допомагає громадянам розпізнавати фейки, аналізувати інформацію, оцінювати джерела та уникати емоційних маніпуляцій [4];

2) прозора та своєчасна державна комунікація. Доступ до достовірної інформації через офіційні канали державних органів знижує рівень паніки та недовіри [1];

3) підтримка ментального здоров'я. Державні та громадські психологічні сервіси, гарячі лінії та онлайн-консультації допомагають громадянам справлятися зі стресом і тривожністю. Особлива увага приділяється ветеранам, військовослужбовцям та членам їхніх сімей, а також людям у прифронтових регіонах;

4) громадянська солідарність та соціальна згуртованість. Волонтерські ініціативи, культурні та спортивні заходи, громадські акції допомагають підтримувати колективне почуття єдності;

5) протидія дезінформації та інформаційне просвітництво. Проєкти на кшталт StopFake, Центру стратегічних комунікацій та інших платформ активно спростовують фейки і навчають населення розпізнавати маніпуляції [3, 5];

6) розвиток критичного мислення та навичок саморегуляції. Психологічна стійкість вимагає не лише знання, а й практичних умінь: управління емоціями, стресостійкість, уміння приймати рішення в умовах невизначеності;

7) міжнародний досвід та обмін практиками. Вивчення успішних моделей психологічної стійкості в інших країнах, обмін досвідом із партнерами НАТО, ЄС та ООН допомагає впроваджувати ефективні методики, адаптовані до українських реалій.

Українське суспільство під час повномасштабної війни 2022–2025 рр. продемонструвало високий рівень психологічної стійкості. Попри щоденні інформаційні загрози, кібератаки та масові спроби поширення дезінформації, громадяни зберегли віру у власні сили, довіру до Збройних Сил і готовність діяти спільно для захисту країни. Це стало можливим завдяки

комплексному підходу, який поєднав державну політику, медіаграмотність, активність громадянського суспільства та волонтерські ініціативи.

Державні структури, такі як Центр стратегічних комунікацій, своєчасно спростовували фейки та надавали громадянам достовірну інформацію, мінімізуючи паніку. Водночас широкомасштабна волонтерська діяльність, культурні події, ініціативи психологічної допомоги та взаємодопомога у громадах формували відчуття єдності та підтримки, що значно підвищувало стійкість населення. Особливо ефективною виявилася робота державних і громадських платформ, таких як StopFake, гарячі лінії психологічної підтримки, інформаційні кампанії з медіаграмотності, а також ініціативи з розвитку критичного мислення серед молоді. Ці заходи дозволили не лише нейтралізувати вплив дезінформації, а й підвищити готовність суспільства до спільних дій у кризових умовах.

Український досвід показує, що психологічна стійкість населення є не лише результатом індивідуальної витримки, а й комплексним ефектом координації держави, медіа, громадських організацій і самих громадян. Стійке суспільство стало важливою складовою національної оборони, рівнозначною армії чи кіберзахисту, і слугує прикладом для інших держав, що опинилися під інформаційним тиском та агресією.

Психологічна стійкість – це не лише риса особистості, а стратегічний ресурс держави. Вона формує інформаційний щит, який захищає суспільство від паніки, фейків і маніпуляцій. Формування цієї стійкості потребує спільних зусиль держави, освіти, медіа та кожного громадянина. У війні за свідомість людей перемагає не той, хто має більше інформації, а той, хто здатен мислити критично й залишатися внутрішньо сильним..

Література

1. Національна рада України з питань телебачення і радіомовлення. *Протидія дезінформації в умовах війни, українське законодавство та роль медіа.* URL: https://webportal.nrada.gov.ua/protydiya-dezinformatsiyi-v-umovah-vijny-ukrayinske-zakonodavstvo-ta-rol-media/ (дата звернення: 11.11.2025).

2. Корольова Н.Д., Матохнюк Л.О., Таран А.А. Психологічна стійкість молоді в умовах військової агресії. *Вісник Донецького національного університету імені Василя Стуса. Серія Психологічні науки*. 2025. Вип. 2(5). С. 72–79. DOI: 10.31558/2786-8745.2024.2(5).8.

3. StopFake.org. URL: https://www.stopfake.org/uk/ (дата звернення: 11.11.2025).

4. Ласкова-Ярмоленко А., Слинькова Т. Медіаграмотність в системі освіти: вимоги сучасності у сфері соціальної комунікації. *Педагогічні інновації: ідеї, реалії, перспективи*. 2024. Том 1. № 32 (2024). С 100–105. DOI: 10.32405/2413-4139-2024-1(32)-100-105.

5. Центр стратегічних комунікацій. URL: https://spravdi.gov.ua/ (дата звернення: 11.11.2025).

УДК 004.056.5:004.738.5

КОНЦЕПТУАЛЬНА МОДЕЛЬ МІНІМІЗАЦІЇ ВИТОКІВ ДАНИХ У КОРПОРАТИВНОМУ СЕРЕДОВИЩІ НА ОСНОВІ ПРИНЦИПІВ ZERO TRUST АРХІТЕКТУРИ

Анастасія СОРОКА, Валентина ЯЩУК, Валерія БАЛАЦЬКА
Львівський державний університет безпеки життєдіяльності

Анотація. *Запропоновано концептуальну модель мінімізації витоків даних у корпоративному середовищі, засновану на принципах архітектури Zero Trust. Проаналізовано обмеження традиційних периметрових моделей безпеки та обґрунтовано необхідність переходу до динамічної системи довіри, де кожна взаємодія перевіряється у режимі реального часу. Визначено три базові рівні моделі — ідентифікаційно-контрольний, сегментаційно-політичний і моніторингово-аналітичний. Показано, що реалізація Zero Trust-підходу дає змогу зменшити ризики витоків даних і підвищити рівень кіберстійкості корпоративної інфраструктури.*

Ключові слова: *Zero Trust, кібербезпека, витік даних, корпоративне середовище, мікросегментація, політики доступу, кіберстійкість.*

Abstract. *A conceptual model for minimizing data leaks in a corporate environment is proposed, based on the principles of the Zero Trust architecture. The limitations of traditional perimeter security models are analyzed and the need to transition to a dynamic trust system is justified, where each interaction is checked in real time. Three basic levels of the model are identified - identification and control, segmentation and policy, and monitoring and analysis. It is shown that the implementation of the Zero Trust approach allows you to reduce the risks of data leaks and increase the level of cyber resilience of corporate infrastructure.*

Keywords: *Zero Trust, cybersecurity, data leakage, corporate environment, microsegmentation, access policies, cyber resilience.*

У сучасному корпоративному середовищі, що характеризується високим рівнем цифровізації бізнес-процесів, використанням хмарних сервісів та зростанням кількості віддалених користувачів, питання забезпечення конфіденційності й цілісності даних набуває стратегічного значення. Традиційні периметрові моделі захисту більше не відповідають сучасним викликам, адже межі корпоративних мереж стають розмитими, а дані циркулюють між внутрішніми й зовнішніми середовищами. У цих умовах особливого значення набуває архітектура Zero Trust (ZTA), побудована на принципі «ніколи не довіряй, завжди перевіряй». Концепція передбачає відмову від довіри за замовчуванням, застосування постійної автентифікації користувачів і пристроїв, а також мінімізацію рівня доступу відповідно до контексту ризику.

Метою даного дослідження є розроблення концептуальної моделі мінімізації витоків даних у корпоративному середовищі на основі принципів Zero Trust, що поєднує ідентифікаційні, політичні та аналітичні механізми безпеки в єдину динамічну систему управління довірою.

Запропонована концептуальна модель мінімізації витоків даних у корпоративному середовищі базується на трирівневій архітектурі, що інтегрує принципи Zero Trust із сучасними технологіями ідентифікації, сегментації та аналітичного моніторингу. Така багаторівнева структура забезпечує комплексне покриття основних етапів життєвого циклу даних — від доступу до виявлення та реагування на інциденти — і спрямована на усунення довіри за замовчуванням у будь-яких взаємодіях між користувачами, пристроями та сервісами.

Ідентифікаційно-контрольний рівень виконує функції автентифікації, авторизації та перевірки цілісності взаємодій у реальному часі. У межах цього рівня передбачено впровадження багатофакторної автентифікації (MFA), що поєднує щонайменше два незалежні фактори — знання (пароль), володіння (токен, мобільний пристрій) та біометричний параметр (відбиток пальця, розпізнавання обличчя). Додатково застосовується поведінкова аналітика, яка аналізує шаблони активності користувача (час входу, місце, тип пристрою, характер дій) для формування динамічної оцінки ризику. Система контекстного доступу приймає рішення про дозвіл чи блокування операції з урахуванням поточних умов — геолокації, статусу пристрою, рівня загрози в мережі. Таким чином, доступ до даних здійснюється лише за умови відповідності всім політикам безпеки, що значно знижує ризик компрометації облікових записів та внутрішніх загроз.

Сегментаційно-політичний рівень забезпечує просторову і логічну ізоляцію інформаційних потоків у межах корпоративної інфраструктури. Ключовим механізмом є мікросегментація, що передбачає поділ мережі на ізольовані домени з мінімально необхідними маршрутами взаємодії між ними. Такий підхід запобігає горизонтальному переміщенню зловмисників після первинного проникнення. Для керування доступом використовуються контекстно-залежні політики, зокрема RBAC (Role-Based Access Control) — доступ на основі ролей користувачів, ABAC (Attribute-Based Access Control) — доступ, що враховує динамічні атрибути (місце, час, пристрій, рівень ризику), та Risk-Based Access, який автоматично адаптує рівень доступу залежно від оціненого ризику конкретної сесії. Усі політики реалізують принцип найменших привілеїв (Least Privilege), згідно з яким користувач або процес отримує лише ті права, які необхідні для виконання конкретних завдань. Це мінімізує наслідки можливих витоків та обмежує масштаб потенційних інцидентів.

Моніторингово-аналітичний рівень виконує функції спостереження, виявлення аномалій і реагування на загрози. Центральним елементом цьо-

го рівня є системи управління інформаційною безпекою (SIEM), які здійснюють кореляційний аналіз подій із різних джерел — серверів, робочих станцій, мережевого обладнання, хмарних сервісів. Для підвищення точності детекції застосовуються алгоритми машинного навчання та штучного інтелекту, які здатні самостійно формувати профілі нормальної поведінки системи та виявляти відхилення, що можуть свідчити про витік або спробу несанкціонованого доступу. Також впроваджується механізм адаптивного реагування, який дозволяє автоматично змінювати політики доступу, ізолювати підозрілі вузли або активувати процедури інцидент-респонсу в режимі реального часу.

Загалом, взаємодія трьох рівнів забезпечує замкнений цикл безпеки, де автентифікація, сегментація та моніторинг утворюють самопідсилювальну систему динамічного контролю довіри. Така архітектура дозволяє не лише мінімізувати ризики витоків даних, а й формує основу для побудови адаптивної кіберстійкої корпоративної екосистеми, здатної ефективно функціонувати в умовах постійної еволюції цифрових загроз. Інтеграція цих рівнів у єдину архітектуру дозволяє реалізувати динамічну модель довіри, яка зменшує ризик несанкціонованого доступу, внутрішніх порушень і компрометації облікових даних. За результатами аналітичного моделювання доведено, що застосування Zero Trust-підходу може знизити ймовірність витоку даних на 70–80% у порівнянні з традиційними стратегіями захисту.

Запровадження Zero Trust-архітектури у корпоративному середовищі є ефективним кроком до формування проактивної системи безпеки, орієнтованої на мінімізацію ризиків витоків даних і підвищення кіберстійкості організації. Подальші дослідження доцільно спрямувати на створення інтегрованих моделей Zero Trust для мультихмарних середовищ та розроблення алгоритмів автоматичного управління політиками довіри у динамічних цифрових екосистемах.

Література

1. Kindervag, J. (2010). Build security into your network’s DNA: The Zero Trust network architecture. Forrester Research.

2. Ящук В.І., Івануса А.І., Маслова Н.О., Ткачук Р.Л., Брич Т.Б. Концептуалізація інтегративного використання баз даних вразливостей у контексті системного менеджменту інформаційної безпеки // Вісник Львівського державного університету безпеки життєдіяльності. – 2025. – Т. 31. – С. 59–61

3. Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero Trust Architecture (NIST SP 800-207). National Institute of Standards and Technology.

4. Scarfone, K., & Jansen, W. (2021). Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security (NIST SP 800-46 Rev. 2). National Institute of Standards and Technology

УДК 004.056.5:659.126:342.9

КІБЕРБЕЗПЕКА В ЦИФРОВОМУ МАРКЕТИНГУ: ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ У РЕКЛАМНИХ КАМПАНІЯХ

Артем СУКАЧ, Валентина ЯЩУК, Наталія ФЕДИНЕЦЬ
Львівський державний університет безпеки життєдіяльності

Анотація. *Досліджено питання захисту персональних даних у цифровому маркетингу та методи їх подолання. Досліджується вплив законодавства (зокрема GDPR), технічних засобів захисту та практик прозорості брендів на довіру споживачів. Представлено результати аналізу сучасних випадків витоків даних, а також опитування маркетологів щодо ступеня готовності до ризиків і впровадження засобів захисту. Делегується модель рекомендацій, яка поєднує юридичні, технічні та організаційні підходи.*

Ключові слова: *цифровий маркетинг, персональні дані, кібербезпека, GDPR, довіра споживачів.*

Abstract. *The issue of personal data protection in digital marketing and methods for overcoming them are investigated. The impact of legislation (in particular, GDPR), technical protections and brand transparency practices on consumer trust is investigated. The results of the analysis of modern cases of data leaks are presented, as well as a survey of marketers on the degree of readiness for risks and the implementation of protections. A recommendation model is proposed that combines legal, technical and organizational approaches.*

Keywords: *digital marketing, personal data, cybersecurity, GDPR, consumer trust.*

Зростання ролі персоналізації та масштабного збору даних в рекламних кампаніях призводить до підвищених ризиків витоків інформації, зловживань та порушень конфіденційності. Регулювання (GDPR, інші міжнародні та національні норми) змушує компанії адаптуватися, але технічні та організаційні прогалини залишаються. Тема є важливою для забезпечення законності, етики та збереження репутації брендів. Проблеми, перераховані вище, та їхня актуальність зумовили вибір теми статті, визначили її мету та завдання. Метою дослідження є визначення методичних підходів до оцінювання існуючих загроз для персональних даних у цифровому маркетингу та формування комплексної моделі захисту, яка може бути застосована у підприємствах різного масштабу. Об’єкт дослідження є процеси збору, обробки та використання персональних даних у рекламних кампаніях цифрового маркетингу. Предметом дослідження є

методи, технології і організаційні практики, які забезпечують захист персональних даних.

Аналіз літературних джерел [1-11] дозволив зробити висновки, що найпоширенішими загрозами у цифровому маркетингу є зловмисні рекламні мережі (malvertising), фішинг, несанкціонований доступ через слабкі третьосторонні сервіси, внутрішні витоки. З опитування маркетологів випливає, що більшість визнає важливість стандартів захисту та шиф-

рування, але лише частина використовує багатофакторну автентифікацію та регулярні аудити [6-9, 11].

Сьогодні Регламент Європейського Союзу GDPR (General Data Protection Regulation) є фундаментальним нормативним актом у сфері захисту персональних даних, який визначає стандарти їхнього збору, обробки та зберігання. Для цифрового маркетингу він має стратегічне значення, оскільки саме маркетингові кампанії часто базуються на аналітиці поведінки користувачів. Відповідно до вимог GDPR, компанії зобов'язані отримувати явну та добровільну згоду на використання персональних даних, у тому числі через файли cookie, таргетовану рекламу чи email-розсилки. Регламент також забороняє автоматизоване профілювання без інформованої згоди суб'єкта даних і надає право на «забуття». Виконання вимог GDPR сприяє підвищенню рівня довіри споживачів, зміцненню репутації бренду та зменшенню ризику кібератак і витоків інформації. Таким чином, дотримання регламенту не лише забезпечує юридичну відповідність, але й формує етичну та безпечну екосистему цифрового маркетингу, у якій конфіденційність користувача виступає ключовою цінністю.

Досвід застосування GDPR показує, що вимоги до явної згоди, обмеження цілей збору, принцип мінімізації даних та прозорість політик суттєво підвищують довіру споживачів і знижують правові ризики.

Враховуючи викладене вище, виниакає потреба у створенні комплексу заходів, які включатимуть юридичні аспекти (комплекс з GDPR тощо), технічні засоби (шифрування, MFA, контроль доступу), організаційні практики (навчання персоналу, політика мінімізації даних, прозорість для клієнтів). На рис. 1 наведено структурну схему захисту персональних даних у цифровому маркетингу, яка поєднує юридичні, технічні та організаційні компоненти.

Запропонована схема базується на інтеграції юридичних, технічних та організаційних механізмів, спрямованих на зменшення ризиків витоку, зловживання чи несанкціонованого доступу до персональних даних користувачів у процесі реалізації рекламних кампаній. Її концепція відповідає принципам GDPR та сучасним підходам до інформаційної безпеки.

Юридичний компонент визначає нормативно-правові засади функціонування системи захисту даних. Він охоплює відповідність міжнародним стандартам — насамперед GDPR, а також національному законодавству щодо захисту персональних даних; політику прозорої згоди (explicit consent) користувачів на обробку даних; угоди про обробку даних між рекламодавцями, маркетинговими агентствами та платформами; регламент повідомлення про інциденти — обов'язок інформувати контролюючі органи та користувачів про витік протягом 72 годин. Юридичний компонент формує нормативне середовище, яке задає межі та стандарти безпечного поводження з даними.

Рисунок 1 – Структурна схема захисту персональних даних у цифровому маркетингу

Технічний рівень схеми покликаний забезпечити конфіденційність, цілісність та доступність персональної інформації. До основних інструментів належать шифрування даних під час зберігання й передавання (end-to-end encryption); багатофакторна автентифікація (MFA) для адміністраторів і маркетологів; контроль доступу на основі ролей (RBAC) і журналювання дій користувачів; регулярні аудити безпеки та тестування на проникнення; анонімізація або псевдонімізація даних, що мінімізує наслідки потенційного витоку. Завдяки технічним засобам досягається практична реалізація вимог GDPR щодо “privacy by design”.

Організаційний блок моделі спрямований на формування культури безпеки в компанії. Його елементами є навчання персоналу щодо політик конфіденційності та кібергігієни; впровадження політики мінімізації даних — збір лише необхідної інформації; внутрішній моніторинг та аудит дотримання правил обробки даних; прозорість для клієнтів — відкриті політики конфіденційності, зрозумілі повідомлення про cookies і права користувача; призначення відповідального за захист даних (Data Protection Officer). Організаційні заходи забезпечують сталість системи, зменшують людський фактор і сприяють довірі до бренду.

Запропонована структурна схема є системним підходом до забезпечення кібербезпеки цифрового маркетингу, що поєднує нормативне регулювання, технологічний захист і корпоративну культуру відповідального ставлення до даних. Її реалізація дозволяє не лише дотримуватися вимог законодавства, а й створює конкурентну перевагу завдяки підвищенню рівня довіри споживачів і зниженню репутаційних ризиків.

Захист персональних даних у цифровому маркетингу є невід'ємною умовою стійкості бізнесу у сучасному середовищі. Комплексний підхід, який поєднує законодавчі вимоги, технічні засоби та культурно-організаційні трансформації, здатний знизити ризики витоків та збільшити довіру споживачів. Для маркетингових компаній та рекламодавців надзвичайно важливо не лише відповідати нормативам, але й проактивно впроваджувати практики захисту для зміцнення брендової репутації.

Література

1. Durmuş Şenyapar H. Nurgül. Digital Marketing in the Age of Cyber Threats: A Comprehensive Guide to Cybersecurity Practices. The Journal of Social Science, 2024. (ResearchGate)

2. Rehman N. A., Hussain Syed Munassir. Cyber Security Challenges in Digital Marketing: Protecting Consumer Data in the Era of Big Data and AI. The Academic, 2025.

3. Oklander I., Data Protection in Digital Marketing. MIND Journal, 2023. (mindjournal.wseh.pl)

4. Security in Digital Marketing, Kobis P., Kisiołek A., Karyy O., Pawliczek A., Chmielarz G. Intersections of Niche Tourism and Marketing. Procedia Computer Science, 2024. (OUCI)

5. Cybersecurity in Digital Marketing: Protecting Customer Data and Brand Reputation. Octopus Intelligence, 2025. (octopusintelligence.com) Cybersecurity in Digital Marketing: Protecting Customer Data

6. Балацька В. С., Опірський І. Р. Забезпечення конфіденційності персональних даних і підтримки кібербезпеки за допомогою блокчейну // Кібербезпека: освіта, наука, техніка. – 2023. – № 4 (20). – С. 6–19. DOI: https://doi.org/10.28925/2663-4023.2023.20.619

7. Балацька В., Побережник В. 2024. Концепція застосування

блокчейн-технологій для підвищення захищеності персональних даних платформи «Дія»: відповідність вимогам GDPR та українському законодавству. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка». 2, 26 (Груд 2024), 268–290. DOI: https://doi.org/10.28925/2663-4023.2024.26.681

8. Балацька В., Дмитрів Н. Міжорганізаційний обмін конфіденційними персональними даними на основі дозвільного блокчейн // Кібербезпека: освіта, наука, техніка. – 2025. – № 2(29). – С. 178–193. – DOI: https://doi.org/10.28925/2663-4023.2025.29.875\

9. Ящук В. Захист об'єкта інформаційної діяльності шляхом впровадження інтегрованої системи безпеки / Ящук В., Мисько Р. // Інформаційна безпека та інформаційні технології: збірник доповідей V Міжнародної науково-практичної конференції, ІБІТ 2024, м. Львів, 27 листопада 2024 року. Львів, ЛДУ БЖД, 2024, 661 с. (С.328-331).

10. Ящук В.І. Моніторинг процесів функціонування інформаційно-комунікаційних систем / В. Ящук // ITSec: Безпека інформаційних технологій: матеріали XIII Міжнар. наук.-техн. конф., м. Львів, 9-11 трав. 2024 р. Л.: ЛНУ ім. І. Франка, 2024, 257 с. (С. 253-254.)

11. Ящук В.І Блокчейн технології при реалізації системи електронного голосування /В. Ящук, Н. Фединець // ITSec: Безпека інформаційних технологій: матеріали XIII Міжнар. наук.-техн. конф., м. Львів, 9-11 трав. 2024 р. Л.: ЛНУ ім. І. Франка, 2024, 257 с. (С.255-256.)

УДК 004.7:621.39

АНАЛІЗ МЕТОДІВ АРХІТЕКТУРНОЇ ОПТИМІЗАЦІЇ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ: ПЕРЕВАГИ ТА РИЗИКИ ZERO TOUCH PROVISIONING

Роман ТОПАЛА
Державний університет «Київський авіаційний інститут»

Анотація. *У роботі розглядаються зміни в підходах до управління телекомунікаційною інфраструктурою. Проведено оцінку як традиційних методів, так і технологій Zero Touch Provisioning (ZTP). Ключові вектори кіберзагроз при автоматизованому розгортанні мереж були визначені та запропоновані архітектурні рішення для нейтралізації цих загроз.*

Ключові слова: *телекомунікаційна інфраструктура, ZTP, автоматизація мереж, інформаційна безпека, людський чинник, DHCP-snooping, mTLS.*

Abstract. *The paper examines the changes in approaches to telecommunication infrastructure management. A comparative assessment of both traditional methods and Zero Touch Provisioning (ZTP) technologies is conducted. Key cyber threat vectors associated with automated network deployment are identified, and architectural solutions for the neutralization of these threats are proposed.*

Keywords: *telecommunication infrastructure, ZTP, network automation, information security, human factor, DHCP snooping, mTLS.*

У зв'язку з переходом від апаратно-орієнтованих до програмно-визначених архітектур сучасна телекомунікаційна інфраструктура відбувається значний перехід. Розширення кількості підключених пристроїв, впровадження стандартів зв'язку п'ятого покоління (5G) і зростання Інтернету речей (IoT) вимагають мережевих інженерів швидкості реакції, яку неможливо забезпечити ручним управлінням [2]. Людський фактор залишається основною проблемою класичних методів адміністрування. Повільне масштабування, неузгодженість конфігурацій і помилки при введенні команд є прикладами таких проблем. У цьому дослідженні розглядаються сучасні методи архітектурної оптимізації, зосереджуючись на технології «нульового дотику» (ZTP), яка розглядається як найбільш перспективний інструмент для мінімізації людського впливу [1]. Також розглядаються окремі загрози безпеці, пов'язані з цією технологією.

Огляд методів управління інфраструктурою.

Інтерфейс командного рядка (CLI) був історично основним методом керування мережевим обладнанням. Однак цей метод недостатньо масштабований, щоб надати повний контроль над пристроєм. У випадку, якщо потрібно змінити налаштування сотень маршрутизаторів, оператор змушений виконувати однотипні дії, що призводить до помилок. Використання скриптової автоматизації, такої як Python, Ansible або Terraform, було наступним кроком. Конфігурації можна тиражувати за допомогою цього методу, але він часто залежить від конкретного виробника обладнання (vendor

lock-in) і вимагає постійної підтримки коду скриптів [3]. Найсучаснішим методом є використання архітектури SDN (Software-Defined Networking) разом із Zero Touch Provisioning. У цьому підході мережевий пристрій «з коробки» не має попередньої конфігурації, але отримує її автоматично від центрального контролера при першому підключенні до мережі [2]. Такий підхід широко використовується у центрах обробки даних, хмарних інфраструктурах та розподілених мережах провайдерів (SD-WAN).

Аналіз технології Zero Touch Provisioning (ZTP).

Технологія ZTP базується на автоматичному завантаженні образу операційної системи та файлу конфігурації через мережу під час завантаження пристрою. Процес зазвичай ініціюється через протокол DHCP, який вказує пристрою адресу файлового сервера (TFTP/HTTP/HTTPS) [4].

Переваги ZTP. Головною перевагою є виключення інженера з процесу фізичного налаштування на об'єкті. Це критично важливо для розгортання мереж у важкодоступних локаціях або при масовому оновленні обладнання. По-друге, ZTP гарантує стандартизацію: усі пристрої отримують ідентичний, перевірений шаблон налаштувань («золотий образ»), що усуває проблему «дрейфу конфігурацій» [3]. По-третє, значно скорочується час введення системи в експлуатацію (Time-to-Market).

Недоліки та обмеження. До недоліків методу можна віднести складність первинної підготовки інфраструктури (Bootstrap-серверів). Якщо сервер конфігурацій недоступний, пристрій залишається непрацездатним. Крім того, налагодження помилок у процесі автоматичного завантаження є складнішим, ніж при ручному налаштуванні, оскільки інженер не бачить зворотного зв'язку від пристрою в реальному часі.

Загрози інформаційній безпеці в середовищі ZTP.

Незважаючи на переваги, впровадження ZTP створює нові вектори атак, які необхідно враховувати при проектуванні архітектури [5]:

1. Атака «Людина посередині» (Man-in-the-Middle). Якщо процес передачі файлу конфігурації не зашифрований (наприклад, використовується TFTP), зловмисник може перехопити трафік, проаналізувати його та отримати чутливі дані, такі як паролі адміністратора, ключі шифрування або топологію мережі.
2. Підміна сервера завантаження (Rogue DHCP). Зловмисник може розгорнути в локальній мережі власний DHCP-сервер, який спрямує нові пристрої на фальшивий сервер конфігурацій. Це дозволяє завантажити на обладнання шкідливе програмне забезпечення або конфігурацію з бекдорами.
3. Підключення неавторизованих пристроїв. Існує ризик, що зловмисник підключить свій пристрій до мережі, і система автоматично видасть йому робочу конфігурацію, надавши доступ до внутрішніх ресурсів компанії.

Шляхи вирішення проблем безпеки. Для нівелювання зазначених ризиків архітектурна оптимізація повинна включати комплекс захисних заходів [1]:

- Взаємна автентифікація (mTLS). Перехід від простих протоколів передачі файлів до HTTPS із взаємною перевіркою сертифікатів. Сервер конфігурацій повинен перевіряти сертифікат пристрою (підписаний виробником — IDevID), а пристрій — сертифікат сервера.
- Захист ланцюжка завантаження (Secure Boot). Використання криптографічної перевірки цілісності образу операційної системи перед її запуском. Це унеможливлює виконання модифікованого коду навіть у випадку успішної атаки на етапі передачі даних.
- Ізоляція мережі управління (Out-of-Band Management). Процес ZTP повинен відбуватися в ізольованому VLAN або через окремий фізичний порт, доступ до якого суворо обмежений.
- Валідація пристроїв (Device Fingerprinting). Використання стандартів на кшталт IEEE 802.1AR, що дозволяють однозначно ідентифікувати апаратне забезпечення перед наданням йому будь-яких налаштувань.

Висновки

Плани архітектурної оптимізації телекомунікаційної інфраструктури рухаються до повної автоматизації. Оскільки вона значно знижує операційні витрати та мінімізує людські помилки, технологія Zero Touch Provisioning є безальтернативним рішенням для масштабних систем. Однак недбале використання ZTP без оцінки конкретних небезпек безпеки може зробити мережу уразливою. На етапі початкового завантаження даних необхідно забезпечити конфіденційність і цілісність. Розробка адаптивних алгоритмів виявлення аномалій у процесі автоматизованого розгортання мереж буде центром подальшого дослідження.

Література

1. RFC 8572. Secure Zero Touch Provisioning (SZTP). Internet Engineering Task Force, 2019.

2. Stallings W. Foundations of Modern Networking: SDN, NFV, QoE, IoT, and Cloud. — Addison-Wesley Professional, 2016. — 544 p.

3. Widdix T. Infrastructure as Code: Managing Servers in the Cloud. — O'Reilly Media, 2020.

4. Cisco Systems. Zero Touch Provisioning: Advanced Security Considerations for Network Engineers. White Paper, 2023.

5. Гайдар Г. В., Поліщук С. П. Аналіз загроз безпеці в програмно-конфігурованих мережах // Сучасний захист інформації. — 2022. — № 4. — С. 55–62.

УДК 004.89:004.056.5:355.45

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ВИЯВЛЕННЯ ТА РЕАГУВАННЯ НА КІБЕРЗАГРОЗИ ПІД ЧАС ВІЙНИ

Фединець Н.І., Сорока А.А.
Львівський державний університет безпеки життєдіяльності

Анотація. *Сучасна війна характеризується активним використанням кіберпростору як арени бойових дій. Кібератаки стають важливою складовою гібридної агресії. В умовах постійної зміни тактик противника традиційні методи кіберзахисту виявляються недостатньо ефективними. Особливого значення набуває використання технологій штучного інтелекту (ШІ) для автоматизованого виявлення, аналізу та реагування на кіберзагрози*..

***Ключові слова**: кібербезпека, кіберзагрози, штучний інтелект, кіберзахист, моніторинг, кіберпростір*.

***Abstract**: Modern warfare is characterized by the active use of cyberspace as an arena for combat operations. Cyberattacks are becoming an important component of hybrid aggression. In the face of constantly changing enemy tactics, traditional methods of cyber defense are proving to be ineffective. The use of artificial intelligence (AI) technologies for automated detection, analysis, and response to cyber threats is becoming particularly important.*

***Keywords**: cybersecurity, cyber threats, artificial intelligence, cyber defense, monitoring, cyberspace*..

Під час війни зростає кількість і складність кібератак. Зазвичай вони мають цілеспрямований характер і супроводжуються психологічними або інформаційно-підривними операціями. Основними типами загроз є:

- DDoS-атаки на державні портали та критичну інфраструктуру;
- спроби зламу систем управління об'єктами енергетики, транспорту, зв'язку;
- фішингові кампанії, спрямовані на військових і волонтерів;
- дезінформаційні операції, що використовують соціальні мережі та чат-боти;
- злам урядових акаунтів і поширення фальшивих повідомлень [2].

У таких умовах людські ресурси кіберзахисту не можуть оперативно обробляти великий обсяг даних про інциденти. Виникає потреба у використанні інтелектуальних систем, здатних самостійно навчатися, виявляти аномалії та передбачати потенційні атаки.

Штучний інтелект забезпечує новий рівень проактивного кіберзахисту, дозволяючи не лише реагувати на загрози, а й передбачати їх. Одним із ключових напрямків його застосування є машинне навчання для виявлення аномалій [3]. Алгоритми аналізують поведінку користувачів, мережевий трафік та системні журнали з метою визначення відхилень від нормальної діяльності. Наприклад, системи на базі машинного навчання можуть виявити підозрілу активність ще до того, як атака розгорнеться повністю. Іншим ва-

жливим напрямком є використання нейронних мереж для класифікації шкідливого програмного забезпечення. Завдяки глибинному навчанню такі системи здатні швидко розпізнавати нові типи вірусів, троянів або експлойтів, навіть якщо їхні сигнатури раніше не були відомі. Значну роль також відіграє аналіз великих даних (Big Data Analytics), адже системи штучного інтелекту можуть обробляти терабайти журналів подій та телеметрії, оперативно виявляючи зв'язки між окремими інцидентами й формуючи цілісну картину кіберактивності противника. Окрім цього, активно застосовуються інтелектуальні системи реагування, або SOAR-платформи, які інтегрують функції автоматичного реагування на інциденти, що дозволяє мінімізувати час між виявленням загрози та її нейтралізацією.

Після початку широкомасштабної агресії Росії проти України у 2022 році значно активізувалося впровадження систем штучного інтелекту в оборонному та кібернетичному секторах. Українські структури кіберзахисту, зокрема CERT-UA та їхні партнери, активно використовують системи автоматичного моніторингу на основі технологій машинного навчання для аналізу шкідливого трафіку, виявлення аномальної активності та попередження кібератак на державні й приватні інформаційні ресурси [1]. Паралельно міжнародні технологічні компанії, такі як Microsoft, Google та Mandiant, застосовують алгоритми штучного інтелекту для прогнозування атак з боку російських хакерських угруповань, аналізу їхніх тактик і моделювання можливих сценаріїв кіберагресії. Водночас активну роль у протидії інформаційним загрозам відіграють волонтерські кіберспільноти, які залучають нейронні мережі для аналізу фішингових листів, відстеження бот-мереж, виявлення фейкових новин і дезінформаційних кампаній у соціальних мережах. У результаті штучний інтелект поступово стає невід'ємною частиною оборонної кіберінфраструктури України, підвищуючи її стійкість і ефективність. Завдяки можливості швидко обробляти великі обсяги даних, виявляти закономірності та реагувати на загрози в режимі реального часу, системи ШІ забезпечують такий рівень швидкості, точності та масштабованості реагування, який неможливо досягти лише зусиллями людини.

Попри значний потенціал і широкі можливості, використання систем штучного інтелекту в сфері кібербезпеки супроводжується низкою проблем і обмежень, які впливають на ефективність та надійність їхнього застосування. Однією з ключових проблем є висока залежність ШІ-моделей від якісних і репрезентативних даних. Для навчання таких систем необхідні великі масиви достовірної інформації, однак у воєнний час процес збору, перевірки та оновлення даних часто ускладнений через нестачу ресурсів, кібератаки на джерела даних чи обмежений доступ до інфраструктури. Це може призводити до зниження точності прогнозів або до хибних спрацьовувань. Ще одним серйозним викликом є можливість навмисного обману моделей, так званих adversarial attacks, коли противник модифікує вхідні дані або створює спеціальні патерни, здатні ввести систему в оману.

У результаті ШІ може неправильно класифікувати загрозу, пропустити атаку або, навпаки, помилково вважати безпечну активність підозрілою.

Не менш важливими є етичні та правові аспекти використання штучного інтелекту. Автоматизоване прийняття рішень у кібербезпеці несе ризик неправомірного блокування користувачів, обмеження доступу до інформації чи порушення прав людини у разі помилки алгоритму. Це вимагає створення чітких нормативних рамок, прозорих процедур аудиту моделей та механізмів людського контролю. Крім того, існує проблема нестачі кваліфікованих кадрів. Для ефективного управління системами ШІ потрібні фахівці, які одночасно володіють знаннями у галузях кібербезпеки, машинного навчання, аналітики даних та етики штучного інтелекту. Недостатня підготовка таких спеціалістів може знизити ефективність впровадження технологій та підвищити ризик помилок. Таким чином, хоча штучний інтелект відкриває нові можливості для посилення кіберзахисту, його використання потребує обережності, системного підходу та постійного вдосконалення як технічних, так і організаційних механізмів.

Подальший розвиток застосування штучного інтелекту у кібербезпеці має базуватися на комплексному підході, що поєднує технології, організацію та освіту. Важливим кроком є створення національних платформ кіберзахисту, які інтегрують алгоритми ШІ для виявлення та нейтралізації загроз у режимі реального часу, об’єднуючи інформацію з різних джерел і автоматизуючи реагування на інциденти.

Штучний інтелект відкриває нові можливості для ефективного управління інформаційною безпекою під час війни. Його застосування дозволяє виявляти невідомі раніше загрози, зменшувати час реагування та підвищувати стійкість державних і приватних кіберсистем. Разом із тим, необхідно враховувати етичні, правові та технологічні обмеження, забезпечуючи контроль людини над критичними рішеннями.

Література

1. Microsoft Threat Intelligence. *Defending Ukraine: Early Lessons from the Cyber War*, 2023. URL: https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/defending-ukraine-early-lessons-from-the-cyber-war.

2. Сердюков К.С. Інтелектуалізація кіберзахисту: роль штучного інтелекту у своєчасному виявленні аномалій в умовах еволюції гібридних загроз. №12. 2025. Актуальні питання економічних наук. URL: https://a-economics.com.ua/index.php/home/article/view/602.

3. Трофименко О. Г., Соколов А. В., Чикунов П. О. Штучний інтелект у військовій кіберсфері. Технології та інжиніринг. 2024. № 4 (21). С. 85-92.

УДК 004.056:005.8:355

ХМАРНІ ТЕХНОЛОГІЇ В УМОВАХ ВІЙНИ: БАЛАНС МІЖ МОБІЛЬНІСТЮ ТА БЕЗПЕКОЮ

Фединець Н.І., Конепуд М.І.
Львівський державний університет безпеки життєдіяльності

Анотація. *Сучасні військові та цивільні операції дедалі більше залежать від цифрових технологій, і хмарні сервіси стають ключовим елементом цієї трансформації. В умовах війни, коли оперативність, мобільність і адаптивність стають критично важливими, хмарні технології пропонують унікальні можливості для швидкого розгортання додатків, обміну даними та координації дій.*

Ключові слова. *хмарні технології, безпека, кіберзагрози, кібербезпека, кіберзахист, моніторинг, кіберпростір.*

Abstract. *Modern military and civilian operations are increasingly dependent on digital technologies, and cloud services are becoming a key element of this transformation. In wartime, when agility, mobility, and adaptability become critically important, cloud technologies offer unique opportunities for rapid application deployment, data exchange, and coordination.*

Keywords. *cloud technologies, security, cyber threats, cybersecurity, cyber defense, monitoring, cyberspace*

У контексті військових конфліктів та надзвичайних ситуацій значення хмарних технологій зростає, оскільки швидке реагування та мобільність підрозділів прямо залежать від можливості оперативно обмінюватися інформацією та приймати рішення на основі актуальних даних. Однак застосування хмарних технологій у військовій сфері пов'язане з ризиками інформаційної безпеки: витоки даних, кібератаки та несанкціонований доступ можуть мати критичні наслідки. Тому одним із ключових завдань є забезпечення балансу між мобільністю користувачів та захистом інформації. Хмарні сервіси надають користувачам можливість швидкого розгортання додатків, забезпечують доступ до інформації з будь-якої точки, що дозволяє військовим підрозділам працювати з даними в реальному часі, незалежно від географічного розташування [1]. Крім того, хмарні технології забезпечують масштабованість ресурсів, що дозволяє у випадку активізації операцій швидко збільшити обчислювальні потужності та зберігання даних без фізичних обмежень. Ці переваги роблять хмарні технології надзвичайно корисними в умовах війни, коли час і мобільність мають критичне значення.

Попри очевидні переваги, використання хмарних рішень супроводжується низкою загроз. Серед них – кібератаки та шкідливе програмне забезпечення, несанкціонований доступ до конфіденційних даних, що може призвести до втрати стратегічної інформації, а також залежність від

інтернет-з'єднання (відсутність стабільного зв'язку у зоні бойових дій може обмежити ефективність хмарних систем). Тому важливо застосовувати комплексний підхід до безпеки, включаючи шифрування даних, багаторівневу аутентифікацію та резервне зберігання критичних ресурсів.

Досягнення оптимального балансу між мобільністю та безпекою вимагає інтеграції технічних і організаційних заходів. Вибір правильної моделі хмарних сервісів, наприклад приватні або гібридні хмари, може забезпечити кращий контроль над чутливими даними [2]. Використання сучасних протоколів шифрування та ролевого доступу мінімізує ризики витоку інформації. Постійний моніторинг активності користувачів та загроз дозволяє швидко локалізувати проблеми, а навчання персоналу зменшує ймовірність помилок, які можуть призвести до порушення безпеки.

Література

1. Батаєв С.В., Мельник О.С. Аналіз принципів роботи, переваг та викликів у використанні хмарних технологій в умовах сьогодення. Вчені записки. 2024. URL: tech.vernadskyjournals.in.ua.

2. Колісниченко К. Хмарні технології та ризики інформаційної безпеки в умовах війни. Theoretical and Applied Cybersecurity : Матеріали III Всеукраїнської науково-практичної конференції (TACS-2025). 29 травня 2025 р. Київ, 2025. С. 219-222.

УДК 004.056:004.412.2

ВИЯВЛЕННЯ КІБЕРЗАГРОЗ У СКБД НА ОСНОВІ ПОВЕДІНКОВОЇ АНАЛІТИКИ ТА НЕКОНТРОЛЬОВАНОГО НАВЧАННЯ

Микола ЦІКО[1], Ростислав ТКАЧУК[1,2], Артур ТКАЧЕНКО[1]
[1]Львівський державний університет безпеки життєдіяльності
[2]Національний університет «Львівська політехніка»

Анотація. *У роботі представлено інтелектуальну систему виявлення аномальної активності в базах даних, спрямовану на підвищення інформаційної безпеки в умовах зростання обсягів даних та кіберзагроз. Проведено аналіз сучасних методів детекції аномалій, нормативних вимог і доступних рішень, що підтвердило потребу у створенні адаптивного та модульного програмного комплексу. Обґрунтовано вибір технологічного стеку (Python, FastAPI, Scikit-learn, PostgreSQL, React) і алгоритму Isolation Forest для обробки SQL-запитів у режимі реального часу. Система реалізована як мікросервісна архітектура, яка забезпечує збір, класифікацію та візуалізацію логів, підтримує перенавчання моделі та інтеграцію в корпоративну інфраструктуру.*

Ключові слова*: аномалії в базах даних, інформаційна безпека, поведінкова аналітика, машинне навчання, логування, детекція загроз, моніторинг активності, мікросервісна архітектура.*

Abstract. *The paper presents an intelligent system for detecting abnormal activity in databases, aimed at improving information security in the face of growing data volumes and cyber threats. An analysis of modern methods of anomaly detection, regulatory requirements and available solutions was conducted, which confirmed the need to create an adaptive and modular software package. The choice of a technology stack (Python, FastAPI, Scikit-learn, PostgreSQL, React) and the Isolation Forest algorithm for processing SQL queries in real time is justified. The system is implemented as a microservice architecture that provides collection, classification and visualization of logs, supports model retraining and integration into corporate infrastructure.*

Keywords: *anomalies in databases, information security, behavioral analytics, machine learning, logging, threat detection, activity monitoring, microservice architecture.*

У сучасному цифровому середовищі інформація є ключовим ресурсом для економіки, обороноздатності та суспільного функціонування, а обсяг даних, що перевищив 100 зетабайтів і подвоюється приблизно кожні два роки, створює серйозні виклики для кіберзахисту. Бази даних залишаються одними з найбільш вразливих елементів IT-інфраструктури: 44 % інцидентів безпеки пов'язані з неправомірним доступом до СКБД, з яких значна частка — внутрішні загрози [1]. Традиційні засоби захисту — автентифікація, контроль доступу, шифрування — не завжди виявляють нетипову активність користувачів, тому критично важливим стає впровадження систем виявлення аномалій (Anomaly Detection Systems), зокрема на основі алгоритму Isolation Forest. Нормативні вимоги GDPR та ISO/IEC 27001 [6] і резонансні витоки даних, як у Equifax [1], підкреслюють необхідність практичних, адаптивних і ефективних рішень на основі Python, PostgreSQL, FastAPI та сучасних веб-фреймворків.

Зростання обсягів і критичності даних у фінансових, медичних та державних сервісах актуалізує застосування поведінкової аналітики. Понад 80 % інцидентів у СКБД пов'язані з компрометацією доступу, а приклад Equifax (2017) демонструє наслідки відсутності ефективного автоматичного моніторингу [1]. Традиційні механізми захисту не здатні розпізнавати інсайдерські атаки чи поступові відхилення поведінки користувачів, тому машинне навчання для аналізу SQL-запитів, аутентифікаційних подій і логів у реальному часі стає найбільш ефективним способом виявлення загроз.

Предметна область дослідження охоплює широкий спектр об'єктів контролю — SQL-запити, процедури автентифікації, зміну прав доступу, мережеві транзакції — та різноманітні джерела даних, такі як transaction logs, query logs, audit logs і системні журнали. Для виявлення аномалій застосовуються статистичні підходи, методи кластеризації, outlier-детекція та нейромережеві моделі. У контексті практичних систем безпеки особливо цінними є неконтрольовані алгоритми, здатні самостійно формувати модель «норми» та виявляти відхилення без потреби у великих мічених вибірках [2, 3]. Алгоритм Isolation Forest, на якому базується створений модуль, має низку переваг — лінійну складність, стійкість до викидів, здатність працювати зі стримінговими даними, а також сумісність із Python-екосистемою, що робить його одним із найефективніших методів для систем реального часу [2, 4].

Аналіз сучасних промислових рішень (IBM Guardium, Oracle Audit Vault, McAfee DAM) показав їх високу технічну надійність та масштабованість, однак водночас — значну вартість, складність налаштування та обмежену адаптивність для малих і середніх організацій. Open-source платформи (OpenDLP, Apache Spot) є економічно доступними, але нерідко обмежені функціонально або потребують значних інженерних доопрацювань. Це підтвердило необхідність створення програмного рішення, яке поєднує надійність, доступність, модульність і адаптивність, та є реалістичним в умовах корпоративних IT-інфраструктур.

На підставі порівняльного аналізу методів детекції аномалій обрано Isolation Forest як найбільш збалансований підхід. Він дозволяє працювати без мічених даних, забезпечує масштабованість для опрацювання потоків логів, підтримує аналіз у режимі реального часу та має низькі вимоги до ресурсів. Інтеграція цього алгоритму з FastAPI, PostgreSQL і Python-модулями забезпечує високу продуктивність та стабільність роботи [5, 6], що підтверджує практичну доцільність його застосування у створеній системі.

Розроблена система виявлення аномальної активності має модульну багаторівневу архітектуру, що включає клієнтську частину на React, серверну логіку на FastAPI, модуль машинного навчання з Isolation Forest, PostgreSQL та допоміжні сервіси. Така структура забезпечує масштабованість, незалежний розвиток компонентів та можливість гнучкого розширення. Взаємодія між модулями реалізована через REST API, що дозволяє інтегрувати систему у різні корпоративні середовища без потреби у глибокій перебудові їхньої інфраструктури.

Модуль машинного навчання завантажує попередньо треновану модель Isolation Forest, аналізує нові лог-події в режимі реального часу та записує результати класифікації у таблицю query_logs PostgreSQL, з активацією системи сповіщень при виявленні критичних відхилень. Функція адаптивного перенавчання через endpoint /retrain-model підтримує актуальність моделі та стійкість системи до змін поведінки користувачів. Центральна таблиця query_logs оптимізована індексами та денормалізацією для швидкого виконання запитів і побудови аналітичних візуалізацій, а логічна модель дозволяє додавати сутності users, roles або alerts для подальшого розширення. Інтерфейс користувача реалізовано як адаптивний дашборд з таблицями логів, графіками, фільтрами, мультимовністю, темною/світлою темою та експортом PDF, що забезпечує оперативне оновлення даних і швидке реагування аналітиків на загрози.

Система демонструє високу практичну цінність, забезпечує автоматизований моніторинг поведінки користувачів та дозволяє значно зменшити ризики порушення безпеки даних, що робить її актуальним та надійним інструментом у сучасних умовах зростаючих кіберзагроз.

Література

1. World Economic Forum. The Global Risks Report 2023: 18th edition [Електронний ресурс]. – Режим доступу: https://www.weforum.org/reports/global-risks-report-2023.

2. Ahmed M., Mahmood A. N., Hu J. A survey of network anomaly detection techniques // Journal of Network and Computer Applications. – 2016. – Т. 60. – С. 19–31.

3. Ящук В. І., Івануса А. І., Маслова Н. О., Ткачук Р. Л., Брич Т. Б. Інтеграція баз даних вразливостей у СУІБ – шлях до підвищення кіберстійкості критичних систем, Resilient Systems: Secure Digital Technologies and Critical Infrastructure: Proceedings of 1st International Scientific and Practical Conference. Drohobych: Donetsk National Technical University, 2025. pp. 60–65.

4. Ткачук Р. Л., Ткаченко А. М., Андріїв Р. Р. Розроблення та застосування експлойтів з подальшою інтеграцією в ботнет. Безпека інформаційних технологій : матеріали XIII Міжнародної науково-технічної конференції ITSec-2024 (Львів, 9–11 травня 2024 р.). Львів : ЛНУ ім. І. Франка, 2024. С. 200–202.

5. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements. – Geneva: ISO, 2022. – 33 p.

6. Ящук В.І., Івануса А.І., Маслова Н.О., Ткачук Р.Л., Брич Т.Б. Концептуалізація інтегративного використання баз даних вразливостей у контексті системного менеджменту інформаційної безпеки. Вісник Львівського державного університету безпеки життєдіяльності : зб. наук. пр. Львів : ЛДУ БЖД, 2025. № 31. С. 126–139. DOI: https://doi.org/10.32447/20784643.31.2025.13

UDC 004.056.5

INTELLIGENT CYBERSECURITY SYSTEM BASED ON ARTIFICIAL INTELLIGENCE

Paola CINQUE
Institute of Printing Art and Media Technologies
Lviv Polytechnic National University

Abstract*. This paper presents a concept of an intelligent cybersecurity system that employs artificial intelligence algorithms for real-time detection and mitigation of cyber threats. The proposed architecture ensures adaptability, precise analytics, and efficient module interaction, enhancing the overall security of information systems through automated analysis and dynamic response mechanisms.*

Keywords*: cybersecurity, artificial intelligence, machine learning, deep learning, threats.*

Анотація*. У роботі розглянуто концепцію інтелектуальної системи кіберзахисту, що використовує алгоритми штучного інтелекту для автоматичного виявлення та нейтралізації загроз у режимі реального часу. Запропонована архітектура забезпечує адаптивність, точність аналізу та ефективну взаємодію модулів для підвищення рівня безпеки інформаційних систем.*

Ключові слова*: кіберзахист, штучний інтелект, машинне навчання, глибинне навчання, загрози.*

The paper examines modern approaches to building cybersecurity systems using artificial intelligence technologies. The fundamental principles of intelligent security systems are analyzed, as well as their advantages compared to traditional methods of detecting and neutralizing cyber threats.

Problem Statement and Relevance.

With the growing number of cyber threats and the increasing sophistication of attack techniques, classical antivirus systems are no longer able to promptly respond to new and previously unknown threats. This creates the need to implement intelligent solutions capable of autonomously analyzing network behavior, detecting anomalies, and adapting to dynamic changes in the environment.

Purpose of the Study.

The purpose of this work is to develop a conceptual model of an intelligent cybersecurity system that employs machine learning and artificial intelligence algorithms to enable automatic detection, analysis, and neutralization of cyber threats in real time.

Research Description

The proposed system consists of several functional modules that provide a comprehensive approach to cybersecurity.

The data acquisition module captures network activity and system events, ensuring continuous monitoring of all elements within the information infra-

structure. The AI-powered analytical module performs classification and prediction of potential threats using modern machine learning and deep learning algorithms, enabling the identification of hidden or complex attack patterns.

The decision-making module determines an appropriate response to suspicious behavior by assessing risks and prioritizing security measures. The response module automatically blocks or isolates malicious processes, minimizing the impact on users and critical resources.

The use of deep learning technologies enables the system to continually improve attack detection accuracy, adapt to new threat types, and effectively forecast their development. Cloud-based infrastructure ensures continuous data exchange between nodes, facilitating collaborative analysis and the creation of more precise cybersecurity models. Furthermore, the integration of all modules into a unified system provides scalability, flexibility, and the ability to gradually enhance algorithms based on accumulated experience and analytical insights.

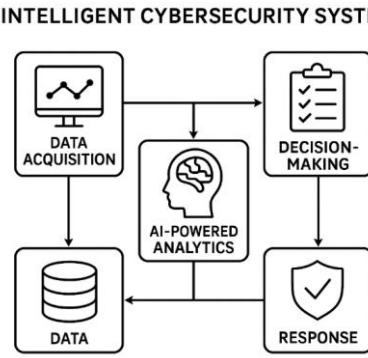

Figure 1 – Hierarchical structure of the AI-based intelligent cybersecurity system

Conclusions.

The application of artificial intelligence in cybersecurity enables proactive threat response, reduces the time required to detect attacks, and increases the overall efficiency of security systems. This approach forms the foundation for creating new adaptive systems capable of operating effectively in a rapidly evolving cyber environment.

References

1. Chen, T., Zhang, H., & Li, Y. (2021). AI-driven cybersecurity: Trends, challenges, and future directions. IEEE Access, 9, 12345–12359.

2. Al-Mhiqani, M., et al. (2022). Deep learning approaches for network intrusion detection: A review. Computers & Security, 114, 102594.

3. Zhang, X., Wang, S., & Liu, J. (2020). Intelligent cyber defense systems based on machine learning and cloud architecture. Journal of Information Security and Applications, 53, 102541

UDC 004.056.5:004.738.5

IMPLEMENTATION OF ZERO-TRUST ARCHITECTURE WITH BLOCKCHAIN-BASED ACCESS AUDIT FOR CLOUD STORAGE SECURITY

Kamelia CINQUE
Institute of Printing Art and Media Technologies
Lviv Polytechnic National University

Abstract. *The vulnerabilities of traditional perimeter-based security in cloud environments were analyzed. A Zero-Trust architecture integrated with blockchain technology for immutable access logging was proposed. The implementation framework ensures continuous verification and transparent audit trails for sensitive data protection.*

Keywords. *Zero-Trust architecture, blockchain, cloud security, access control, audit trail.*

Анотація. *Проаналізовано вразливості традиційної периметральної безпеки у хмарних середовищах. Запропоновано архітектуру Zero-Trust з інтеграцією blockchain для незмінного журналювання доступу. впровадження забезпечує безперервну верифікацію та прозорі аудиторські сліди для захисту чутливих даних.*

Ключові слова: *архітектура Zero-Trust, blockchain, хмарна безпека, контроль доступу, аудиторський слід.*

The increasing adoption of cloud storage solutions has significantly changed how organizations handle their digital assets. Traditional security approaches based on network perimeter defense are proving insufficient for protecting against contemporary security threats. Enterprises handling sensitive intellectual property, confidential client data, and proprietary business information face critical challenges in securing cloud-stored assets against both external threats and insider risks. Current statistics indicate that 34% of data breaches involve insider threats, while 82% of cloud security incidents stem from misconfigured access controls and insufficient audit capabilities.

The fundamental weakness of conventional cloud security lies in its implicit trust model. Once authenticated, users typically gain broad access to resources based on their network location or initial credential verification. This approach becomes particularly problematic when employees access cloud systems from various locations and devices, creating multiple potential compromise points. Modern work environments require access to sensitive data from factory floors, remote offices, home networks, and mobile devices, significantly expanding the attack surface. A single compromised credential can provide an attacker with extensive access to confidential information, with the breach potentially remaining undetected for extended periods due to inadequate real-time monitoring.

Analysis of current security infrastructure in typical enterprise environments revealed several critical deficiencies. First, access decisions rely primarily on initial authentication without continuous verification of user identity and device security posture throughout the session. Second, the absence of granular, context-aware access controls means that users often possess excessive permissions beyond their immediate operational requirements. Third, audit logs stored within the same cloud provider's infrastructure are vulnerable to tampering by privileged users or attackers who gain administrative access, compromising forensic capabilities and compliance verification.

The proposed solution implements a Zero-Trust architecture fundamentally reconceptualizing cloud security by eliminating implicit trust and enforcing continuous verification. The core principle states: "Never trust, always verify." Every access request undergoes real-time evaluation regardless of its origin, user identity, or previous authentication status.

Each access event generates a cryptographic hash containing the timestamp, user identity, accessed resource, action performed, and contextual parameters. This hash is recorded as a transaction on a private blockchain network, creating a permanent, tamper-evident record. Any attempt to modify historical access logs would require changing the entire blockchain, which is computationally infeasible and immediately detectable through hash verification.

The Zero-Trust architecture operates as a central verification engine that continuously evaluates trust signals from multiple sources (Figure 1). Unlike traditional perimeter-based security, this model treats users, devices, locations, cloud applications, private clouds, and data centers as independent verification points that must collectively validate each access request.

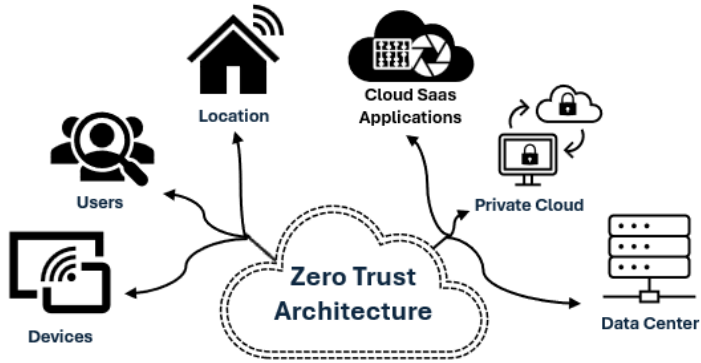

Figure 1 – Zero-Trust Architecture: Central Verification Hub with Multiple Trust Signals

As shown (Figure 1), every connection passes through the Zero-Trust verification hub regardless of origin. This ensures that no single compromised element can grant full access to protected resources.

The system integrates with existing cloud infrastructure through API connections, avoiding the need for complete platform migration. Machine learning algorithms continuously refine behavioral models and threat detection capabilities based on accumulated access patterns and security events. Regular blockchain audits provide compliance verification for industry regulations and data protection requirements.

Thus, implementing Zero-Trust architecture with blockchain-based audit capabilities represents a paradigm shift in cloud security for modern enterprises. The combination of continuous verification, dynamic access control, and tamper-proof logging provides comprehensive protection against contemporary threat vectors while ensuring regulatory compliance and maintaining operational efficiency. This approach establishes a robust security foundation capable of protecting valuable intellectual property and sensitive business data in an increasingly hostile cyber environment.

References

1. Rose S., Borchert O., Mitchell S., Connelly S. Zero Trust Architecture. NIST Special Publication 800-207. 2020. 59 p.

2. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. 9 p.

3. Gartner Inc. Market Guide for Zero Trust Network Access. 2023. 45 p.

4. Kshetri N. Blockchain's roles in meeting key supply chain management objectives. International Journal of Information Management. 2018. Vol. 39. P. 80-89.

УДК 004.056.5

КОМБІНОВАНІ КРИПТОГРАФІЧНІ ТА СТЕГАНОГРАФІЧНІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

Паола ЧІНКУЕ
Інститут поліграфії та медійних технологій НУ «Львівська політехніка»

Анотація. *У роботі розглянуто комбінований підхід до захисту інформації, що поєднує криптографію та стеганографію. Запропоновано модель, у якій дані спочатку шифруються, а потім приховуються в графічному контейнері. Оцінено стійкість системи та її переваги над традиційними методами.*

Ключові слова: *криптографія, стеганографія, захист даних, прихований канал, інформаційна безпека*

Abstract. *The paper examines a combined information protection approach integrating cryptography and steganography. A model is proposed where data is first encrypted and then hidden inside an image container. The system's security, resistance to detection, and advantages over conventional protection methods are analyzed.*

Keywords: *cryptography, steganography, data protection, covert channel, information security.*

Сучасні кіберзагрози потребують багаторівневих методів захисту, здатних забезпечити як конфіденційність інформації, так і прихованість самого факту її передавання. Традиційні криптографічні алгоритми ефективно захищають зміст даних, проте не забезпечують маскування процесу комунікації. Стеганографічні системи, навпаки, дозволяють приховати факт передавання, але без криптографічного підсилення їх стійкість суттєво знижується. Тому поєднання цих двох підходів набуває особливої актуальності в умовах зростання інтенсивності інформаційних атак.

Метою роботи є розроблення комбінованої моделі захисту інформації, що інтегрує криптографічні та стеганографічні методи з метою створення прихованого каналу зв'язку, стійкого до аналізу та перехоплення. Для цього запропоновано архітектуру, у якій дані спочатку шифруються криптографічним модулем, а потім приховуються у графічному контейнері з використанням стеганографічного модуля. Загальна структура системи подана на рис. 1.

Запропонована система реалізує чітко розмежовані етапи обробки даних. На першому етапі формується секретний ключ та здійснюється криптографічне перетворення повідомлення. На другому етапі зашифрований блок інтегрується у вибраний графічний контейнер методом модифікованої LSB-заміни або за допомогою стеганографічних алгоритмів, оптимізованих для мінімізації візуальних та статистичних спотворень. На етапі отримання стегоконтейнера виконується зворотна процедура: спочатку виділення прихованих даних, а потім їхнє криптографічне розшифрування.

Побудова комбінованого захисту дозволяє суттєво підсилити стійкість системи. Навіть у разі виявлення стеганографічного контейнера зловмисник не має змоги прочитати інформацію без відповідного ключа. Використання подвійного захисту забезпечує ефективну протидію як статистичному аналізу зображень, так і криптоаналітичним атакам.

Запропонована модель також демонструє кращі результати за критеріями непомітності, стійкості та складності виявлення прихованого каналу. Це робить її перспективною для застосування в умовах обмежених каналів зв'язку, конфіденційного документообігу, телеметрії, а також у військових і спеціальних комунікаційних системах. Подальші дослідження можуть включати вдосконалення механізмів приховування за допомогою глибинних нейронних мереж, застосування трансформерних моделей для адаптивного стегоаналізу та інкорпорацію постквантових протоколів для підвищення криптографічної стійкості.

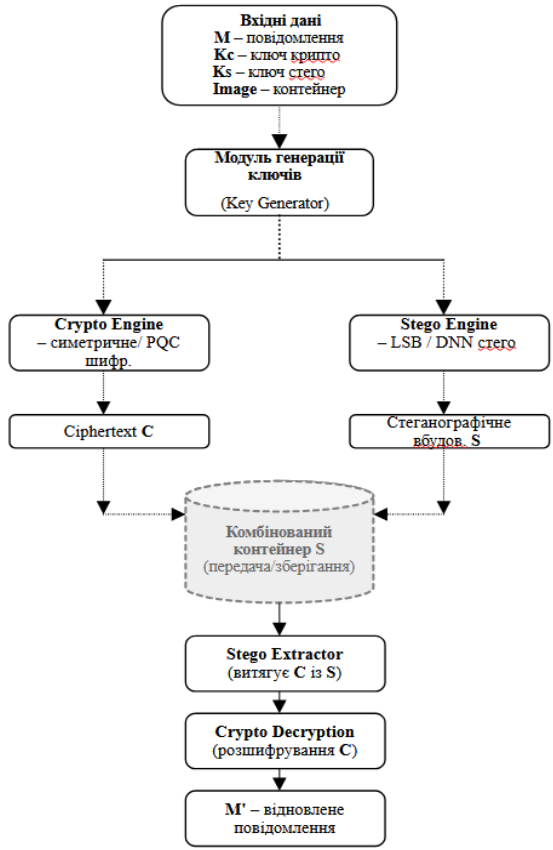

Рисунок 1 – Архітектура комбінованої системи Crypto+Stego

Висновки. Розроблена комбінована система забезпечує багаторівневий захист даних шляхом поєднання криптографічного шифрування та стеганографічного приховування. Запропонована архітектура підвищує конфіденційність, прихованість та стійкість інформаційного обміну. Отримані результати підтверджують ефективність моделі та визначають перспективи її подальшого розвитку в напрямі постквантових та нейромережевих технологій.

Література

1. Кауфман Ч., Перлман Р. Специфікація безпечних систем. – Нью-Йорк: Wiley, 2021.

2. Al-Mhiqani, M., et al. (2022). Deep learning approaches for network intrusion detection: A review. Computers & Security, 114, 102594. Johnson N. F., Jajodia S. Exploring Steganography: Seeing the Unseen. – IEEE Computer, 1998.

3. Katz J., Lindell Y. Introduction to Modern Cryptography. – CRC Press, 2020

УДК 621.3

АНАЛІЗ СТАНУ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ОБ'ЄКТІВ ЗБЕРЕЖЕННЯ ЦИФРОВОЇ ІНФОРМАЦІЇ В УМОВАХ ВОЄННОГО СТАНУ

Роман ШЕВЧЕНКО, Юлія ПОГРІБНА
Національний університет цивільного захисту України, м. Черкаси

Анотація. *Активна цифровізація та інформатизація суспільства, розширення сфер застосування електронних технологій зумовили необхідність трансформації традиційних підходів до створення, обігу, зберігання інформації та посилення вимог до безпеки електронних документів. У воєнних умовах цифрові архіви й інфраструктура стають вразливими до кібератак, фізичних руйнувань, пожежних та техногенних ризиків, що потребує комплексної стратегії їх захисту та стійкості.*

Ключові слова: *воєнний стан, нормативно-правове регулювання, інформаційна безпека, електронний документ, збереження інформації, пожежна безпека, martial law, regulatory and legal regulation, information security, electronic document, information retention, fire safety.*

Суб'єкти електронного документообігу зобов'язані зберігати електронні документи на електронних носіях інформації у такій формі, що забезпечує можливість перевірки їхньої цілісності, а також дотримуватися строків зберігання не менших, ніж передбачено законодавством для паперових аналогів [1]. Зазначені вимоги спрямовані на гарантування юридичної чинності, достовірності та стабільності електронних документів протягом усього періоду їх використання.

Запровадження електронного документообігу має наслідком необхідність зміни підходів до архівної діяльності, враховуючи, що в майбутньому переважатиме документ у форматі електронних даних та існуватиме безмежжя програм із керування документаційними процесами. Також функціонування електронного документа, електронного архіву вимагає відповідної технічної інфраструктури [2].

Дослідження вказують, що в умовах військових конфліктів, надзвичайних ситуацій природного та техногенного характеру цифровий простір стає не менш уразливим, ніж фізична інфраструктура, а отже потребує переосмислення підходів до його захисту та стійкості.

Питання інформаційної безпеки та культури в умовах війни є питанням виживання людини, суспільства та держави. Адже забезпечення інформаційної безпеки визначається не тільки інтересами держави, а й інтересами особи в контексті забезпечення її прав і свобод. Основою сучасної інформаційної безпеки є цілісність даних, доступність інформації,

конфіденційність і надійність її збереження. Інформаційна безпека включає не лише нормативно-політичну складову, а й інституційну сферу, яка передбачає діяльність органів, що її забезпечують, а також використання програмно-технічних засобів [3].

В дослідженні CD Nguyen розвінчується ілюзія невразливості цифрових репозиторіїв та цифрових архівів шляхом розкриття їхньої вразливості до військових дій на основі історичних прикладів та сучасних викликів, де зазначається, що ілюзія виникає через неврахування складної природи конфліктів, де як фізичний, так і цифровий простори стають полями битви. Тому збалансований підхід передбачає визнання обмежень заходів безпеки та включення стійкості в саму основу стратегій цифрового збереження. Ця стійкість охоплює не лише технологічні запобіжні заходи, але й заходи щодо пом'якшення впливу конфліктів у громадах, яким служать ці сховища та архіви [4].

В епоху швидкого розвитку інформаційних технологій центри обробки даних мають вирішальне значення для функціонування сучасного суспільства, оскільки в них зберігається цінне обладнання та величезні обсяги даних. Пожежа в центрах обробки даних призведе до незмірних втрат, що робить системи активного пожежогасіння необхідними [5].

З метою підвищення інформаційної стійкості держави в умовах воєнного стану, захисту державних даних від кібератак, фізичного знищення або втрати, та забезпечення їх відновлюваності розпорядники систем, об’єктів критичної інформаційної інфраструктури для забезпечення їх належного функціонування та захисту інформації, що обробляється в них забезпечують створення резервних копій державних інформаційних ресурсів, систем, об’єктів критичної інформаційної інфраструктури на окремих фізичних носіях у зашифрованому вигляді та їх подальшу передачу (переміщення) для зберігання в установленому законодавством порядку, у тому числі за межами України (зокрема в закордонних дипломатичних установах України), під час дії воєнного стану в Україні та протягом шести місяців з дня його припинення чи скасування [6].

Зберігання резервних копій інформації на фізичних носіях, потребує забезпечення виконання протипожежних та техногенних заходів в місцях їх зберігання.

В дослідженні Min Li зазначено, що об'єкти Всесвітньої спадщини можуть опинитися під загрозою пошкодження зокрема від пожеж (68,8%). Інші антропогенні небезпеки включають зокрема тероризм (16,7%) та збройні конфлікти (10,4%) [7].

Отже спектр загроз, характерний для фізичних об’єктів, має прямі аналогії у сфері збереження цифрової інформації. Так само як природні небезпеки чи техногенні аварії можуть руйнувати матеріальні структури, цифрові сховища вразливі до пожеж, відмов обладнання, стихійних ката-

строф та наслідків кліматичних явищ, які впливають на інфраструктуру дата-центрів. Крім того, цифрові ресурси піддаються антропогенним ризикам від кібератак і несанкціонованого доступу до зумисного знищення даних унаслідок терористичних дій чи збройних конфліктів.

У цих умовах забезпечення надійності цифрових систем вимагає комплексного, багаторівневого підходу, що охоплює заходи пожежної та техногенної безпеки, як об'єктів зі збереження цифрової інформації так і приміщень збереження фізичних носіїв інформації, стійкість до зовнішніх впливів, а також кіберзахист і плани безперервності діяльності. Ефективне збереження цифрової інформації ґрунтується на усвідомленні того, що жодна система не є повністю захищеною від загроз, а отже, ключовим завданням є не лише попередження інцидентів, а й створення механізмів, здатних мінімізувати їхні наслідки та забезпечити відновлення даних у будь-яких кризових сценаріях.

Аналізом нормативно-правових актів які регулюють дотримання норм протипожежної та техногенної безпеки встановлено, що більшість нормативно-правових актів та заходів щодо забезпечення пожежної та техногенної безпеки були розраховані на мирний час і потребують адаптації до умов воєнного стану (особливого періоду) та функціонування в кризових умовах.

Література

1. Закон України «Про електронні документи та електронний документообіг» від 22 трав. 2003 р. № 851-IV.

2. Бездрабко В. Архів, архівіст, архівна культура: ідея, метафора, постання майбутнього образу. Архіви України. 2019. Вип. 2 (319). Квітень–червень.

3. Смотрич Д. В., Браілко Л. Інформаційна безпека в умовах воєнного стану. Науковий вісник Ужгородського національного університету. 2023. Вип. 77, ч. 2.

4. Nguyen C.D. Digital cultural heritage in the crossfire of conflict: cyber threats and cybersecurity perspectives. Insights: The UKSG Journal, 2024.

5. Wei Jin, Zhuopin Yuan, Huang Tang, Yu Fang, Song Li. Discussion on active fire protection systems for data center. In: Proceedings of the 2025 8th International Conference on Traffic Transportation and Civil Architecture (ICTTCA 2025). Atlantis Highlights in Engineering. 2025. P. 638–643. doi: 10.2991/978-94-6463-793-9_54.

6. Закон України «Про захист інформації в інформаційно-комунікаційних системах» від 05 лип. 1994 р. № 80/94-ВР.

7. Min Li. Disaster Risk Management of Cultural Heritage: A Global Scale Analysis of Characteristics, Multiple Hazards, and Issues Based on Historical Disasters and Current DRR Measures in World Heritage Sites. International Journal of Disaster Risk Reduction, 2024.

УДК 004.056.53

ЗАХИСТ ВІД MITM АТАК У ПРОТОКОЛАХ АВТОРИЗАЦІЇ БАНКІВСЬКИХ ТРАНЗАКЦІЙ НА ОСНОВІ СХЕМИ ШНОРА

Вікторія ШЛАПАК, Сергій СЕМЕНЮК
Національний університет "Львівська політехніка"

Анотація *У роботі проаналізовано захист банківських транзакцій на базі протоколу Шнора від атак типу «людина посередині» (MITM). Показано, що спроби підміни параметрів доказу є неефективними за умови захищеного обміну публічними ключами. Це гарантує безпеку автентифікацію транзакцій без розкриття секретних даних клієнта.*

Ключові слова: *криптографічний протокол, доказ з нульовим розголошенням, схема Шнора, MITM атака.*

Зростання обсягів цифрових банківських операцій вимагає впровадження надійних методів автентифікації, які гарантують конфіденційність, цілісність та автентичність даних. При цьому традиційні методи часто стають вразливими до перехоплення, тому актуальним є використання доказів з нульовим розголошенням. Однією з таких є схема Шнора [1], яка базується на складності задачі дискретного логарифмування. Дана робота розглядає модель загрози "Людина посередині" (MITM) [2] для цієї схеми та методи протидії їй.

Процес авторизації за схемою Шнора передбачає взаємодію між клієнтом (Prover) та банком (Verifier). На етапі підготовки обираються публічні параметри: просте число p та генератор g. Клієнт володіє секретним ключем x та публічним ключем $y = g^x \bmod p$, значення якого відоме банку.

Протокол складається з трьох етапів:

1. Формування доказу: Клієнт генерує число *r*, пов'язане з транзакцією та передає банку значення $t = g^r \bmod p$.
2. Виклик (Challenge): Банк надсилає унікальне випадкове число *e*.
3. Відповідь (Response): Клієнт обчислює $s = r + e \cdot x \bmod p - 1$.

Авторизація вважається успішною, якщо виконується рівність $g^s \equiv t \cdot y^e \bmod p$

Найбільш критичним вразливим місцем є середовище передачі даних, де зловмисник може спробувати реалізувати атаку MITM, перехопивши або модифікувавши параметри транзакції. У змодельованому сценарії атаки зловмисник перехоплює значення t замінюючи його на t'.

Однак, стійкість запропонованої моделі забезпечується тим, що значення публічного ключа y передається через захищений канал зв'язку (наприклад, під час первинної реєстрації) і не може бути підмінене зловмис-

ником у рамках поточної сесії. Оскільки зловмисник не володіє секретним ключем x, він не може обчислити валідне значення s', яке б задовольнило перевірочне співвідношення для модифікованого t' та оригінального y. В результаті, банк при перевірці виявить невідповідність і транзакція буде відхилена. Для додаткового захисту від атак повторного відтворення (Replay Attack) до протоколу включаються часові мітки або унікальні ідентифікатори сесії.

Література

1. RFC 8235. Schnorr Non-interactive Zero-Knowledge Proof. IETF Standards Track, 2017, https://datatracker.ietf.org/doc/html/rfc8235.

2. Bellare M., Palacio A. GQ and Schnorr Identification Schemes: Proofs of Security against Impersonation under Active and Concurrent Attacks. Advances in Cryptology — CRYPTO 2002. Lecture Notes in Computer Science, vol 2442. Springer, 2002. P. 162–177.

ПРОЕКТУВАННЯ РОЗПОДІЛЕНИХ ПРОГРАМНИХ СЕРВІСІВ

Іван РОВЕЦЬКИЙ
Львівський державний університет безпеки життєдіяльності

На даний час актуальною проблемою під час проектування розподілених програмних систем є те, що вони мають стабільно працювати в умовах високого навантаження, коли десятки і сотні тисяч користувачів хочуть отримати певні ресурси, які надаються сервісами системи. Для того, щоб забезпечити високу доступність та стійкість високонавантажених програмних сервісів, їх розгортають у керованих мультипроцесорних розподілених системах (кластерах). Такого роду ресурси є високо вартісними, тому на практиці, найчастіше, використовують різноманітні хмарні платформи (Google Cloud, Amazon, Azure та ін.). Кластерні системи надають паралельні апаратні ресурси, однак для того, щоб сервіси використовували надані ресурси у повному обсязі, їх необхідно проектувати, використовуючи спеціальні архітектурні рішення. Тому мета даного дослідження полягає у аналізі архітектурних рішень та особливостей їхнього використання під час проектування програмних сервісів розподілених систем.

Ключові слова: розподілені системи, кластери, хмарні платформи, мікросервіси, мікросервісна архітектура, багатопоточність.

Currently, a pressing problem in the design of distributed software systems is that they must operate stably under high load conditions, when tens and hundreds of thousands of users want to receive certain resources provided by system services. In order to ensure high availability and stability of highly loaded software services, they are deployed in managed multiprocessor distributed systems (clusters). Such resources are of high value, therefore, in practice, most often, various cloud platforms (Google Cloud, Amazon, Azure, etc.). Cluster systems provide parallel hardware resources, however, in order for services to be able to use the provided resources in full during their work, they must be designed using special architectural solutions. Therefore, the purpose of this study is analyzing architectural solutions and the features of their use when designing software services of distributed systems

Key words: distributed systems, clusters, cloud platforms, microservices, microservice architecture, multithreading

На даний час актуальною проблемою є забезпечення високої доступності та стабільності роботи розподілених програмних систем в умовах високого навантаження [1, 2]. Цю проблему потрібно вирішувати певними архітектурними рішеннями вже на стадії проектування архітектури системи. Необхідною умовою стабільної роботи програмної системи в умовах високого навантаження є її розгортання в деякій програмно керованій паралельній розподіленій системі – кластері.

Для забезпечення автоматизації розгортання, масштабування та управління програмними додатками у фізичному чи віртуальному кластері, на даний час основним інструментом є програмна платформа з відкритим

вихідним кодом Kubernetes [3], розроблена компанією Google. Найважливішою особливістю системи Kubernetes є те, що вона може керувати тільки контейнерними програмними додатками, коли додаток і все, що необхідне для його роботи (код, бібліотеки, файли конфігурації і навіть операційна система) упаковані в контейнері. На даний час, на практиці найбільшого поширення мають контейнери, побудовані на платформі Docker.

Отже, для того, щоб мати можливість ефективно масштабувати програмний додаток в кластері під керуванням Kubernetes, він має бути спроектований у вигляді окремих слабозв'язаних програмних компонент, які можна легко розгорнути в контейнерах. Така архітектура називається мікросервісною архітектурою [4], а її компоненти – мікросервісами.

Кожний мікросервіс має керувати доступом тільки до даних, за які він відповідає. Жодні інші мікросервіси не повинні мати можливості безпосереднього доступу до баз даних, за які вони не відповідають, такі дані мають бути доступні тільки через API відповідного сервісу. Це дає можливість кожному мікросервісу керувати консистентністю та структурою бази даних, за яку він відповідає, а також використовувати найбільш відповідну СУБД для конкретних цілей без будь-якої залежності від вимог системи в цілому. Наприклад, один сервіс може використовувати нормалізовану SQL-базу даних, тоді як інший може отримати переваги з NoSQL-бази даних.

На практиці, коли мова йде про мікросервісну архітектуру, зрозуміло, що необхідно продумати механізм взаємодії мікросервісів. Найбільш загальний і простий спосіб комунікації мікросервісів – це комунікація на основі обміну повідомленнями за певним протоколом, яку ще називають Message Driven Architec-ture (MDA). У цьому випадку один мікросервіс надсилає повідомлення (request), а інший – опрацьовує його та надсилає інше повідомлення у відповідь (response). У цьому контексті сервіс, який виконує запит називається клієнтом, а інший – сервером.

Набір правил, які описують процес обміну повідомленнями в моделі "клієнт-сервер" називаються REST API (Representational State Transfer). На даний час, на практиці, REST API дуже часто будується на синхронній моделі комунікації, де клієнт відправляє запит і отримує відповідь у межах одного з'єднання. При цьому клієнт очікує, доки не повернеться результат. Синхронна архітектура є класичним підходом, коли для опрацювання кожного клієнтського запиту виділяється окремий потік. Так працюють класичні веб-сервери. Ця архітектура працює доволі добре і дає можливість масштабувати сервіс в залежності від навантаження, збільшуючи або зменшуючи кількість потоків у сервісі.

Існує інший спосіб комунікації мікросервісів, який базується на архітектурному паттерні Publisher-Subscription-Subscriber [5], коли взаємодія мікросервісів реалізовується з використання розподілених черг даних (Kafka, RabbitMQ, JMS, Google Pub/Sub). У цьому випадку, система буду-

ється так, що зміна стану одного мікросервіса, ініційована до прикладу певним клієнтським запитом, активує зміну стану інших мікросервісів. При цьому мікросервіс, у якого змінився стан, створює подію (Event) і надсилає в розподілену чергу в наперед визначену тему (topic). Інші мікросервіси, які підписані на цю тему, зчитують та опрацьовують цю подію, і відповідно змінюють свій стан. Така архітектура взаємодії мікросервісів є повністю асинхронною і називається подійно-орієнтованою Event Driven Architecture(EDA). Мікросервісна архітектура, побудована на асинхронній комунікації даного типу, дає можливість прийняти та опрацювати більшу кількість запитів, і використовується у більш високонавантажених системах.

У результаті проведеного дослідження встановлено, що особливістю проектування програмного забезпечення розподілених систем є використання мікросервісної архітектури та мікросервісів, які розгортаються у контейнерних середовищах. Мікросервісну архітектуру, в залежності від класу задач, можна побудувати за принципом обміну повідомленнями (REST API), або за принципом, орієнтованим на опрацювання подій, які генеруються у системі після отримання клієнтського запиту. REST API є синхронним за своєю природою, в той час як подійно-орієнтована архітектура (EDA) є асинхронною і підходить для дуже високонавантажених слабозв'язаних сервісів. Синхронна модель показує хорошу продуктивність, однак має обмеження, пов'язані з блокуванням потоків, доки не буде отримано результати клієнтських запитів. Асинхронна модель дає можливість прийняти більшу кількість запитів, на відміну від синхронної, однак вимагає повністю асинхронного API під час роботи із зовнішніми сервісами, а також є складнішою під час відлагодження сервісів та виправлення помилок.

Література

1. Burns, B. (2025). Designing Distributed Systems: Patterns and Paradigms for Scalable, Reliable Systems Using Kubernetes: O'Reilly.
2. Tanenbaum, A. S., Steen, M. (2006). Distributed Systems: Principles and Paradigms: Pearson.
3. Luksa, M. (2023). Kubernetes in Action: Manning.
4. Newman, S. (2015). Building Microservices: Designing Fine-Grained Systems: O'Reilly
5. Joshi, U. (2023). Patterns of Distributed Systems: Addison-Wesley Professional

УДК 004.41:005.8:005.32

КОМАНДНА РОЗРОБКА ІТ-ПРОЕКТІВ НА ОСНОВІ AGILE-МЕТОДОЛОГІЇ

**Василь СМУТОК, Віктор РОГІНСЬКИЙ,
Роман ОЛІЙНИК, Павло ЛУБ**
*Львівський національний університет ветеринарної медицини
та біотехнологій імені С.З. Гжицького, м. Львів, Україна*

Анотація. *Наведено гнучкі методології розробки програмного забезпечення, що ґрунтуються на принципах Agile та орієнтовані на ітеративність, адаптивність і взаємодію між розробниками й замовником. Означено властивості Agile-підходів, а також зазначено найпоширеніші методи, зокрема Scrum, XP і Kanban. Підкреслено унікальність запропонованої системи командної розробки, реалізованої у вигляді окремого API, що забезпечує високу гнучкість, швидку інтеграцію та оптимізацію роботи з проектними даними. Наведено переваги – прискоренні розробки, розширюваності та підтримці сучасних інструментів, таких як Spring Security, системи звітності, зв'язування тікетів та гнучкі механізми комунікації й фільтрації інформації.*

Ключові слова: *Agile-методологія, програмне забезпечення, управління проєктами, інтеграція API, командна взаємодія, Scrum.*

Abstract. *The text presents flexible software development methodologies based on Agile principles, focusing on iterative processes, adaptability, and collaboration between developers and clients. The characteristics of Agile approaches are outlined, and the most widely used methods, including Scrum, XP, and Kanban, are highlighted. The uniqueness of the proposed team-based development system, implemented as a standalone API, is emphasized, providing high flexibility, rapid integration, and optimized handling of project data. The advantages of the system include accelerated development, extensibility, and support for modern tools such as Spring Security, reporting systems, ticket linking, and flexible communication and filtering mechanisms.*

Keywords: *Agile methodology, software development, project management, API integration, team collaboration, Scrum.*

Гнучкі технології розробки програмного забезпечення (ПЗ) скеровані на безперервний зворотній зв'язок і врахування зміни у вимогах протягом життєвого циклу ПЗ, підтримувати тісну співпрацю між клієнтами і розробниками, а також забезпечувати перспективні програмні функції (рис.).

Маніфест *Agile* – база, на якій побудовані методи гнучких технологій розробки ПЗ. Він опублікований групою розробників ПЗ та консультантів: "*….ми постійно відкриваємо для себе більш досконалі методи розробки ПЗ, займаючись розробкою безпосередньо і допомагаючи в цьому іншим. Завдяки виконаній роботі ми змогли усвідомити, що*: 1) *люди і взаємодія важливіше процесів та інструментів;2) працюючий продукт важливіше вичерпної документації; 3) співпраця з замовником важливіше узгодження умов контракту; 4) готовність до змін важливіше проходження попереднім планом".*

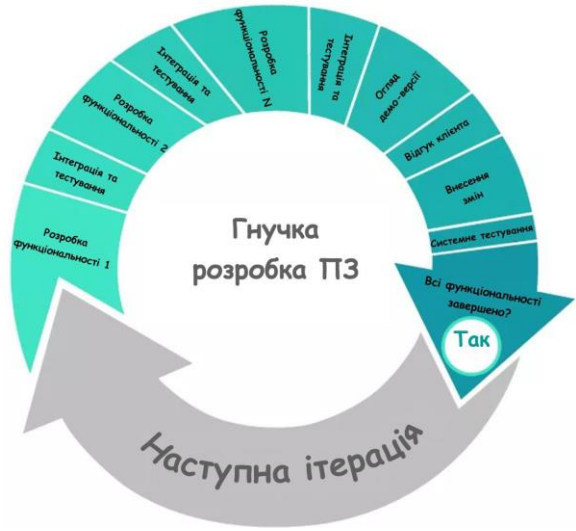

Рис. – Життєвий цикл гнучкої розробки ПЗ

Гнучкі методології можна визначити як групу процесів розробки ПЗ, які є:

– *ітераційними* як спроба вирішення проблем шляхом пошуку послідовних наближень до рішення (наприклад, розроблена повна система змінює функціональність підсистем з кожним випуском внаслідок оновлення вимог);

– *поступовими* як підхід, який передбачає розподіл системи на функціональні підсистеми та додавання нової функціональності до загальної системи з кожним випуском;

– *самоорганізуючими* як концепція, що дає команді можливість організовувати самостійно процес для найкращого результату завдання (наприклад, взаємодія в команді, динаміка роботи, робочий час команда самостійно розподіляє для найліпшого вирішення);

– *виникаючими* як досвід навчання з кожного проекту, внаслідок того, що кожен проект організовується по-різному, застосовуючи ітеративні, поступові, самоорганізуючі та новітні методи.

Деякі з відомих методів гнучких технологій розробки ПЗ – це екстремальне програмування (XP), Scrum, кристальні методології Crystal Clear, Kanban, розробка керована функціями, динамічний метод розробки. Зокрема, найпоширенішими є такі три методи – Scrum, XP, Kanban.

Унікальність запропонованої нами системи командної розробки та управління проектами полягає в тому, що вона реалізована як окремий

API. Це дасть користувачам-розробникам зручний спосіб використання всіх функціональних можливостей системи без необхідності працювати з складним користувацьким інтерфейсом. Це дозволяє їм інтегрувати систему управління проектами у свої проекти швидко та ефективно. Тоді, розробники отримають гнучкість у виборі того, які функції вони хочуть використовувати. Вони можуть вибрати лише ті API-методи, які їм потрібні для їх конкретних потреб та ігнорувати інші. Це дозволяє оптимізувати використання ресурсів і забезпечити ефективну роботу із системою командного управління IT-проектами.

Окремий API для системи управління проектами також прискорює процес розробки. Розробники можуть скористатися готовими функціями та модулями системи управління проектами, що дозволяє їм уникнути повторної розробки та зосередитися на вирішенні специфічних завдань своїх проектів. Це збільшує швидкість розробки та скорочує час досягнення мети. В запропонованій системі управління передбачаються такі розширення функціональності, що в майбутньому зможуть надати більше можливостей якісно керувати проектом:

Spring Security. Структура, надана Spring, яка допомагає налаштувати доступ і процес автентифікації – відіграє дуже важливу роль у забезпеченні безпеки програм.

Звітність. В системах управління проектами звітність відіграє важливу роль у процесі контролю та оцінки прогресу проектів. Це процес збору, аналізу та представлення інформації про ключові аспекти проекту, що дозволить керівникам та зацікавленим сторонам отримувати необхідні дані для прийняття рішень та встановлення планів дій.

Ticket linking (Зв’язок між тікетами). В системі управління проектами та використовується поняття "зв'язок між тікетами" для встановлення зв'язку між основним тікетом та підтікетом (sub ticket). Основний тікет може бути, наприклад, головним запитом чи задачею, яку треба вирішити. Підтікет є додатковою задачею, яка пов'язана з основним квитком і потребує окремого виконання.

Коментарі усюди. Коментарі можуть бути додані до різних об'єктів у системі управління проектами, таких як задачі, спринти, проектні документи, зміни, помилки тощо. Це дозволить створювати контекстні обговорення та забезпечить збереження комунікації відносно конкретного елемента проекту.

Можливість відмічати користувачів в коментарях. Це дозволить полегшити комунікацію та спілкування між учасниками проекту, особливо у випадах, коли коментарі можуть містити багато інформації або стосуються конкретних питань, які потребують уваги конкретних користувачів.

Фільтрація за періодом. Можливість фільтрувати спринти, епіки та тікети за періодом дозволить користувачам швидко знаходити та переглядати проекти, завдання або інші елементи, які були створені, змінені або закриті протягом певного періоду часу.

УДК 004.021:004.94

ПРОЦЕСИ МОДЕЛЮВАННЯ ДАНИХ ТА ЇХ ПРИКЛАДНЕ ЗНАЧЕННЯ

Віктор ЯНЕНКО, Юрій ЛЕЩИШИН, Павло ЛУБ
Львівський національний університет ветеринарної медицини та біотехнологій імені С.З. Гжицького, м. Львів, Україна

Анотація. *Розкрито поняття моделювання даних як процесу створення структурованого набору даних для прийняття рішень в управління виробничими процесами. Наведено основні етапи моделювання – концептуальне, логічне та фізичне. Підкреслено роль сучасних нотацій і програмних засобів, що забезпечують узгодженість моделей та спрощують їх впровадження. Акцентовано на практичному значенні процесів моделювання даних для структуризації інформації, підтримки управлінських рішень, аналізу ризиків і підвищення ефективності виробничих процесів.*

Ключові слова: *моделювання даних; інформаційні системи; концептуальна модель; логічна модель; управлінські рішення.*

Abstract. *The concept of data modeling is presented as a process of creating a structured set of data to support decision-making in the management of production processes. The main stages of modeling – conceptual, logical, and physical – are outlined. The role of modern notations and software tools that ensure model consistency and simplify their implementation is emphasized. The practical significance of data modeling processes is highlighted in terms of information structuring, supporting managerial decisions, risk analysis, and improving the efficiency of production processes.*

Keywords: *data modeling; information systems; conceptual model; logical model; managerial decisions.*

Моделювання даних – це процес створення узагальненого опису (моделі) структури даних, їхніх властивостей та взаємозв'язків між ними з метою ефективного зберігання, обробки й використання інформації. Він дозволяє у зрозумілій формі відобразити, як організовані дані у певній системі чи предметній області, щоб забезпечити їх логічність, цілісність і доступність. Загалом моделювання даних застосовується для планування інформаційних систем, управління процесами, аналітики або наукових досліджень. Результатом є модель – концептуальна, логічна чи фізична – яка показує, як дані взаємодіють між собою та як вони можуть бути реалізовані у базах даних або інформаційних середовищах.

Процес моделювання даних охоплює кілька послідовних етапів. Спочатку здійснюється аналіз предметної області з метою визначення сутностей і зв'язків між ними. Далі формується концептуальна модель, що описує інформаційні об'єкти без технічних деталей. Наступним кроком є створення логічної моделі, де уточнюються атрибути, типи зв'язків, обме-

ження цілісності та правила взаємодії. Завершальним етапом виступає побудова фізичної моделі, яка визначає способи реалізації даних у конкретній системі керування базами даних, враховуючи аспекти продуктивності, індексування, безпеки та оптимізації запитів.

У практичній діяльності застосовуються різні методи та нотації для побудови моделей, зокрема ERD (Entity–Relationship Diagram), UML (Unified Modeling Language) або IDEF1X. Для їх реалізації використовуються програмні засоби, такі як *ERwin Data Modeler, PowerDesigner, Visual Paradigm, Lucidchart* чи *Microsoft Visio*. Використання таких інструментів дає змогу автоматизувати процес створення моделей, перевіряти їх на узгодженість і спрощувати подальше впровадження у бази даних.

Головні завдання моделювання даних:

1) *структуризація інформації* – упорядкування даних про ресурси, персонал, обладнання, терміни та фінанси;

2) *аналіз ризиків* – виявлення потенційних відхилень від плану, оцінка їхнього впливу на строки та собівартість;

3) *планування і прогнозування* – створення моделей сценаріїв розвитку проекту для вибору оптимальної стратегії;

4) *підтримка управлінських рішень* – забезпечення доступу до актуальної та аналітично обробленої інформації;

5) *оптимізація ресурсів* – виявлення надлишкових або недостатніх витрат ресурсів і пропозиція шляхів їх перерозподілу.

Таким чином, моделювання даних у сфері управління виробничими проектами – це процес створення логічної та структурної моделі інформації, яка відображає взаємозв'язки між ресурсами, процесами, ризиками, витратами та результатами виробництва. Така модель дозволяє системно аналізувати потоки даних, прогнозувати наслідки управлінських рішень і підвищувати ефективність планування виробничих процесів. Головні завдання моделювання даних полягають у структуризації інформації, аналізі ризиків, плануванні й прогнозуванні, підтримці управлінських рішень і оптимізації використання ресурсів.

Сучасні тенденції моделювання даних орієнтовані на інтеграцію з технологіями великих даних (Big Data), використання семантичних моделей, графових баз даних та побудову цифрових двійників підприємств (Digital Twins). Це дозволяє перейти від статичного відображення структури інформації до динамічного моделювання поведінки системи в реальному часі, що значно розширює можливості для аналітики, прогнозування та стратегічного управління.

Існують три різних типи моделей даних, що виробляються протягом переходу від вимог до дійсної бази даних для використання в інформаційній системі. У процесі переходу від етапу формування вимог до створення реальної бази даних, яка функціонуватиме в інформаційній системі, розро-

бляють три основні типи моделей даних. Спочатку вимоги до інформації формалізуються у вигляді концептуальної моделі даних, що є набором описів сутностей і зв'язків без урахування технічних аспектів. Вона слугує основою для узгодження бачення структури даних між аналітиками та представниками бізнесу.

Далі концептуальна модель трансформується у логічну модель даних, у якій деталізується структура інформації, визначаються атрибути, зв'язки та обмеження, що можуть бути реалізовані у базі даних. У деяких випадках для однієї концептуальної моделі може бути створено кілька логічних моделей, залежно від вимог до різних підсистем або типів сховищ даних.

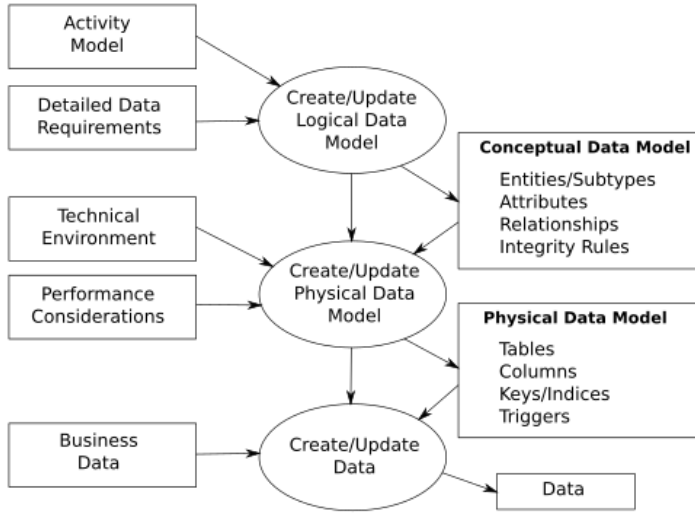

Рисунок – Процес моделювання даних

Отже, завершальним етапом процесу моделювання даних є побудова фізичної моделі, яка ґрунтується на логічній та відображає фактичну реалізацію структури бази даних. На цьому етапі інформація організовується у таблиці, визначаються механізми доступу, оптимізації продуктивності та особливості зберігання даних. Моделювання даних охоплює не лише визначення окремих елементів інформації, а й описує їхню внутрішню структуру, логічні взаємозв'язки та способи взаємодії в межах інформаційної системи.

З М І С Т

Секція 1

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Секція 2

КІБЕРБЕЗПЕКА

Наукове видання

ІНФОРМАЦІЙНА БЕЗПЕКА ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Збірник тез доповідей
VII Всеукраїнської науково-практичної конференції

Відповідальні за випуск **Назарій БУРАК**
Олександр ХЛЕВНОЙ

Оригінал-макет **Юлія НАЗАР, Ольга СМОТР, Роман ГОЛОВАТИЙ, Діана РАЙТА, Віра ДОВБНЯК, Іван РОВЕЦЬКИЙ, Наталія ЖЕЗЛО-ХЛЕВНА**

Підписано до друку 12.11.2025 р.
Формат 60×84/16. Гарнітура Times New Roman.
Друк на різографі. Папір офсетний.
Ум. друк. арк. 30.

Друк ЛДУ БЖД
79007, Україна, м. Львів, вул. Клепарівська, 35
тел./факс: (032) 233-32-40, 233-24-79.