МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ

VI НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ «ПРОБЛЕМИ КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ»

3 грудня 2025 року

Збірник тез

м.Київ

VI науково-практична конференція «Проблеми комп’ютерної інженерії». Збірник тез. – К.: ДУІКТ, 2025.

Збірник містить тези доповідей учасників конференції, представлених на VI науково-практичній конференції «Проблеми комп’ютерної інженерії», яка проводилась 5 грудня 2025 р. на кафедрі Комп’ютерної інженерії Навчально-наукового інституту інформаційних технологій Державного університету інформаційно-комунікаційних технологій, м.Київ.

Робочі мови – українська та англійська.

На конференції проведено апробацію результатів наукових досліджень, обговорено перспективи та різноманітні підходи до вирішення сучасних проблем комп’ютерної інженерії.

Технічний секретар конференції:
Коротков Сергій Станіславович– доцент каф. КІ,
Державний університет інформаційно-комунікаційних технологій
e-mail: pki.conf@gmail.com

НАПРЯМ 1. КОМП'ЮТЕРНІ МЕРЕЖІ, КІБЕРБЕЗПЕКА ТА ІНЖЕНЕРІЯ ДАНИХ

Філик Павло Васильович
студент 6 курсу, групи КСДМ-61
Державного університету
інформаційно-комунікаційних технологій
м. Київ
pavelfilyk28@gmail.com
Слєпчук Ростислав Віталійович
студент 6 курсу, групи КСДМ-61
Державного університету
інформаційно-комунікаційних технологій
м. Київ
fewrules10@gmail.com

ОГЛЯД АРХІТЕКТУРИ БЕЗШОВНОЇ WI-FI МЕРЕЖІ

Постановка задачі. Сучасні корпоративні мережі стикаються з проблемою зростання кількості мобільних пристроїв та обсягів мультимедійного трафіку, що робить традиційні підходи до побудови WLAN на базі розрізнених точок доступу неефективними. Застарілі офісні мережі характеризуються наявністю «мертвих зон», високим рівнем інтерференції та відсутністю механізмів безшовного переміщення користувачів (роумінгу), що призводить до зниження продуктивності праці. Виникає нагальна потреба у проектуванні архітектури мереж корпоративного класу на базі сучасних стандартів IEEE 802.11ax та технологій централізованого управління радіоресурсами.

Мета дослідження. Метою роботи є розробка та обґрунтування архітектури відмовостійкої безшовної Wi-Fi мережі підприємства для забезпечення надійного доступу до інформаційних ресурсів та підтримки мобільності користувачів.

Результати дослідження. У ході дослідження проведено аудит існуючої інфраструктури, який виявив критичні недоліки «клаптикової» топології на базі SOHO-маршрутизаторів.[1] На основі розрахунку ємності мережі та радіопланування обґрунтовано необхідність встановлення 4-х точок доступу для забезпечення перекриття сигналів на рівні 15–20%, що є необхідною умовою для коректної роботи роумінгу. Запропоновано використання точок доступу Cisco Catalyst 9105AX з підтримкою стандарту Wi-Fi 6 та технології MU-MIMO[2]. Ключовим архітектурним рішенням стало використання технології Cisco Embedded Wireless Controller, що дозволило реалізувати функціонал

централізованого контролера безпосередньо на точці доступу, оптимізувавши капітальні витрати. Розроблено логічну топологію з використанням VLAN для сегментації трафіку на службовий, корпоративний та гостьовий, що підвищує рівень інформаційної безпеки.

Висновки та перспективи. Запропонована архітектура забезпечує суцільне радіопокриття офісного приміщення та вирішує проблему «липких клієнтів» завдяки підтримці протоколів швидкого роумінгу. Використання діапазону 5 ГГц та стандарту 802.11ax дозволяє підвищити пропускну здатність каналів та мінімізувати вплив інтерференції. Перспективи подальшого розвитку системи полягають у масштабуванні мережі за допомогою підключення нових точок доступу до віртуального контролера EWC та впровадженні політик QoS для пріоритизації мультимедійного трафіку.

Список використаних джерел:

1. IEEE Standard for Information technology—Telecommunications and information exchange between systems Local and metropolitan area networks—Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, IEEE Std 802.11-2020.

2. Cisco Embedded Wireless Controller on Catalyst Access Points Configuration Guide. Cisco Systems, Inc., 2021.

Ільїн С. А.,
аспірант, Інститут програмних систем
Національної академії наук України

ОПТИМІЗАЦІЯ МАРШРУТИЗАЦІЇ ТА РОЗПОДІЛУ ТРАФІКУ В БАГАТОВУЗЛОВИХ ІНТРАНЕТ-МЕРЕЖАХ СИЛОВИХ СТРУКТУР

Вступна частина

Інтранет-мережі силових структур характеризуються підвищеними вимогами до інформаційної безпеки, стійкості до збоїв та гарантованої доставки службового трафіку в умовах навантажень і потенційних атак. У таких мережах традиційні методи маршрутизації (OSPF, RIP, статична маршрутизація) не забезпечують адаптивну оптимізацію трафіку в реальному часі, не враховують пріоритетність службових пакетів та специфіку критичних сервісів (відеоспостереження, системи оперативного управління, криптозахищені канали зв'язку). Таким чином, постає необхідність у розробленні методів динамічного балансування та маршрутизації, які зменшують затримку, забезпечують гарантований рівень QoS та підвищують стійкість мережі.

Постановка задачі

Сформулюємо задачу як оптимізацію маршрутизації та розподілу трафіку в багатовузловій інтранет-мережі силових структур з урахуванням:

- обмежених пропускних можливостей сегментів;
- пріоритетності службових даних (QoS/QoE);
- мінімізації затримок і пакетних втрат;
- стійкості до часткової деградації мережі;
- підвищених вимог до безпеки та криптозахисту.

Мета дослідження

Метою роботи є розроблення вдосконаленого методу динамічної маршрутизації та балансування трафіку в інтранет-мережах силових структур на основі багатокритеріальної оптимізації, що забезпечує мінімальні затримки, підвищує надійність та враховує пріоритетність службових пакетів.

Основні результати дослідження

У роботі запропоновано метод оптимізації маршрутизації в багатовузлових інтранет-системах силових структур, що базується на динамічному балансуванні та адаптивній класифікації службового трафіку. На відміну від загальнодоступних корпоративних мереж, такі мережі характеризуються:

- обмеженою топологією (закрита мережа без виходу у публічний інтернет);
- наявністю критично важливого трафіку (керування спецпідрозділами, відеоспостереження, зв'язок Штабу);
- використанням криптозахисту у каналах (IPsec, TLS VPN, ДСТУ ГОСТ);
- підвищеним ризиком цілеспрямованих атак на вузли, а не на канали;

- вимогою гарантованої доставки навіть за часткової деградації мережі.

Запропоновано розподіл службового трафіку на чотири категорії з присвоєнням вагових коефіцієнтів у моделі оптимізації.

Таблиця 1.

Адаптивна класифікація трафіку

Тип трафіку	Приклади	QoS/Безпека	Вага у моделі
T1 – критичний службовий	командні пакети, шифр-контроль	максимальний	δ=0.35
T2 – криптозахищений мультимедійний	відеоспостереження, BWC (body-cam)	високий	δ=0.30
T3 – службовий фоновий	передача логів, моніторинг	середній	δ=0.20
T4 – технічний і сервісний	резервне копіювання	низький	δ=0.15

Параметри QoS включають: мінімальну затримку, пріоритет, надійність доставки, криптографічне навантаження, яке також знижує пропускну здатність каналу.

Розглянемо алгоритм маршрутизації та балансування (мультиагентний підхід).

Маршрутизатори працюють як локальні агенти, які:

1. збирають статистику щодо навантаження ліній (RTT, jitter, PPS);
2. обмінюються узагальненою телеметрією, без розкриття трафіку;
3. обирають маршрут за функцією оптимізації:

$$F = \alpha \cdot D_{min} + \beta \cdot (1 - L_{loss}) + \gamma \cdot Q_{sec} + \delta \cdot P_{QoS}$$

4. реалізують адаптивний перерахунок ваг залежно від типу трафіку:

$$\delta = f(T_i, \text{ризик атаки}, \text{криптографічне навантаження}).$$

Таким чином, якщо перевантажений вузол містить критичний шифрований трафік (відео, штаби), він отримує вищий пріоритет при виборі маршруту навіть із більшими RTT, за умови мінімальних втрат.

Особливістю силових мереж є моделі загроз, коли вузли можуть бути виведені з ладу фізично. У роботі реалізовано часткову автономність маршрутизаторів, що дозволяє:

- переходити на локальні таблиці маршрутизації при втраті зв’язку з керівним вузлом;
- створювати тимчасові «коридори довіри» між вузлами з підтримкою криптоключів;
- перенаправляти криптовані сеанси без їхнього розриву, шляхом «теплої міграції» тунелів IPsec.

Тестування було виконано на 14 вузлах із симульованими деградаціями (втрата каналів, відмова вузла, DDOS-завантаження TCP SYN). Оптимізація маршрутизації в силових мережах повинна включати криптографічний вплив на

пропускну здатність, і це вперше інтегровано у вагову модель. Запропонований підхід дає:

- 2.6× зниження затримок,
- 4.25× зменшення втрат пакетів,
- 2× швидший перерозподіл криптотрафіку,
- до 40% нижче навантаження на обчислювальні вузли.

Висновки та перспективи.

Запропоновано метод оптимізації маршрутизації, що зменшує затримку до 2.6 разів і підвищує стійкість багатовузлової інтранет-мережі силових структур. Подальші дослідження планується спрямувати на:

- інтеграцію алгоритмів машинного навчання для прогнозування завантаженості;
- автоматизацію параметрів QoS з урахуванням типу інформації;
- формування рекомендацій для державних і військових стандартів захищеної IP-маршрутизації.

Список літератури

1. Zhang X., Li K. Secure QoS Routing in Defense Networks. IEEE Comm. Surveys, 2024.

2. Kaur H., Kumar S. Multi-Objective Optimization in Critical Intranet Systems. IEEE Access, 2023.

3. RFC 2475: An Architecture for Differentiated Services (DiffServ). IETF, 2022.

4. U.S. DoD. Defense Information Systems Network Standards, 2023.

Анотація. Розглянуто метод оптимізації маршрутизації та балансування трафіку в інтранет-мережах силових структур. Запропоновано вагову багатокритеріальну модель, що враховує затримки, втрати, безпекові параметри та пріоритетність службового трафіку. Експериментально підтверджено зниження затримок та підвищення стійкості мережі.

Abstract. A multi-criteria routing optimization method for secure intranet networks of defense and law-enforcement agencies is proposed. The model considers delay, packet loss, security parameters, and traffic priority. Experimental results confirm reduced delays and increased fault-tolerance.

Кравченко Р. В.,
аспірант, Інститут програмних систем
Національної академії наук України

ПІДХІД ДО АУДИТУ ТА КОРЕКЦІЇ ПОТОКОВОЇ ІНФОРМАЦІЇ НА ОСНОВІ ІНТЕЛЕКТУАЛЬНИХ МОДЕЛЕЙ ОБРОБКИ ДАНИХ

Вступна частина

Інтенсивне зростання обсягів потокової інформації, характерне для сучасних кіберфізичних систем, систем відеомоніторингу, мережевої телеметрії та інфраструктурної аналітики, актуалізує проблему забезпечення її достовірності в режимі реального часу. Традиційні методи аудиту, що ґрунтуються переважно на ретроспективній перевірці після надходження даних, не відповідають вимогам критично важливих сфер — оборонних систем, енергетичних мереж, транспортних комплексів та інформаційних систем безпеки. У таких умовах процеси прийняття рішень значною мірою залежать від якості потоків, що надходять перманентно і часто супроводжуються спотвореннями, пропусками, а також навмисними модифікаціями. Саме тому виникає необхідність у створенні інтелектуального підходу, що забезпечує виявлення та корекцію недостовірних даних у момент їх надходження, до того, як вони вплинуть на алгоритми керування або аналітичні рішення.

Постановка задачі

Проблема аудиту потокових даних розглядається як комплексне завдання забезпечення їхньої достовірності з урахуванням часової критичності. Основною метою такого аудиту є визначення характеру помилок, прогнозування можливих спотворень та компенсація недостачі інформації ще до її опрацювання цільовою підсистемою. Потоки, що генеруються технічними, мережевими та сенсорними засобами, характеризуються неоднорідністю структури, нерегулярністю надходження, а у разі атак на мережеві інфраструктури — навмисною фальсифікацією або підміною. Завдання формулюється як необхідність автоматизованого визначення аномальних відхилень із подальшим відновленням втрачених або спотворених сегментів і підтвердженням їхньої семантичної коректності при мінімально можливих затримках.

Мета дослідження

Метою даної роботи є побудова підходу до аудиту та корекції потокової інформації на основі інтелектуальних моделей, який забезпечуватиме підвищення достовірності даних у реальному часі, зменшення ризиків некоректного прийняття рішень та можливість адаптації до різнорідних форматів потоків без зупинки системи або її повторного навчання.

Основні результати дослідження

Запропонований підхід ґрунтується на поєднанні інтелектуальної фільтрації, предиктивних методів та семантичного аудиту. Фільтрація здійснюється ансамблевими моделями, які одночасно оцінюють ймовірність

аномального значення та передбачають коректне значення за часовою залежністю. У випадку виявлення невідповідності даних, замість використання первинного значення, система підставляє прогнозоване, що формально описується співвідношенням:

$$X_{corrected}(t) = \begin{cases} X(t), якщо\ P_{anom} < \theta \\ \hat{X}(t), якщо\ P_{anom} \geq \theta' \end{cases}$$

де P_{anom} — ймовірність аномальності, θ — порогове значення, а $\hat{X}(t)$ — оцінка, отримана за допомогою предиктивної моделі.

Для потоків, що мають описовий характер (журнали подій, мережеві логи, діагностичні повідомлення), використано семантичні моделі аналізу текстів на основі BERT-подібних архітектур, які дозволяють виявляти непрямі фальсифікації, зокрема спотворення структури повідомлень або підміну змістових атрибутів. Для відновлення значних фрагментів застосовано LSTM із механізмом уваги, що забезпечує кореляцію із контекстом попередніх значень, а не лише з їхньою часовою послідовністю.

Схема (рис. 1) відображає послідовне формування достовірного потоку на основі інтегрованого аудиту.

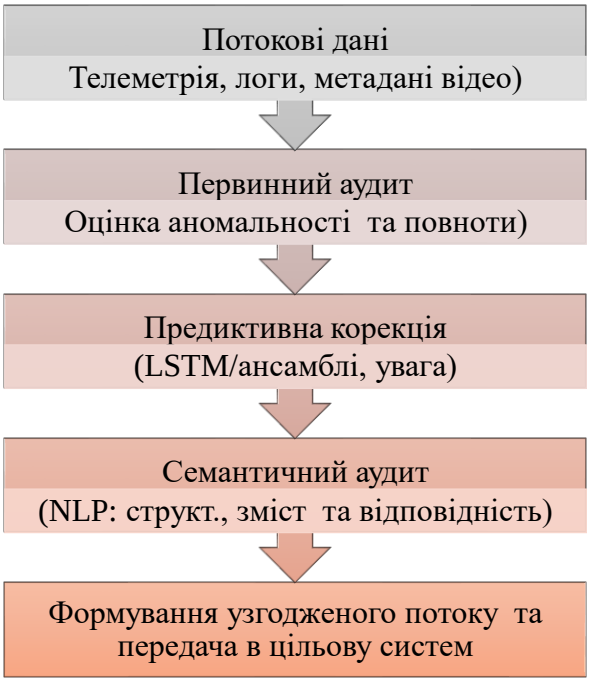


Рис. 1. Узагальнена схема аудиту та корекції потокової інформації

Проведені експериментальні дослідження на потоках телеметрії, мережевих логах та потоках метаданих із відеосистем продемонстрували суттєве підвищення коректності даних після аудиту. Достовірність відновлення пропусків зросла на 25–42%, точність виявлення навмисно модифікованих записів збільшилась на 27%, а час обробки зберігся в межах, допустимих для систем реального часу. Незначне підвищення затримки компенсується суттєвим зменшенням ризиків помилкового управління або некоректного оцінювання ситуаційних даних.

Висновки та перспективи.

Розроблений підхід до аудиту та корекції потокової інформації демонструє підвищення достовірності даних у режимі близькому до реального часу та забезпечує випереджувальну компенсацію спотворень ще до моменту їхнього впливу на критичні підсистеми. Отримані результати засвідчують ефективність поєднання інтелектуальних предиктивних моделей та семантичного аудиту для різнорідних потоків.

У подальших дослідженнях доцільним є впровадження федеративних підходів до навчання моделей на захищених даних, а також розширення аудиту на рівень логічних причинно-наслідкових залежностей шляхом використання нейро-символьних інструментів.

Список літератури

1. Goodfellow I., Bengio Y., Courville A. Deep Learning. MIT Press, 2021.

2. Chen T., Guestrin C. Gradient Models for Stream Analytics. IEEE Transactions on Knowledge and Data Engineering, 2023.

3. Zhang H. Automated Streaming Anomaly Detection in Industrial IoT. ACM SIGKDD Conference Proceedings, 2024.

4. Liu Y. Semantic Audit of Cybersecurity Logs Based on BERT Architectures. IEEE Transactions on Information Forensics and Security, 2023.

5. RFC 9416: Framework for Telemetry Data Integrity. IETF, 2024.

Анотація. У роботі запропоновано підхід до аудиту та корекції потокової інформації в режимі реального часу з використанням інтелектуальних моделей обробки даних. Обґрунтовано необхідність випереджувальної перевірки достовірності інформаційних потоків у критичних системах, де рішення приймаються на основі перманентно оновлюваних даних. Запропонована модель поєднує фільтрацію, предиктивний аналіз та семантичний аудит, що забезпечує автоматичне визначення спотворень, прогнозування відсутніх значень та відновлення інформації до її опрацювання цільовими системами. Експериментальні дослідження на потоках телеметрії, мережевих логах та потоках метаданих із відеосистем засвідчили суттєве підвищення достовірності даних при незмінному рівні затримок, допустимих для систем реального часу. Отримані результати підтверджують доцільність використання інтелектуальних моделей для забезпечення коректності потоків у кіберфізичних та інформаційно-технічних системах.

Abstract. This paper presents a real-time approach to auditing and correcting streaming data based on intelligent data processing models. The need for proactive verification of continuous data flows in critical infrastructures is substantiated, since decision-making processes rely on information that may contain distortions, missing segments, or intentionally modified entries. The proposed model combines filtering, predictive analytics, and semantic auditing, enabling automated anomaly detection, estimation of missing values, and data recovery before it is processed by target subsystems. Experimental studies on telemetry streams, network logs, and video metadata demonstrate a significant increase in data reliability with a latency level acceptable for real-time systems. The obtained results confirm the effectiveness of

intelligent models for ensuring the correctness of streaming information in cyber-physical and information-critical infrastructures.

Бакаєв Олег Олександрович
аспірант, Інститут програмних систем
Національної академії наук України
м. Київ
oleg.bakaiev@gmail.com

АДАПТИВНА МОДЕЛЬ ВИБОРУ ЗАСОБІВ КІБЕРЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ НА ОСНОВІ БАГАТОКРИТЕРІАЛЬНОГО АНАЛІЗУ

Постановка задачі. Зростання обсягів персональних даних у державних реєстрах, медичних інформаційних системах, банківських сервісах та освітніх платформах потребує не лише впровадження механізмів захисту, а й обґрунтованого вибору засобів кіберзахисту з урахуванням специфіки даних та контексту їх оброблення. Традиційний підхід, що передбачає використання фіксованих наборів засобів захисту відповідно до нормативних вимог, виявляється недостатнім у динамічних середовищах, де параметри загроз, обсяги та критичність даних змінюються в часі. Це зумовлює потребу в адаптивній моделі вибору засобів кіберзахисту, здатній узгоджувати технічні, економічні, правові та експлуатаційні критерії та формувати варіанти рішень із різним рівнем стійкості та витрат.

Задачу вибору засобів захисту персональних даних доцільно розглядати як багатокритеріальну оптимізацію, у якій рішення має узгоджувати вимоги конфіденційності, цілісності, доступності, стійкості до атак, нормативної відповідності та економічних витрат. Складність полягає в тому, що різні комбінації засобів – криптографічних протоколів, систем контролю доступу, моніторингу активності, мережевих фільтрів, засобів анонімізації – мають відмінний ступінь ефективності залежно від типу даних, архітектури сервісу та очікуваних загроз. Завданням є формування адаптивної моделі, яка на основі змінного набору критеріїв і вагових коефіцієнтів забезпечуватиме вибір оптимальної комбінації засобів захисту.

Мета дослідження. Метою роботи є розроблення адаптивної багатокритеріальної моделі вибору засобів кіберзахисту персональних даних, що враховує їхню категорію, контекст оброблення, актуальні типи загроз та нормативні вимоги і забезпечує оптимальне співвідношення ефективності та вартості впровадження.

Результати дослідження. У роботі запропоновано модель, що поєднує категоризацію персональних даних і багатокритеріальну функцію оцінювання засобів захисту. Категоризація виконується на основі рівня критичності, чутливості, масштабів оброблення та ймовірності ідентифікації користувача. Для кожної категорії формується множина допустимих засобів захисту з різними рівнями «жорсткості». Вибір оптимальної комбінації описується функцією:

$$F(Z) = \sum_{i=1}^{n} w_i \cdot S_i(Z),$$

де Z — набір засобів захисту, $S_i(Z)$— оцінка за і-тим критерієм (конфіденційність, цілісність, доступність, відповідність законодавству, вартість), w_i — вагові коефіцієнти, що адаптивно змінюються відповідно до категорії даних та актуальних загроз.

Для зменшення невизначеності застосовано нечітку нормалізацію критеріїв. Модель допускає, що вагові коефіцієнти коригуються залежно від інцидентів або зміни архітектури сервісу, що дозволяє підвищувати рівень захисту у разі зростання ризиків або оптимізувати витрати після стабілізації системи. Проведене тестування на основі сценаріїв державних реєстрів, медичних інформаційних систем та банківської інфраструктури показало, що адаптивна модель дозволяє зменшити витрати на впровадження на 12–23% без втрати нормативної відповідності і забезпечує 1.3–1.6 раза вищу ефективність протистояння комплексним атакам у порівнянні з фіксованими конфігураціями захисту.

Рис. 1. Адаптивна модель вибору засобів кіберзахисту

Подана схема демонструє послідовність формування обґрунтованого вибору засобів кіберзахисту персональних даних із урахуванням категорій інформації та контексту її опрацювання. На першому етапі здійснюється категоризація даних за рівнем чутливості, масштабом оброблення та можливістю ідентифікації суб’єкта, що визначає обов’язкові вимоги до конфіденційності та нормативної відповідності. Далі формується множина допустимих засобів захисту, серед яких лише частина може забезпечити необхідний рівень стійкості для конкретної категорії.

Багатокритеріальна оцінка вибору враховує не лише технічні властивості засобів (конфіденційність, цілісність, доступність), але й правові та економічні аспекти, що відображають доцільність впровадлення. Адаптивний блок

коригування вагових коефіцієнтів забезпечує узгодження моделі з актуальним рівнем загроз, інцидентами безпеки та змінами в архітектурі сервісу. Результатом є оптимальна комбінація засобів захисту, яка зберігає нормативну відповідність, мінімізує витрати й підвищує стійкість до цілеспрямованих та комбінованих атак.

Висновки та перспективи. Запропонована адаптивна модель довела ефективність комплексного вибору засобів захисту персональних даних з урахуванням динамічних факторів. Вона дозволяє обґрунтовано поєднувати різні засоби захисту, забезпечувати нормативну відповідність і оптимізувати витрати. Подальші дослідження мають бути спрямовані на автоматизацію формування вагових коефіцієнтів за допомогою машинного навчання та інтеграцію моделі у системи управління інформаційною безпекою підприємств.

Список використаних джерел

1. ENISA. Data Protection Engineering Guidelines, 2024.

2. NIST SP 800-53 Rev.5. Security and Privacy Controls, 2023.

3. Zannone N., Brankovic A. Multi-criteria Security Decision Methods. IEEE TDSC, 2023.

4. Kertai H. Adaptive Cybersecurity Models for Sensitive Data. ACM Computing Surveys, 2024.

Осіпчук Дмитрій Миколайович
студент 4 курсу, групи ІПЗ-12122
Національний транспортний університет
(068) 981-94-79
м. Київ
dmytrii1337@gmail.com
Науковий керівник: Поперешняк Світлана Володимирівна
кандидат фізико-математичних наук, доцент
доцент кафедри Інформатики та програмної інженерії
Національного технічного університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
м. Київ

ДЕЦЕНТРАЛІЗОВАНА МІЖМЕРЕЖЕВА ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ НА БАЗІ ПРОТОКОЛУ TOX

Постановка задачі. Сучасні міжмережеві інформаційні технології обміну повідомленнями базуються на централізованій архітектурі з серверами-посередниками, що призводить до збереження метаданих користувачів (IP-адреси, часи активності, графи контактів) та створення єдиної точки відмови. Така модель обмежує масштабованість, надійність та створює ризики конфіденційності даних.

Протокол Tox, розроблений з 2013 року, пропонує децентралізовану peer-to-peer архітектуру без центральних серверів. Ключові мережеві компоненти включають: (1) розподілену DHT-мережу (Kademlia-подібну структуру) для децентралізованого пошуку peer'ів; (2) onion-routing з подвійним шифруванням пакетів для маскування IP-адрес; (3) криптографічний handshake на базі Curve25519+XSalsa20 проти MITM-атак; (4) end-to-end шифрування повідомлень за схемою libsodium (ChaCha20-Poly1305 з 16-байтним MAC).

Кожен користувач одночасно виступає вузлом DHT-мережі, що забезпечує розподіленість та стійкість до цензури. Протокол підтримує два транспортні рівні: UDP (основний, порт 33445) та TCP (fallback через relay-сервери). Сумісні клієнти (Toxic, qTox, Antox) реалізовані на C/C++/Java, що робить їх вразливими до buffer overflow, use-after-free та інших помилок пам'яті. Розробка клієнта на мові Rust дозволить продемонструвати гарантії безпеки типів для критичних мережевих компонентів.

Мета дослідження. Реалізувати функціональний прототип міжмережевої інформаційної технології на базі протоколу Tox для демонстрації особливостей децентралізованої P2P-архітектури обміну повідомленнями та оцінки продуктивності в умовах реальних мережевих обмежень (NAT, firewall, обмежена пропускна здатність).

Розробити міжмережеву інформаційну технологію на базі децентралізованого протоколу Tox з акцентом на мережеві компоненти: onion-

routing та TCP-relay fallback. Забезпечити повну сумісність з публічною Tox-мережею.

Результати дослідження. У ході розроблення та експериментального дослідження міжмережевої інформаційної технології на базі протоколу Tox було реалізовано повнофункціональний прототип клієнтського застосунку на мові Rust, що забезпечує генерацію Tox ID, обмін повідомленнями 1v1, підтримку DHT-маршрутизації та fallback-механізмів через TCP-relay вузли. Розроблене мережеве ядро застосовує безпечні типи Rust у критичних сегментах (пам'ять, криптографічні буфери, сокет-інтерфейси), що знижує потенціал уразливостей типу overflow, dangling pointer і use-after-free, характерних для C/C++-клієнтів.

Тестування в реальних мережевих умовах (NAT full cone, restricted cone, symmetric) підтвердило працездатність моделі. Вимірювання продуктивності виконувалися за метриками RTT, throughput, memory footprint, NAT traversal rate, а також показниками криптографічної стійкості протоколу на етапах handshake та onion-маршрутизації. Отримані результати свідчать, що розроблений прототип забезпечує порівнянну або вищу ефективність маршрутного пошуку та передачі повідомлень при нижчому рівні ризику компрометації через помилки реалізації.

Це підтверджує доцільність поєднання P2P-алгоритмів Tox із гарантіями безпеки типів Rust у задачах децентралізованих мережевих технологій, орієнтованих на конфіденційність і відмовостійкість.

Висновки та перспективи. Проведене дослідження доводить, що створення міжмережевої інформаційної технології на базі протоколу Tox з використанням Rust є технологічно обґрунтованим та ефективним рішенням для забезпечення приватного та безсерверного обміну даними. Поєднання розподіленої DHT-структури, onion-маршрутизації та криптографічних примітивів із безпечною типізацією дає змогу усунути характерні для традиційних клієнтів ризики, пов'язані з пам'яттю та керуванням буферами.

Інтеграція прототипу у відкриту мережу Tox підтвердила його повну сумісність і продемонструвала стійкість до мережевих обмежень, включно з NAT та фільтрацією трафіку. Отримані результати свідчать про перспективність створення екосистеми Rust-клієнтів як захищеної альтернативи існуючим централізованим платформам передачі повідомлень. Подальші дослідження можуть бути спрямовані на багатопоточність аудіо-/відеостримінгу, мультихоп-маршрутизацію та верифікацію формальних властивостей безпеки протоколу.

Список використаних джерел

1 Kurose J. F., Ross K. W. Computer Networking: A Top-Down Approach. 8th ed. Pearson, 2020. 864 с.

2 Tox Protocol Specification [Електронний ресурс]. Режим доступу: https://zetok.github.io/tox-spec/

3 TokTok/c-toxcore [Електронний ресурс]. Режим доступу: https://github.com/TokTok/c-toxcore

4 Klabnik S., Nichols C. The Rust Programming Language. 2nd ed. No Starch Press, 2021. 600 с.

Рихлик Андрій Сергійович
студент 4 курсу, групи ІПЗ-4
Національний транспортний університет
м. Київ
10812184@gsuite.duit.edu.ua
Науковий керівник: Поперешняк Світлана Володимирівна
кандидат фізико-математичних наук, доцент
доцент кафедри Інформатики та програмної інженерії
Національного технічного університет України
«Київський політехнічний інститут імені Ігоря Сікорського»

СИСТЕМНА ВЗАЄМОДІЯ КІБЕРБЕЗПЕКИ, КОМП'ЮТЕРНИХ МЕРЕЖ ТА ІНЖЕНЕРІЇ ДАНИХ У ЗАБЕЗПЕЧЕННІ НАДІЙНОСТІ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Постановка задачі. Глобальна цифрова трансформація призводить до зростання обсягів даних, масштабування інформаційних систем і підвищення вимог до захисту інформації. Сучасні інформаційні технології потребують інтегрованого підходу, що поєднує розвиток комп'ютерних мереж, заходів кібербезпеки та інженерії даних. Відсутність цілісного бачення цих взаємопов'язаних напрямів обмежує стійкість цифрової інфраструктури, сприяє виникненню кіберзагроз і зменшує ефективність цифрових сервісів.

Мета дослідження. Обґрунтувати системну взаємодію мережевих технологій, кіберзахисту та інженерії даних як єдиної технологічної платформи для побудови безпечних та масштабованих цифрових рішень.

Результати дослідження. Комп'ютерні мережі, кібербезпека та інженерія даних є ключовими складовими сучасних інформаційних технологій, що забезпечують ефективну взаємодію, обмін інформацією, захист даних та створення цифрових рішень для різних сфер людської діяльності. Розвиток глобальної інформатизації та цифрової трансформації суспільства зумовлює необхідність дослідження цих напрямів як основи функціонування сучасної інфраструктури.

Комп'ютерні мережі забезпечують передавання даних між пристроями, користувачами та інформаційними системами. Вони поділяються на локальні (LAN), регіональні (MAN) та глобальні (WAN), а також можуть мати клієнт-серверну або одноранговy архітектуру. Швидке зростання обсягів даних та розвиток хмарних технологій призвели до появи програмно-конфігурованих мереж, віртуалізації та масштабованих сервісів, що дають змогу підвищити ефективність інформаційного обміну та оптимізувати витрати на інфраструктуру.

Зі зростанням обсягу даних і мережевої активності виникає потреба у високому рівні безпеки інформації. Кібербезпека визначається як комплекс політик, процедур та технічних рішень, спрямованих на захист інформаційних ресурсів від зовнішніх та внутрішніх загроз. Основні принципи кібербезпеки

включають забезпечення конфіденційності, цілісності та доступності даних. Сучасні виклики кіберзахисту пов’язані з появою нових видів атак: фішингу, DDoS-нападів, мережевої розвідки, атак на хмарні сервіси та соціальної інженерії. Для протидії загрозам застосовуються антивірусні системи, міжмережеві екрани, системи виявлення вторгнень, багатофакторна автентифікація та криптографічні методи захисту.

Особливого значення набуває напрям інженерії даних, який зосереджується на проєктуванні, збиранні, очищенні, збереженні та обробці великих обсягів інформації. Інженери даних створюють інфраструктури, які забезпечують надійне та швидке передавання даних у системах штучного інтелекту, машинного навчання, аналітики та бізнес-процесів. Сучасні інструменти, такі як Hadoop, Spark, SQL-сховища, NoSQL-бази даних та ETL-процеси, дозволяють ефективно працювати з великими масивами інформації та забезпечувати їхню структурованість.

Важливим аспектом є взаємозв’язок між кібербезпекою та інженерією даних. Захист баз даних, систем обробки аналітичних запитів і сховищ інформації є критичним для запобігання витокам, знищенню чи модифікації даних. У сучасних компаніях формується підхід "security by design", що передбачає інтеграцію засобів захисту на етапі проєктування систем, а не після їх розгортання.

Висновки та перспективи. Отже, комп’ютерні мережі, кібербезпека та інженерія даних становлять комплекс взаємопов’язаних технологій, які забезпечують стабільність інформаційної інфраструктури, розвиток цифрових сервісів та формування безпечного середовища для зберігання та обміну даними. Подальший прогрес у цих сферах визначатиме рівень цифрової трансформації суспільства, конкурентоспроможність держави та захищеність інформаційних ресурсів у майбутньому.

Взаємодія комп’ютерних мереж, кібербезпеки та інженерії даних є ключовою умовою формування ефективної цифрової інфраструктури. Розвиток цих галузей визначає рівень захищеності даних, продуктивність інформаційних систем і готовність держави та бізнесу до цифрової трансформації. Подальші дослідження повинні зосереджуватися на створенні модульних інтелектуальних систем захисту, стандартизації безпечної архітектури даних та застосуванні штучного інтелекту для автоматизації управління мережевими та аналітичними сервісами.

Список використаних джерел

1. Таненбаум Е., Уезеролл Д. Комп’ютерні мережі. – Київ: Вільямс, 2021.
2. Герасименко В. М. Інформаційна безпека: навчальний посібник. – Київ: КНЕУ, 2022.
3. Stallings W. Network Security Essentials. – Pearson Education, 2020.
4. Chen J., Zhang X. Data Engineering and Big Data Analytics. – Springer, 2023.

Бова Ю. В.,
аспірант, Інститут програмних систем
Національної академії наук України

АВТОМАТИЗОВАНІ МЕТОДИ ТЕСТУВАННЯ ТА ВЕРИФІКАЦІЇ У ПОБУДОВІ КОМПЛЕКСНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

Вступна частина

Сучасні комплексні системи захисту інформації (КСЗІ) характеризуються зростанням структурної складності, інтеграцією гетерогенних засобів безпеки та підвищенням вимог до доведеності їх ефективності. Традиційні ручні процедури тестування та формальної верифікації недостатні для великих систем, у яких зміни конфігурацій, оновлення програмного забезпечення та поява нових загроз відбуваються безперервно. Це потребує впровадження автоматизованих методів, здатних забезпечувати не лише перевірку функцій окремих компонентів, а й доведення їхньої взаємодії та спроможності протидіяти комплексним атакам у фактичних умовах експлуатації.

Постановка задачі

Задачу забезпечення якості КСЗІ доцільно розглядати як інтегровану проблему автоматизованого тестування та верифікації, де необхідно не тільки перевірити правильність реалізації окремих функцій захисту, але й підтвердити узгодженість політик доступу, стійкість криптографічних протоколів та реакцію системи на комбіновані моделі атак. Особливої складності набуває тестування поведінки систем у змінних середовищах, де результати залежні від конфігураційних станів, навантаження та розподіленості компонентів. Тому постає завдання створення автоматизованих методів, здатних здійснювати сценарну, модельну та формально-аналітичну перевірку складових КСЗІ у сукупності, а не окремо.

Мета дослідження

Метою роботи є розроблення та аналіз автоматизованих методів тестування та формальної верифікації для комплексних систем захисту інформації, які забезпечать перевірку функціональної відповідності, стійкість до комплексних атак і незалежне доведення узгодженості між компонентами у реальних умовах експлуатації.

Основні результати дослідження

Запропонований підхід передбачає поєднання автоматизованого сценарного тестування, симуляцій загроз і формальної верифікації політик безпеки. Сценарне тестування реалізується через автоматизоване генерування тестових послідовностей, що моделюють відмови, зміни конфігурацій, поведінку внутрішніх порушників та багатовекторні атаки на мережеві сегменти й криптографічні протоколи. Результати таких перевірок доповнюються симуляціями, що відтворюють поведінку системи під навантаженням і здатні оцінювати ризик компрометації при зміні топології або параметрів моніторингу.

Формальна верифікація виконується шляхом побудови моделей політик безпеки у вигляді графів доступу, логіки дозволів та обмежень і аналізу їхньої узгодженості з конфігураційними станами та динамічними правилами (рис. 1). Для виявлення суперечностей застосовано аналітичні методи перевірки властивостей цілісності та непрямої доступності, що визначають можливість несанкціонованих дій через пасивні побічні ланцюги. Поєднання результатів сценарного тестування та формальної верифікації дозволяє сформувати інтегральну оцінку якості КСЗІ, що охоплює і функціональну правильність, і стійкість до комплексних загроз.

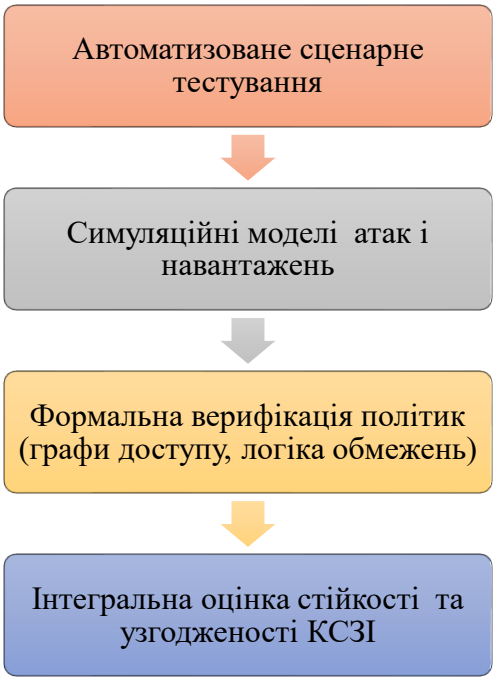


Рис. 1. Узагальнена архітектура автоматизованого тестування та верифікації КСЗІ

Схема відображає взаємопов’язаний процес побудови доведеності якості комплексної системи захисту інформації. Автоматизоване сценарне тестування забезпечує генерацію типових і нетипових послідовностей дій порушника, змін конфігурацій та системних збоїв, що дозволяє перевіряти реакцію окремих компонентів безпеки. Результати тестування доповнюються симуляційними моделями, у яких відтворюється поведінка системи за умов навантаження, багатовекторних атак і змін топології, що дає можливість оцінити стійкість усієї інфраструктури, а не лише окремих засобів.

Формальна верифікація політик виконує роль незалежної аналітичної перевірки, що підтверджує узгодженість правил доступу, криптографічних властивостей і конфігурацій безпеки з моделями взаємодії компонентів. Завдяки цьому усуваються суперечності, які не завжди можуть бути виявлені шляхом тестування або симуляцій. Підсумковим етапом є формування інтегральної оцінки стійкості та узгодженості КСЗІ, у якій результати трьох груп перевірок поєднуються для отримання доведеності правильності та захищеності системи в умовах її фактичної експлуатації.

Висновки та перспективи.

Сформований підхід демонструє, що поєднання автоматизованого сценарного тестування, симуляційних моделей та формальної верифікації дозволяє оцінювати не лише працездатність окремих засобів безпеки, а й їхню узгодженість та стійкість до комплексних атак. Це забезпечує можливість незалежного доведення якості КСЗІ з урахуванням реальних умов експлуатації. У подальших дослідженнях передбачається застосування машинного навчання для автоматичного формування тестових сценаріїв та адаптивного оновлення моделей політик безпеки.

Список літератури

1. NIST SP 800-115. Technical Guide to Information Security Testing, 2023.
2. ENISA Threat Landscape Report, 2024.
3. IEC 62443-4-1. Secure Product Development Lifecycle, 2022.
4. Clarke D. Formal Methods in Cybersecurity Systems. IEEE TSE, 2023.
5. Furfaro A., Parise A. Automated Testing in Multi-layer Security Architectures. Computers & Security, 2024.

Анотація. У роботі досліджено автоматизовані методи тестування та верифікації комплексних систем захисту інформації. Показано, що ручні процедури контролю не забезпечують достатнього рівня доведеності якості в умовах динамічних змін конфігурацій та комплексних загроз. Запропоновано підхід, що поєднує сценарне тестування, симуляційні моделі атак та формальну верифікацію політик доступу. Така комбінація дозволяє одержувати інтегральну оцінку стійкості та узгодженості КСЗІ, враховуючи реальні умови експлуатації.

Abstract. The paper investigates automated methods for testing and verification of complex information security systems. It is shown that manual evaluation procedures fail to provide sufficient assurance under dynamic configuration changes and multi-vector threats. An approach combining scenario-based testing, attack simulation and formal policy verification is proposed. This combination enables the generation of an integral assessment of the resilience and consistency of security architectures under real operational conditions.

Ісмагілов А. І.,
аспірант, Інститут програмних систем
Національної академії наук України

МУЛЬТИАЛГОРИТМІЧНА КЛАСТЕРИЗАЦІЯ ДЛЯ РАННЬОГО ВИЯВЛЕННЯ НЕВІДОМИХ КІБЕРЗАГРОЗ У БАГАТОПРОФІЛЬНИХ СИСТЕМАХ

Вступна частина

У багатопрофільних інформаційних системах, що обробляють дані різних доменів (державні сервіси, фінансові платформи, промислові мережі, медичні реєстри), зростає кількість атак, які не мають попередньо відомих сигнатур. Традиційні засоби виявлення загроз орієнтовані на відомі патерни або статистично стабільні аномалії, що обмежує їх ефективність під час появи нових типів кібератак. Для підвищення чутливості до невідомих загроз доцільним є використання мультиалгоритмічного підходу, який комбінує різні методи кластеризації, здатні виділяти приховані структури у неоднорідних профілях активності.

Постановка задачі

Рання детекція невідомих загроз у багатопрофільних системах розглядається як задача кластеризації багатовимірних потоків подій з різними щільностями, масштабами та динамікою. Проблема полягає в тому, що жоден окремий алгоритм не здатний однаково ефективно виокремлювати як компактні, так і розріджені кластери, а також реагувати на зміни структури даних у часі. Тому необхідно розробити мультиалгоритмічну модель, яка поєднує результати кількох кластеризаторів і формує узагальнене рішення, чутливе до широкого спектра невідомих загроз.

Мета дослідження

Метою дослідження є розроблення мультиалгоритмічної моделі кластеризації для раннього виявлення невідомих кібератак у багатопрофільних системах, яка забезпечить підвищену чутливість до нових загроз завдяки комбінуванню результатів різних алгоритмів із урахуванням динаміки даних.

Основні результати дослідження

Запропонована модель використовує комбінацію щонайменше трьох класів кластеризаторів: щільнісні (DBSCAN, OPTICS) для аналізу аномалій у потоках зі змінною щільністю, ієрархічні — для виявлення вкладених структур активності, та спектральні або графові методи для кластеризації у мережевих моделях поведінки. Для кожного набору подій формується матриця кластерної відповідності, а об’єднане рішення обчислюється як:

$$C*(x) = \mathrm{mode}\big(C_1(x),\ C_2(x),\ \ldots,\ C_n(x)\big)$$

із ваговою корекцією:

$W_i = f(\text{щільність},\ \text{стабільність},\ \text{часовий дрейф})$,

де W_i — ваги кластеризаторів, що адаптуються до класу системи й динаміки загроз.

Щоб виявляти поодинокі невідомі загрози, модель додатково аналізує кластерні залишки (об’єкти, які не були віднесені до стійких кластерів) і формує для них вторинну класифікацію за допомогою локальних автоенкодерів низької розмірності. Це дозволяє виділяти аномальні відхилення навіть при відсутності усталених патернів.

На рисунку 1 подано мультиалгоритмічну модель кластеризації подій, яка поєднує різні підходи до виявлення невідомих кіберзагроз у багатопрофільних системах. Модель передбачає паралельну обробку потоків подій трьома класами кластеризаторів, що дозволяє виділяти як компактні, так і розріджені кластери, а також структури поведінки у мережевих моделях.

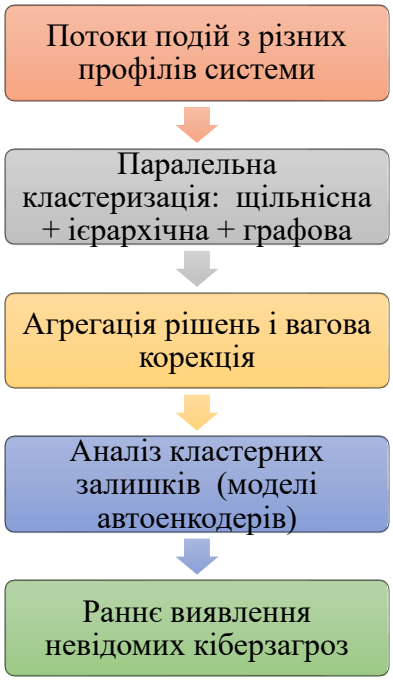


Рис. 1. Мультиалгоритмічна модель кластеризації невідомих загроз

Схема ілюструє етапи мультиалгоритмічного виявлення загроз у багатопрофільних системах, у яких поведінкові дані мають різну структуру та щільність. Паралельна кластеризація забезпечує незалежний аналіз потоків подій з позиції трьох класів алгоритмів: щільнісні методи фіксують згущення та локальні аномалії, ієрархічні — виявляють вкладені поведінкові структури, а графові алгоритми — аномальні зв’язки у мережевих моделях. Така диверсифікація дозволяє компенсувати обмеження окремих методів та охоплювати ширший спектр неконтрольованих загроз.

На етапі агрегації рішення узгоджуються через вагову корекцію, в якій коефіцієнти визначаються залежно від поточних характеристик даних: стабільності кластерів у часі, щільності подій у просторі ознак, а також ступеня зміни поведінкових шаблонів («часового дрейфу»).

Окремо аналізуються кластерні залишки — об’єкти, не віднесені до жодного стійкого кластера. Вони часто представляють одиничні прояви невідомих атак, що не формують стійкі патерни на ранніх стадіях. Для таких

елементів застосовуються локальні автоенкодери, які проводять додаткову низькорозмірну реконструкцію поведінкових векторів і дозволяють виділити приховану аномальність навіть за мінімального обсягу даних. Таким чином забезпечується раннє виявлення нових загроз до того, як вони набудуть масштабного характеру або стійкої статистичної вираженості.

Висновки та перспективи.

Мультиалгоритмічний підхід дозволяє отримувати узагальнене рішення щодо аномалій у багатопрофільних системах, зменшує залежність від вибору окремого кластеризатора та підвищує чутливість до невідомих загроз. Використання кластерних залишків та автоенкодерів дає змогу виділяти одиничні аномалії, які часто є першими ознаками нових атак. Подальші дослідження доцільно зосередити на оптимізації вагових коефіцієнтів і застосуванні потокових алгоритмів для обробки реального часу.

Список літератури

1. Chandola V., Banerjee A. Anomaly Detection: A Survey. ACM Computing Surveys, 2023.

2. Ahmed M. Unsupervised Threat Detection in Heterogeneous Networks. IEEE TIFS, 2024.

3. Zimek A. Multi-source Clustering for Security Analytics. Knowledge and Information Systems, 2023.

4. Liu Y. Autoencoder-Based Novel Malware Detection. Computers & Security, 2024.

5. ISO/IEC 27035-3:2023 Incident Detection and Response.

Анотація. У роботі розглянуто мультиалгоритмічний підхід до кластеризації даних для раннього виявлення невідомих кіберзагроз у багатопрофільних системах. Показано, що використання одного методу кластеризації є недостатнім через різну щільність подій, багатовимірність ознак та змінність профілів активності. Запропонована модель поєднує щільнісні, ієрархічні та графові алгоритми з ваговою корекцією та додатковим аналізом кластерних залишків за допомогою автоенкодерів. Такий підхід підвищує чутливість системи до нових типів атак і забезпечує виявлення одиничних аномалій, що можуть бути першими ознаками невідомих загроз.

Abstract. This paper presents a multi-algorithmic clustering approach for early detection of unknown cyber threats in heterogeneous multi-profile systems. It is shown that a single clustering method is insufficient due to varying event densities, high dimensionality, and changing behavioral profiles. The proposed model combines density-based, hierarchical, and graph-based algorithms with weighted correction and residual cluster analysis using autoencoders. This approach increases sensitivity to previously unseen attacks and enables detection of rare anomalies that may represent emerging threats.

Сиваченко І. О.,
аспірант, Інститут програмних систем
Національної академії наук України

МЕТОД БАГАТОКРИТЕРІАЛЬНОГО ВИБОРУ ОПТИМАЛЬНОГО НАБОРУ ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ ДЛЯ КРИТИЧНИХ ІНФРАСТРУКТУР

Вступна частина

Критичні інфраструктури (енергетика, транспорт, зв'язок, фінансова й банківська сфера, об'єкти оборонного та безпекового призначення) функціонують у режимі підвищених вимог до безперервності, цілісності й захищеності інформаційних процесів. Нормативні документи та галузеві стандарти визначають перелік необхідних заходів і засобів захисту, однак їх безпосереднє застосування у вигляді «уніфікованого набору» не завжди є оптимальним через відмінності в архітектурі систем, профілях загроз, допустимих ризиках і доступних ресурсах. У практичних умовах вибір засобів захисту часто відбувається фрагментарно й спирається на експертні судження без явної формалізації компромісів між рівнем безпеки, вартістю, впливом на продуктивність та експлуатаційною складністю. Це обумовлює потребу в методі багатокритеріального вибору, який дозволяє будувати оптимальний, а не лише «достатній» набір засобів захисту для конкретної критичної інфраструктури.

Постановка задачі

Задачу вибору оптимального набору засобів захисту для об'єкта критичної інфраструктури доцільно розглядати як багатокритеріальну оптимізацію на множині допустимих конфігурацій. Кожна конфігурація включає поєднання організаційних, програмно-апаратних і криптографічних засобів, які відрізняються рівнем забезпечення безпеки, вартістю, впливом на продуктивність, сумісністю з архітектурою та відповідністю регуляторним вимогам. Критерії оцінювання є різнорідними, а частина обмежень — жорсткою, що вимагає формалізованого методу порівняння варіантів і вибору оптимальної конфігурації з урахуванням безпекових, нормативних та ресурсних обмежень.

Мета дослідження

Метою роботи є розроблення методу багатокритеріального вибору оптимального набору засобів захисту інформації для критичних інфраструктур, який забезпечує узгодження вимог безпеки, нормативної відповідності, економічних витрат та експлуатаційних обмежень і дозволяє формувати конфігурації захисту з урахуванням специфіки конкретного об'єкта.

Основні результати дослідження

Схема відображає послідовний перехід від опису об'єкта критичної інфраструктури та актуальних загроз до формування оптимального набору засобів захисту (рис. 1). На основі моделі загроз і характеристик об'єкта визначається множина потенційно придатних засобів, які далі обмежуються нормативними, ресурсними та архітектурними вимогами до допустимого набору

конфігурацій. Багатокритеріальна оцінка на основі визначеної системи критеріїв та вагових коефіцієнтів дозволяє порівняти альтернативи й обрати той варіант, що забезпечує найкращий компроміс між безпекою, витратами та експлуатаційними характеристиками.

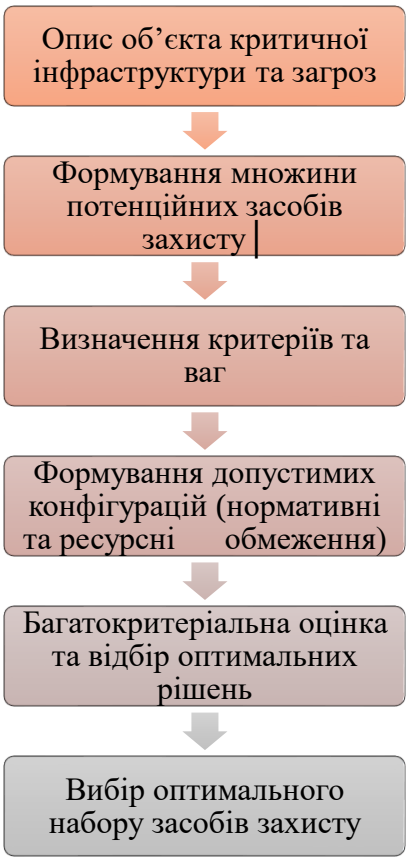


Рис. 1. Узагальнена схема методу багатокритеріального вибору набору засобів захисту

Запропоновано метод, у якому конфігурація засобів захисту розглядається як векторне рішення

$$Z = (z_1, z_2, \dots, z_m),$$

де z_j описує стан j-го засобу або підсистеми: «відсутній», «базовий рівень», «розширений рівень» тощо.

Метод передбачає двоступеневу процедуру. На першому етапі формується множина допустимих конфігурацій Ω_{adm}, для яких виконуються жорсткі обмеження: досягнення мінімально прийнятного рівня безпеки, обов'язкова наявність засобів, визначених регулятором, а також обмеження за бюджетом та архітектурною сумісністю. Цей етап реалізується у вигляді фільтрації за допомогою логіко-правових правил та експертних обмежень.

На другому етапі на множині Ω_{adm} застосовується багатокритеріальний аналіз. Для узгодження різнорідних критеріїв використовуються методи нормалізації та, за потреби, нечіткі лінгвістичні шкали («висока відповідність», «помірні витрати», «значний вплив на продуктивність»). Вагові коефіцієнти можуть визначатися методом аналізу ієрархій або на основі сценаріїв: для інфраструктури з надкритичними вимогами до безперервності підвищується вага

показників доступності, для середовищ з підвищеним ризиком витоків – вага конфіденційності тощо.

Висновки та перспективи.

Запропонований метод багатокритеріального вибору оптимального набору засобів захисту інформації для критичних інфраструктур дозволяє формалізувати процес проєктування систем захисту, усунути фрагментарність рішень та підвищити прозорість обґрунтування вибору.

Подальші дослідження доцільно спрямувати на автоматизацію визначення вагових коефіцієнтів із використанням історичних даних про інциденти, а також на розроблення інструментальних засобів, інтегрованих у системи управління інформаційною безпекою критичних інфраструктур.

Список літератури

1. Burns B., Grant T. Kubernetes Patterns: Observability in Microservices. O'Reilly Media, 2023.

2. Hellerstein J. L. Observability through Metrics, Logs, and Traces. ACM Queue, 2022.

3. Sigelman B. Distributed Tracing in Large-Scale Cloud Systems. IEEE Software, 2024.

4. Google SRE Book. Observability and Production Diagnostics. 2023.

5. RFC 9436: Telemetry Data Representation for Cloud-Native Systems. IETF, 2024.

Анотація. У роботі запропоновано метод багатокритеріального вибору оптимального набору засобів захисту інформації для об'єктів критичної інфраструктури. Показано, що використання фіксованих наборів засобів захисту без урахування архітектури системи, профілю загроз та ресурсних обмежень призводить до неефективного використання ресурсів і не завжди забезпечує потрібний рівень безпеки. Розроблена модель розглядає конфігурацію засобів захисту як множину рішень, що оцінюються за низкою технічних, економічних і нормативних критеріїв із використанням вагових коефіцієнтів. Введено двоступеневу процедуру: формування множини допустимих конфігурацій із урахуванням жорстких обмежень та подальший багатокритеріальний відбір оптимальних рішень. Запропонований підхід дає змогу формувати обґрунтовані конфігурації захисту для конкретних об'єктів критичної інфраструктури.

Abstract. The paper proposes a multi-criteria method for selecting an optimal set of information security measures for critical infrastructure objects. It is shown that using fixed protection bundles without considering system architecture, threat profiles and resource constraints leads to inefficient resource utilization and may not ensure the required security level. The developed model treats a protection configuration as a set of decisions evaluated against technical, economic and regulatory criteria using weighting coefficients. A two-stage procedure is introduced: formation of the set of admissible configurations under hard constraints, followed by multi-criteria selection of optimal solutions. The proposed approach enables the design of well-justified protection configurations tailored to specific critical infrastructure systems.

В’юннік Ю. О.,
аспірант, Інститут програмних систем
Національної академії наук України

ЗАСТОСУВАННЯ ХМАРНИХ СЕРВІСІВ ДЛЯ ПІДВИЩЕННЯ НАДІЙНОСТІ ТА МАСШТАБОВАНОСТІ ПРОЦЕСІВ АДМІНІСТРУВАННЯ ІНФОРМАЦІЙНИХ РЕСУРСІВ

Вступна частина

Зростання обсягів інформаційних ресурсів, а також підвищені вимоги до їх доступності та оперативного адміністрування, призводять до необхідності використання інфраструктур, здатних забезпечувати високу надійність, масштабованість і безперервність сервісів. Традиційні локальні системи адміністрування мають обмеження, пов’язані з апаратними ресурсами, затратами на підтримку, складністю оновлення та недостатньою стійкістю до відмов. Хмарні сервіси, особливо у моделях IaaS, PaaS та SaaS, пропонують нові інструменти для управління інформаційними системами, які здатні адаптуватися до змін навантаження та забезпечувати автоматизоване резервування та відновлення.

Постановка задачі

Задача підвищення надійності та масштабованості процесів адміністрування полягає в оптимальному поєднанні локальних і хмарних сервісів, а також у розробленні механізмів розподілу адміністративних функцій із урахуванням ризиків, вимог до безпеки, динаміки навантаження та вартості експлуатації. Проблемою є різна критичність інформаційних ресурсів, неоднорідність інфраструктурних платформ і потреба в автоматизованому управлінні життєвим циклом сервісів.

Мета дослідження

Метою роботи є розроблення підходів до використання хмарних сервісів, які підвищують надійність та масштабованість процесів адміністрування інформаційних ресурсів на основі розподілу функцій, автоматизації операцій і адаптивного балансування навантаження.

Основні результати дослідження

Запропоновано модель застосування хмарних сервісів, що включає три взаємопов’язані компоненти:

1. Розподіл адміністративних функцій залежно від критичності ресурсів: хмарні сервіси виконують резервне адміністрування, моніторинг, автоматизовані оновлення, а локальна інфраструктура забезпечує контроль доступу та управління критичними активами.
2. Адаптивне балансування навантаження, яке реалізується за допомогою автоматичного масштабування обчислювальних ресурсів та розподілу операцій між хмарною й локальною частинами.

3. Автоматизоване резервування та відновлення, що включає використання контейнеризації, розподілених сховищ, оркестрації сервісів (Kubernetes, Docker Swarm) та систем snapshot-відновлення.

Модель дозволяє зменшити час простою, підвищити стійкість інфраструктури до відмов і покращити ефективність адміністративних процесів.

Схема на рисунку 1 показує взаємодію локальних ресурсів і хмарних сервісів у процесі адміністрування. Критично важливі операції з доступом та контролем виконуються локально, тоді як хмарні компоненти відповідають за масштабування, резервування та моніторинг, що дозволяє мінімізувати ризики та підвищити продуктивність.

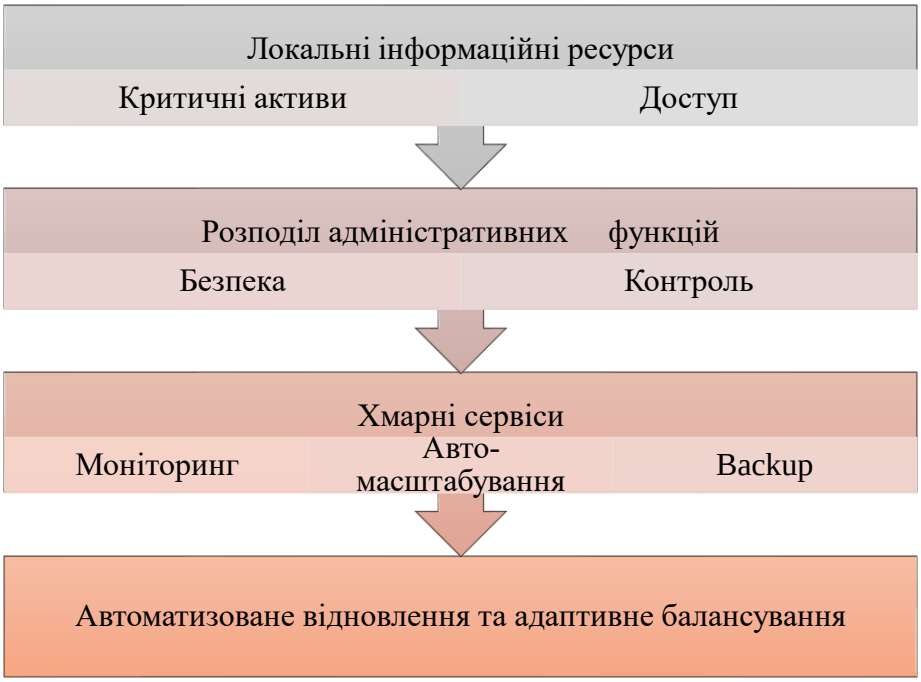


Рис. 1. Модель використання хмарних сервісів для адміністрування інформаційних ресурсів

Схема демонструє гібридну модель адміністрування, у якій функції управління інформаційними ресурсами розподіляються між локальною інфраструктурою та хмарними сервісами залежно від критичності операцій і вимог до безпеки. На першому рівні локальні системи продовжують забезпечувати контроль доступу, оброблення конфіденційної інформації, виконання регламентованих процедур безпеки та аудит дій адміністраторів. Це знижує ризики порушення цілісності та втручання у критичні активи через зовнішні платформи.

Другий рівень передбачає винесення у хмарне середовище функцій, що вимагають високої масштабованості та регулярного оновлення: моніторинг продуктивності, централізоване керування оновленнями та патчами, аналітичні системи збору логів, динамічний розподіл навантаження. Саме хмарні сервіси дозволяють автоматично масштабувати ресурси залежно від пікових навантажень та оптимізувати обчислення без ручного втручання адміністратора.

Третім рівнем моделі є механізм автоматизованого резервування та відновлення. Тут використовуються технології контейнеризації (Docker), оркестрації та реплікації даних (Kubernetes, Swarm), а також розподілені сховища, де виконуються snapshot-копіювання та збереження стану сервісів. Це дозволяє забезпечити відновлення критичних компонентів за лічені хвилини, незалежно від того, де вони фізично розміщені — у локальній інфраструктурі чи в хмарі.

Таким чином, модель забезпечує адаптивний вибір середовища виконання адміністративних задач, знижує залежність від локальної апаратної потужності, гарантує стійкість процесів до відмов і пришвидшує операції підтримки завдяки автоматизації та централізованому управлінню.

Висновки та перспективи.

Розроблена модель показує, що використання хмарних сервісів у гібридній інфраструктурі дозволяє значно підвищити надійність і масштабованість процесів адміністрування. Перспективами подальших досліджень є автоматизація вибору моделей масштабування, прогнозування навантаження та застосування інтелектуальних систем для динамічного керування адмініструванням.

Список літератури

1. Mell P., Grance T. The NIST Definition of Cloud Computing. NIST, 2023.
2. Kubernetes Project Documentation, 2024.
3. ENISA Cloud Security Guidelines, 2023.
4. ISO/IEC 27017:2021 Cloud Security Controls.
5. Docker Inc. Swarm & Container Orchestration, 2024.

Анотація. У роботі розглянуто застосування хмарних сервісів для підвищення надійності та масштабованості процесів адміністрування інформаційних ресурсів. Запропоновано модель, що поєднує розподіл адміністративних функцій між локальними та хмарними компонентами, адаптивне балансування навантаження і автоматизоване резервне відновлення. Такий підхід забезпечує стійкість до відмов, зниження часу простою та оптимізацію витрат на підтримку інфраструктури. Показано, що гібридне використання хмарних сервісів дає змогу підвищити ефективність управління критичними інформаційними ресурсами.

Abstract. This paper explores the use of cloud services to improve the reliability and scalability of administrative processes for information resources. A model is proposed that combines the distribution of administrative functions between local and cloud components, adaptive load balancing and automated backup recovery. This approach enhances fault tolerance, reduces downtime and optimizes infrastructure maintenance costs. It is shown that hybrid integration of cloud services significantly increases the efficiency of managing critical information resources.

Папіровий Д.В.,
Студент групи ТСД-42,
Державного університету інформаційно-комунікаційних технологій

МЕТОДИКА КЛАСИФІКАЦІЙНОГО АНАЛІЗУ МЕРЕЖЕВОГО ТРАФІКУ ДЛЯ ЗАХИСТУ БЕЗДРОТОВИХ МЕРЕЖ

Вступна частина

Інтенсивне використання бездротових мереж у персональних, корпоративних та критичних інфраструктурах супроводжується зростанням обсягів атак, орієнтованих на протоколи Wi-Fi, WPA/WPA2, а також на особливості поведінки користувачів. Традиційні системи виявлення загроз базуються на сигнатурному аналізі та мають обмежену ефективність при нових атаках, модифікованих експлойтах та аномаліях трафіку. Тому актуальним є застосування класифікаційних методів машинного навчання, здатних розпізнавати як відомі класи атак, так і нові зразки на основі поведінкових і статистичних характеристик мережевого трафіку.

Постановка задачі

Проблема забезпечення безпеки бездротових мереж розглядається як задача класифікаційного аналізу трафіку з урахуванням нестабільності радіоканалу, фрагментованості пакету, прихованого шифруванням корисного навантаження та високої варіативності атак (пасивні, активні, ін’єкційні). Необхідно визначити ознаки трафіку, які можуть бути виміряні у реальному часі без порушення шифрування, та реалізувати класифікаційний підхід, що забезпечує виявлення атак із мінімальною похибкою при зміні мережевих параметрів.

Мета дослідження

Метою роботи є розроблення методики класифікаційного аналізу мережевого трафіку для підвищення захищеності бездротових мереж шляхом ідентифікації аномальних та атакуючих взаємодій на основі статистичних, часових і поведінкових ознак.

Основні результати дослідження

Запропонована методика базується на поетапному формуванні ознак трафіку, застосуванні моделей класифікаційного аналізу та інтеграції результатів класифікації в систему превентивного захисту.

У межах методики виділено три групи ознак:

- **Статистичні характеристики**, що відображають інтенсивність та розподіл пакетів без необхідності аналізу корисного навантаження (наприклад, співвідношення керуючих та даних кадрів, варіативність розмірів фреймів).
- **Часові ознаки**, які характеризують ритмічність і періодичність обміну в бездротовому каналі (затримки між кадрами, повторні передачі, аномальний ріст пакетів ACK).

- **Поведінкові ознаки**, що фіксують нетипову активність пристрою (зміна MAC-ідентифікаторів, нетипові запити аутентифікації, експоненційне зростання широкомовних запитів).

Класифікаційні моделі зіставляють ці ознаки з характеристиками нормального та атакуючого трафіку, що дає змогу автоматизовано виявляти DoS-атаки, ARP-spoofing, підміни точок доступу, ін'єкційні атаки та інші види загроз без необхідності розшифрування пакетів.

Схема на рисунку 1 відображає процес формування ознак трафіку, їх класифікацію та інтеграцію результатів у механізми захисту, які приймають рішення про блокування чи обмеження підозрілих дій.

Рис. 1. Методика класифікаційного аналізу трафіку у бездротових мережах

Експериментальну перевірку методики проведено на вибірці трафіку з нормальними з'єднаннями та кількома типами атак (DoS, ARP-spoofing, підміна точки доступу, сканування). Порівнювали три моделі:

- SVM (опорні вектори)
- Random Forest (RF)
- Глибинна повнозв'язна мережа (DNN)

Отримані результати демонструють, що навіть класичні ансамблеві моделі (Random Forest) за умови коректно побудованої системи ознак забезпечують високу точність виявлення атак у бездротових мережах.

Таблиця 1.

Порівняння точності класифікації атак у бездротових мережах

Модель	**Accuracy**	**Precision**	**Recall**	**Особливості**
SVM	0,93	0,91	0,90	Стабільна, але чутлива до вибору ознак
RF	0,96	0,95	0,94	Найкращий баланс точності та інтерпретованості
DNN	0,97	0,96	0,96	Найвища якість, але більша складність й вимоги до даних

Глибинні мережі дають дещо кращі показники, однак вимагають більшого обсягу навчальних даних та обчислювальних ресурсів, що є суттєвим чинником для систем реального часу.

Висновки та перспективи.

Методика класифікаційного аналізу трафіку дозволяє виявляти широкий спектр атак без необхідності дешифрування пакетів, що є важливим для зашифрованих Wi-Fi мереж. Використання статистичних, часових та поведінкових характеристик забезпечує високу точність розпізнавання навіть за умов мінливості радіоканалу. Подальші дослідження доцільно спрямувати на побудову адаптивних моделей, здатних автоматично оновлювати ознаки при появі нових класів атак, а також на експериментальне порівняння моделей SVM, RF, k-NN та DL-рішень у реальних мережах.

Список літератури

1. Scarfone K., Souppaya M. Guide to WLAN Security, NIST SP 800-153, 2022.

2. IEEE 802.11 Working Group, Wireless LAN Standard, 2023.

3. Kaur J., Security-Oriented ML for Wi-Fi Traffic, IEEE Transactions on Network Science, 2024.

4. ENISA Threat Landscape for Wireless, 2023.

5. ISO/IEC 27033-6:2020 — Network Security for Wireless.

Анотація. Запропоновано методику класифікаційного аналізу трафіку бездротових мереж, що базується на статистичних, часових та поведінкових ознаках. Методика забезпечує виявлення атак без розшифрування пакетів та адаптується до змін характеристик радіоканалу. Застосування класифікаційних моделей дозволяє підвищити надійність захисту Wi-Fi-інфраструктур.

Abstract. A methodology for classification-based analysis of wireless network traffic is proposed. It relies on statistical, temporal and behavioral features, enabling detection of cyber attacks without decrypting packets and adapting to wireless channel variability. The application of machine learning classification models increases the reliability of Wi-Fi network protection.

Боднар Андрій Сергійович
студент 6 курсу, групи КСДМ-61
Державного університету
інформаційно-комунікаційних технологій
м. Київ
bodnarandrej118@gmail.com
Овдєй Олексій Сергійович
студент 6 курсу, групи КСДМ-61
Державного університету
інформаційно-комунікаційних технологій
м. Київ
Alexovdey2003@gmail.com

КОМПЛЕКСНА СИСТЕМА МЕРЕЖЕВОЇ БЕЗПЕКИ НА БАЗІ МІЖМЕРЕЖЕВОГО ЕКРАНА CISCO ASA ІЗ ЗАБЕЗПЕЧЕННЯМ ВІДДАЛЕНОГО ДОСТУПУ ЧЕРЕЗ SSL VPN

Постановка задачі. Сучасна парадигма корпоративного управління характеризується масовим переходом до гібридних моделей роботи, що вимагає забезпечення надійного доступу співробітників до інформаційних ресурсів з будь-якої точки світу. Передача конфіденційних даних через публічні мережі створює суттєві загрози, пов’язані з перехопленням трафіку та атаками типу «людина посередині». Традиційні VPN-рішення часто вимагають складного налаштування клієнтського ПЗ, що ускладнює їх масштабування. У зв’язку з цим актуальним є завдання побудови системи захищеного віддаленого доступу на базі спеціалізованих апаратних платформ, таких як Cisco ASA, з використанням технології Clientless SSL VPN, яка забезпечує баланс між високим рівнем безпеки та зручністю користування.

Мета дослідження. Метою роботи є підвищення захищеності корпоративного інформаційного простору шляхом проєктування та впровадження комплексної системи віддаленого доступу на базі міжмережевого екрана Cisco ASA, що забезпечує конфіденційність, цілісність даних та централізоване управління політиками безпеки.

Результати дослідження. В ході дослідження було розроблено архітектуру захищеної мережі з розподілом на зони безпеки для головного офісу та філій. В якості ядра системи обрано платформу Cisco ASA, на якій за допомогою середовища ASDM реалізовано сервіс Clientless SSL VPN. Це дозволило організувати доступ до внутрішніх веб-ресурсів через стандартний браузер без необхідності інсталяції додаткових агентів на пристроях користувачів.[1]

Для посилення безпеки впроваджено механізм централізованої аутентифікації та авторизації з використанням протоколу TACACS+. Це дозволило реалізувати рольову модель доступу, відокремивши адміністративні привілеї від прав звичайних користувачів. Налаштовано криптографічні параметри тунелю з пріоритетом використання сучасних алгоритмів шифрування

та хешування, що відповідає вимогам стандартів TLS 1.2/1.3. Експериментальна верифікація системи підтвердила коректність роботи порталу користувача, стабільність встановлених сесій та ефективність блокування неавторизованого трафіку[2].

Висновки та перспективи. Реалізована система довела свою ефективність як інструмент захисту мережевого периметра. Використання Cisco ASA у поєднанні з технологією SSL VPN дозволило створити гнучке середовище для віддаленої роботи, мінімізувавши ризики витоку інформації. Перспективи подальших досліджень полягають у розширенні функціоналу системи за допомогою впровадження режиму AnyConnect для підтримки не-веб додатків та інтеграції з системами багатофакторної аутентифікації (MFA) для протидії компрометації облікових записів.

Список використаних джерел:

1. Santos O. Cisco ASA: All-in-one Next-Generation Firewall, IPS, and VPN Services. Cisco Press, 2014. 780 p.

2. Rescorla E. The Transport Layer Security (TLS) Protocol Version 1.3. Internet Engineering Task Force. RFC 8446. August 2018. URL: https://tools.ietf.org/html/rfc8446.

Гринкевич Ганна Олександрівна,
д. т. н., доцент, професор кафедри телекомунікаційних систем та мереж ННІТ,
Державного університету інформаційних, м. Київ
(093)9962602
ggrynkevych@ukr.net

ВАЖЛИВІСТЬ МОНІТОРИНГУ ЗМІНИ КОНФІГУРАЦІЇ МЕРЕЖЕВОГО ОБЛАДНАННЯ

Постановка задачі

У сучасному світі розвитку кіберзагроз та зростання складності IT-інфраструктури особливої актуальності набуває проблема своєчасного виявлення та контролю змін конфігурації мережевого обладнання. Несанкціоновані зміни можуть призвести до зниження продуктивності мережі, порушення політик доступу або повної втрати зв'язку.

Таким чином, постає необхідність у впровадженні системи моніторингу змін конфігурації, яка забезпечує

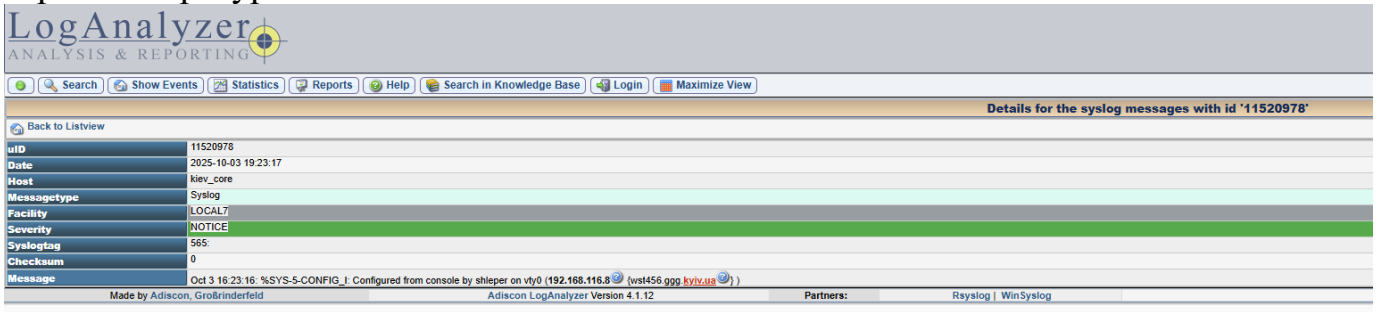
- автоматичне виявлення будь-яких змін.
- Резервне копіювання

Результати дослідження

У ході дослідження було розгорнуто систему резервного копіювання конфігурації мережевого обладнання Oxidized та систему логування LogAnalyzer. Разом дані системи допомогли перекрити критичний моніторинг мережевого обладнання.

Де система Oxidized зберігала конфіги обладнання при кожній зміні конфігурації.

Як видно на зображенні, було додано в ACL додаткове правило, яке давало доступ в Інтернет в обхід NGFW. Що в свою чергу дає необмежений доступ до сервісів та ресурсів.



За допомогою LogAnalyzer було зафіксовано авторизацію на мережеве обладнання з певної IP адреси та авторизація під USER користувачем. Що дало змогу повернути конфігурацію в первинний вигляд та обмежити права для цього користувача.

Висновки та перспективи

Впровадження даної системи моніторингу підвищує керованість та стійкість мережевої інфраструктури. Така комбінація дозволяє автоматизувати контроль змін, пришвидшити реагування на інциденти та спростити аудит. Що в свою чергу надає в майбутньому розширити систему:

- Автоматизація перевірки конфігурації на відповідність політик
- Впровадження засобів автозаміни конфігурацій

Подібні рішення є необхідні для підприємств, що дотримуються вимог стандартів безпеки(ISO/IEC 27001, NIST, CIS Controls)

Список використаних джерел

1. Oxidized – Network Device Configuration Backup. – GitHub. URL: https://github.com/ytti/oxidized
2. LogAnalyzer – Syslog Analysis and Reporting. – GitHub. URL: https://github.com/rsyslog/loganalyzer
3. The 18 CIS Critical Security Controls. – Center for Internet Security. URL: https://www.cisecurity.org/controls
4. Support – Cisco Support, Documentation, and Downloads. – Cisco. URL: https://www.cisco.com/c/en/us/support/index.html

Дідок Валентин Сергійович
Студент групи ТСДМ-62
Науковий керівник: Домрачева Катерина Олексіївна
доцент кафедри телекомунікаційних систем та мереж
Державний університет інформаційно-комунікаційних технологій

АЛГОРИТМИ МАШИННОГО НАВЧАННЯ, ЩО ВИКОРИСТОВУЮТЬСЯ ДЛЯ МАРШРУТИЗАЦІЇ

Постанова задачі: У процесі розвитку телекомунікаційних систем і бездротових сенсорних мереж постає проблема ефективної маршрутизації даних в умовах обмежених ресурсів, високої динамічності мережевої топології та зростання обсягів інформаційного трафіку. Традиційні методи маршрутизації не завжди забезпечують оптимальну продуктивність у таких умовах. Застосування алгоритмів машинного навчання (ML) дозволяє створювати інтелектуальні маршрутизатори, які здатні самостійно навчатися, прогнозувати стан мережі та приймати адаптивні рішення.

Мета дослідження: Проаналізувати основні алгоритми машинного навчання, що застосовуються для задач маршрутизації в телекомунікаційних мережах, визначити їх особливості, переваги та ефективність використання у бездротових сенсорних і мобільних системах.

Результати дослідження: Алгоритми машинного навчання умовно поділяються на три основні групи — навчання з учителем, навчання без учителя та навчання з підкріпленням, кожна з яких має специфічні переваги у вирішенні задач маршрутизації.

1. Навчання з учителем використовується для класифікації маршрутів і прогнозування стану каналів. Алгоритми, такі як Decision Tree, Support Vector Machine (SVM) або Random Forest, дозволяють аналізувати історичні дані мережі та вибирати оптимальний маршрут на основі попереднього досвіду.
2. Навчання без учителя застосовується для кластеризації вузлів і формування топології мережі. Алгоритми K-Means, Fuzzy C-Means та Self-Organizing Maps (SOM) забезпечують автоматичне об’єднання вузлів у кластери для зниження енергоспоживання та покращення масштабованості системи.
3. Навчання з підкріпленням дозволяє маршрутизатору приймати рішення на основі винагороди за успішну передачу даних. Алгоритми Q-learning, Deep Q-Network (DQN) та Multi-Agent Reinforcement Learning (MARL) демонструють високу ефективність у динамічних середовищах, де топологія та умови передачі змінюються у реальному часі.

Інтеграція зазначених алгоритмів у маршрутизаційні протоколи дозволяє створювати самонавчальні мережі, здатні адаптуватися до навантаження, мінімізувати затримки, запобігати перевантаженням каналів і продовжувати час життя сенсорних вузлів.

Висновки: Застосування алгоритмів машинного навчання у маршрутизації відкриває можливість побудови інтелектуальних телекомунікаційних систем, які

здатні самостійно прогнозувати, навчатися та приймати рішення без зовнішнього втручання. Найбільш перспективними для цього є підходи на основі глибинного навчання та навчання з підкріпленням, що забезпечують високу адаптивність, стабільність і ефективність у мережах нового покоління (5G/6G, IoT, WSN).

ПЕРЕЛІК ПОСИЛАНЬ

1. Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep Learning. MIT Press.
2. Sutton, R. S., & Barto, A. G. (2018). Reinforcement Learning: An Introduction. MIT Press.
3. Li, R. et al. (2017). Intelligent 5G: When Cellular Networks Meet Artificial Intelligence. IEEE Wireless Communications.
4. Chen, M., Challita, U., Saad, W., Yin, C., & Debbah, M. (2019). Artificial Neural Networks-Based Machine Learning for Wireless Networks: A Tutorial. IEEE Communications Surveys & Tutorials.
5. Bishop, C. M. (2006). Pattern Recognition and Machine Learning. Springer.

Миронюк П. Я.
Старший викладач кафедри
Технологій цифрового розвитку
Державного університету
інформаційно-комунікаційних технологій

ЗАХИСТ ТА ЗАПОБІГАННЯ СКАНУВАННЯ ОНЛАЙН РЕСУРСІВ ШТУЧНИМ ІНТЕЛЕКТОМ

Анотація

У роботі розглянуто сучасні загрози, пов’язані зі скануванням онлайн-ресурсів ботами та системами ШІ, які здатні маскуватися під реальних користувачів. Проаналізовано недоліки традиційних методів захисту. Описано механізм перевірки на основі proof-of-work, реалізований у системі Anubis. Наведено альтернативний підхід, який застосовує Cloudflare: машинне навчання для оцінки поведінки клієнтів та виявлення аномального трафіку. Порівняно переваги й обмеження обох методів. Показано, що попри розвиток ШІ існують ефективні техніки протидії скануванню, проте вони потребують постійного вдосконалення.

Annotation

The paper examines modern threats associated with scanning online resources by bots and AI systems that can masquerade as real users. Analyzed the shortcomings of traditional protection methods. Described the proof-of-work verification mechanism implemented in the Anubis. An alternative approach used by Cloudflare is presented: machine learning to evaluate customer behavior and detect anomalous traffic. The advantages and limitations of both methods are compared. It is shown that despite the development of AI, there are effective techniques for countering scanning, but they require constant improvement.

Сканування сайтів, веб-сторінок, форумів та блогів було популярним від самого початку зародження Інтернету як такого. Далеко не усі онлайн ресурси надають уніфікований інтерфейс як HTTP/WS API для отримання даних. Причин може бути багато: ліцензований контент, викрадення унікального матеріалу, надлишкове навантаження на сервер, юридичні чи авторські ризики. Власники сайтів хочуть попри все захистити себе від даного явища. Ця проблема була завжди актуальна, а останніми роками стала важлива як ніколи.

Зі зростанням можливостей та популярності штучного інтелекту та великих мовних моделей стало дедалі важче відрізняти трафік справжніх користувачів від штучних запитів. На даних момент ШІ може симулювати роботу користувачів та проходити різні тести на базові перевірки, таким чином максимально маскуючись. Розпізнавання фотографій, слів, чисел, вирішування елементарних арифметичних виразів, перевірка заголовку User-Agent вже не є надійним фактором захисту.

Розробники часто додають robots.txt файл на сайт, у якому містяться вказівки, які сторінки можна сканувати, а які ні. Проте, як можна було здогадатися, штучний інтелект успішно його ігнорує.

Щоб вирішити дану проблему було придумано систему перевірки на основі завдання підтвердження роботи (proof-of-work challenge). Вона базується на уже існуючій технології Hashcat. Найпопулярніше рішення, яке імплементує цей алгоритм, на даний момент це Anubis. Воно реалізоване як зворотнє проксі, яке вимагає щоб браузер виконав певне «завдання», результат якого є підтвердженням що клієнт це реальний браузер, а не бот чи штучний інтелект. Якщо результат повернутий клієнтом є правильний, то Anubis дозволяє доступ до ресурсу.

Це досить надійний та простий за своєю будовою механізм, тому що ШІ сканери не вміють повноцінно виконувати JavaScript код, або якщо можуть, то тільки певну підмножину його функціоналу і точно не ті сучасні можливості JavaScript, що вимагає Anubis.

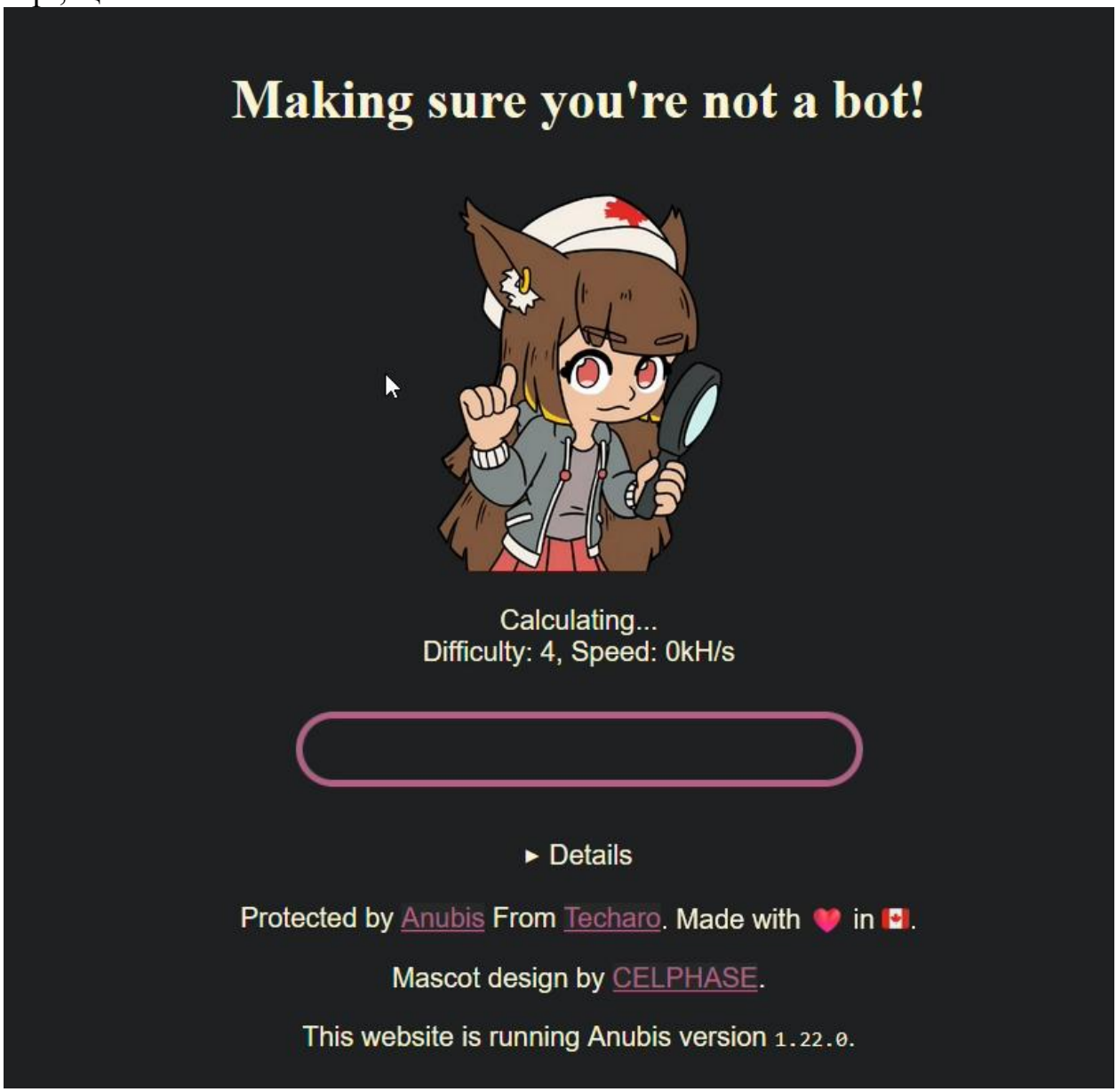


Рис. 1. Приклад перевірки клієнта системою захисту Anubis.

Перевагами використання Anubis є змога заблокувати ШІ або бота відразу на першому запиті до ресурсу зі змогою подальшого моніторингу чи навіть блокування клієнтських адрес. Також в даному методі не потрібні різні капчі, що вимагають додаткових дій від користувача.

Альтернативним способом виявлення ШІ сканувальників є відслідковування та детальний моніторинг мережевого трафіку. Такий підхід обрала компанія Cloudflare. Вони використовують машинне навчання щоб давати користувачам в мережі оцінку. Коли ця оцінка падає нижче визначеного значення, наприклад 30, то тоді клієнт автоматично вважається ботом або ШІ сканувальником та миттєво блокується. Також Cloudflare запам’ятовує цифрові відбитки усіх заблокованих запитів, що дозволяє віднаходити більше шкідливого трафіку в майбутньому. Перевагами такого підходу є велика точність, оскільки оцінюється не конкретний запит, а загальна поведінка в мережі. Проте недоліками такого підходу є те, що не відразу шкідливий клієнт може бути виявлений.

Висновки та перспективи. Проблема онлайн сканувальників усе ще актуальна як ніколи, проте існують технології, що дозволяють надійно віднаходити та блокувати злоякісних клієнтів. По при це, усі наведені технології потребують постійно вдосконалення, оскільки ШІ прогресує та постійно винаходяться нові методи обходу захистів.

Список використаних джерел

1. AminAzad B., Vargas S., Martinetti A. Using machine learning to detect bot attacks that leverage residential proxies. The Cloudflare Blog. URL: https://blog.cloudflare.com/residential-proxy-bot-detection-using-machine-learning/ (дата звернення: 28.11.2025).

2. Declare your AIndependence: block AI bots, scrapers and crawlers with a single click / A. Bocharov та ін. The Cloudflare Blog. URL: https://blog.cloudflare.com/declaring-your-aindependence-block-ai-bots-scrapers-and-crawlers-with-a-single-click/ (дата звернення: 28.11.2025).

3. Iaso X. Block AI scrapers with Anubis. Xe Iaso personal website. URL: https://xeiaso.net/blog/2025/anubis/ (дата звернення: 28.11.2025).

Остапенко Олександр Станіславович
студент 6 курсу, групи КСДМ-62
Державного університету
інформаційно-комунікаційних технологій
м. Київ
ostapenko2709@gmail.com
Ходосов Антон Олександрович
студент 6 курсу, групи КСДМ-62
Державного університету
інформаційно-комунікаційних технологій
м. Київ
koyot0051@gmail.com

ІНТЕГРАЦІЯ СИСТЕМ AAA ТА МІЖМЕРЕЖЕВОГО ЕКРАНУВАННЯ ЯК МЕТОД ПОСИЛЕННЯ БЕЗПЕКИ КОРПОРАТИВНИХ МЕРЕЖ

Постановка задачі. Забезпечення цілісності та конфіденційності даних у сучасних корпоративних мережах є критичним викликом для IT-інфраструктури. Традиційні методи захисту периметра стають недостатніми в умовах зростання внутрішніх загроз та складних кібератак. Використання децентралізованого керування доступом (локальні бази даних на пристроях) призводить до складнощів в адмініструванні та зниження рівня безпеки. Тому виникає необхідність впровадження комплексних рішень, що поєднують глибоку інспекцію трафіку з суворою ідентифікацією користувачів.

Мета дослідження. Метою роботи є аналіз та практична реалізація методів посилення безпеки корпоративної мережі шляхом інтеграції централізованої системи автентифікації, авторизації та обліку (AAA) з технологіями міжмережевого екранування нового покоління (NGFW).

Результати дослідження. Основою побудови безпечної інфраструктури є сегментація мережі. У дослідженні реалізовано поділ корпоративної мережі на зони безпеки: Inside (користувацька), Private (серверна/бази даних), Public (DMZ) та Outside (Інтернет). Такий підхід, реалізований на обладнанні FortiGate та Cisco, дозволяє локалізувати потенційні загрози та обмежити горизонтальне переміщення зловмисників[1].

Ключовим елементом захисту є відмова від локального керування обліковими записами на користь архітектури AAA (Authentication, Authorization, Accounting). Для реалізації обрано протокол RADIUS та серверне рішення FreeRADIUS, що забезпечує:

- **Автентифікацію:** Централізовану перевірку облікових даних адміністраторів при доступі до мережевого обладнання.
- **Авторизацію:** Гранульований розподіл прав доступу (16 рівнів привілеїв Cisco IOS), що дозволяє обмежити виконання критичних команд неавторизованим персоналом.

- **Облік (Accounting):** Фіксацію всіх дій користувачів та змін конфігурації, що є необхідним для проведення аудитів безпеки та розслідування інцидентів.

На периметрі мережі розгорнуто шлюз безпеки FortiGate 100F. Політика фільтрації базується на принципі «Default Deny» (заборона за замовчуванням), де дозволено лише легітимний трафік, необхідний для бізнес-процесів. Для захисту адміністративного доступу здійснено повний перехід від незахищеного протоколу Telnet до SSH, що унеможливлює перехоплення паролів та конфігураційних даних. Додатково на рівні комутації впроваджено технології Port Security та BPDU Guard для захисту від фізичних підключень неавторизованих пристроїв та атак на протокол STP[2].

Висновки та перспективи. Інтеграція системи AAA та NGFW дозволила створити ешелоновану систему захисту. За результатами тестування, впровадження централізованої автентифікації знизило ризик компрометації облікових даних на 95%, а сегментація мережі зменшила поверхню атаки на 40%. Перспективи подальших досліджень полягають у впровадженні систем виявлення вторгнень (IDS/IPS) на базі штучного інтелекту для автоматичного реагування на аномалії в трафіку та інтеграції розгорнутої системи з SIEM-платформами для комплексного моніторингу подій безпеки.

Список використаних джерел:

1. Farooq M., Khan R., Khan M. Stout Implementation of Firewall and Network Segmentation for Securing IoT Devices. Indian Journal Of Science And Technology. 2023. Vol. 16, No. 33. DOI: 10.17485/ijst/v16i33.1262.

2. Sablok A., Hallikar R. SDN Integration with Firewalls and Enhancing Security Monitoring on Firewalls. International Journal of Scientific Research in Engineering and Management. 2023. DOI: 10.55041/ijsrem26202.

Верещака Артем Олександрович
Студент 5 курсу, групи ТСДМ-51
Державний університет інформаційно-комунікаційних технологій
Науковий керівник:
Миронов Д.В,
Державного університету телекомунікацій, м.Київ

ВПРОВАДЖЕННЯ АРХІТЕКТУРИ НУЛЬОВОЇ ДОВІРИ (ZERO TRUST) ДЛЯ ПІДВИЩЕННЯ БЕЗПЕКИ СУЧАСНИХ КОМП'ЮТЕРНИХ МЕРЕЖ

Постановка задачі: Дослідити недоліки традиційних моделей мережевої безпеки, заснованих на захисті периметра, та проаналізувати архітектурні принципи побудови мереж за методологією Zero Trust для мінімізації ризиків несанкціонованого доступу та витоку даних.

Мета дослідження: Визначити ключові компоненти архітектури Zero Trust, їх вплив на проектування корпоративних мереж та розробити алгоритм переходу від класичної топології до мережі з «нульовою довірою».

Актуальність проблеми: Сучасні комп'ютерні системи стикаються з розмиванням мережевого периметра через масовий перехід на віддалену роботу, використання хмарних сервісів (SaaS, IaaS) та концепції BYOD (Bring Your Own Device). Традиційні методи захисту, що довіряють усьому трафіку всередині локальної мережі, стають неефективними проти інсайдерських загроз та складних цільових атак (APT).

Основна мета дослідження: Аналіз архітектурних змін, необхідних для реалізації моделі Zero Trust, та оцінка їх ефективності у протидії латеральному (горизонтальному) переміщенню зловмисників у мережі.

Результати аналізу: Впровадження архітектури Zero Trust (ZTA) змінює фундаментальний підхід до проектування комп'ютерних мереж. Якщо класична модель керується принципом «довіряй, але перевіряй», то ZTA базується на постулаті «ніколи не довіряй, завжди перевіряй», незалежно від того, де знаходиться користувач або пристрій - всередині чи зовні корпоративної мережі.Суть трансформації полягає у відмові від поняття «довіреної зони». У мережі Zero Trust кожен запит на доступ до ресурсу повинен проходити автентифікацію, авторизацію та шифрування в реальному часі. Це вимагає перебудови архітектури з використанням мікросегментації. Мікросегментація дозволяє розділити мережу на дрібні ізольовані зони аж до рівня окремих робочих навантажень. Це критично важливо для обмеження радіусу атаки: якщо зловмисник компрометує один сегмент, він не отримує автоматичного доступу до всієї інфраструктури. Ключовим елементом нової архітектури стає ідентифікація (Identity). У системах це означає інтеграцію потужних систем IAM (Identity and Access Management) з мережевим обладнанням. Рішення про надання доступу приймаються динамічно, базуючись не лише на паролі, а й на контексті: стан безпеки пристрою, геолокація, час доби та поведінкові аномалії.

Важливу роль відіграє технологія програмно-визначеного периметра (SDP — Software Defined Perimeter). Вона дозволяє приховувати мережеві ресурси від неавторизованих користувачів, роблячи інфраструктуру «невидимою» для сканування портів. З'єднання встановлюється лише після підтвердження довіри брокером доступу.

Однак перехід на Zero Trust супроводжується технічними викликами. Це потребує повної інвентаризації всіх активів мережі, що часто є складною задачею для великих підприємств із застарілим (legacy) обладнанням. Крім того, впровадження наскрізного шифрування та постійної перевірки політик створює додаткове навантаження на пропускну здатність мережі та вимагає оптимізації мережевих контролерів. Варто також зазначити, що архітектура Zero Trust тісно пов'язана з автоматизацією та оркестрацією безпеки (SOAR). Ручне керування політиками доступу в динамічному середовищі є неможливим, тому системи повинні автоматично реагувати на інциденти, ізолюючи підозрілі вузли без участі адміністратора.

Висновок: Таким чином, перехід до архітектури Zero Trust є еволюційною необхідністю для сучасних комп'ютерних систем та мереж. Ця модель дозволяє створити адаптивну систему захисту, яка відповідає вимогам децентралізованого IT-середовища. Попри складність реалізації, ZTA забезпечує значно вищий рівень стійкості мережі до зламів порівняно з периметральним захистом.

Перелік посилань:

1. NIST SP 800-207. Zero Trust Architecture. National Institute of Standards and Technology, 2020. - Офіційний стандарт, що визначає ключові принципи, логічні компоненти та моделі розгортання архітектури нульової довіри.
2. Kindervag, J. (2010). Build Security Into Your Network's DNA: The Zero Trust Network Architecture. Forrester Research. – Основоположна робота, в якій вперше було сформульовано концепцію та необхідність переходу до моделі Zero Trust.
3. Rose, S., et al. (2020). Zero Trust Architecture (ZTA) Guide. CISA. - Практичний посібник від Агентства кібербезпеки США щодо стратегій міграції від традиційних мереж до архітектури ZTA.
4. Buck, C., Olenberger, C., et al. (2021). Never Trust, Always Verify: A Survey of Zero Trust Networking Components and Solutions. IEEE Access. - Комплексний огляд технічних компонентів, протоколів та існуючих рішень на ринку для реалізації принципів нульової довіри.
5. Gilman, E., & Barth, D. (2017). Zero Trust Networks: Building Secure Systems in Untrusted Networks. O'Reilly Media. - Детальний технічний аналіз побудови захищених систем без використання традиційного периметра безпеки.

Балвак Андрій Анатолійович
аспірант 4 курсу, групи АКСМ-41
Державного університету
інформаційно-комунікаційних технологій
м. Київ
a.balvak@stud.duikt.edu.ua
Науковий керівник: Лащевська Наталія Олександрівна
кандидат технічних наук, доцент
завідувач кафедри Комп'ютерної інженерії
Державного університету
інформаційно-комунікаційних технологій
м. Київ

ПРОГРАМНА МЕТОДИКА ОПТИМІЗАЦІЇ РОЗМІЩЕННЯ ТОВАРІВ НА ОСНОВІ АНАЛІЗУ ЧАСОВИХ РЯДІВ ПОПИТУ

Постановка задачі. Ефективне функціонування логістичних центрів в умовах електронної комерції нерозривно пов'язане з вирішенням задачі оптимального призначення місць зберігання (Storage Location Assignment Problem, SLAP) [1]. Актуальність цього питання підкреслюється високою трудомісткістю складських операцій. Зокрема, дослідження свідчать, що на комплектування замовлень може припадати понад 55% від усіх операційних витрат складу [2]. Висока мінливість попиту у сфері інтернет-торгівлі демонструє низьку гнучкість традиційних статичних політик розміщення, зокрема ABC-аналізу [3]. Ключова проблема використання таких політик полягає у виникненні операційного дисбалансу, оскільки вони спрямовані на оптимізацію лише процесу комплектування, ігноруючи операційні витрати на розміщення товарів. Такий підхід не сприяє мінімізації сукупних витрат, що зумовлює необхідність пошуку більш комплексних та збалансованих рішень. Таким чином, виникає потреба у динамічних підходах, що базуються не на усереднених показниках, а на реальних патернах попиту, виявлених з історії транзакцій.

Мета дослідження. Метою даного дослідження є представлення програмної методики Часово-орієнтованого Призначення Місць Зберігання (Time-Oriented Assignment of Storage Locations, TOASL), у якій SLAP сформульовано як комплексну оптимізаційну задачу.

Результати дослідження. Запропонований підхід ґрунтується на інтелектуальному аналізі даних та кластеризації часових рядів попиту на окремі товарні позиції (Stock Keeping Unit, SKU) для ідентифікації прихованих залежностей та їх врахуванні при створенні збалансованої схеми зонування складу.

Фундаментальний принцип TOASL полягає у мінімізації комплексної цільової функції Z, що визначає сукупні витрати на переміщення товарів:

$$Z = \alpha \cdot \sum_{k=1}^{K} D_{pick}(O_k, \chi) + \beta \cdot \sum_{i=1}^{N} D_{put}(p_i, \chi),$$

де α та β – вагові коефіцієнти, що відображають пріоритетність процесів комплектування та розміщення для конкретного складу. Величиною $D_{pick}(O_k, \chi)$ виражається довжина маршруту при зборі замовлення O_k за умови розміщення χ, а $D_{put}(p_i, \chi)$ відповідає відстані транспортування одиниці p_i до місця її зберігання, закріпленого у плані χ.

Архітектура методики TOASL реалізується як програмний комплекс, що охоплює чотири етапи.

1. **Підготовка** даних включає агрегацію транзакцій, очищення, формування та нормалізацію часових рядів попиту для кожного SKU.
2. Етап **моделювання** передбачає застосування алгоритмів кластеризації для виявлення груп SKU зі схожою динамікою попиту й формування на їх основі логічних зон складу.
3. Етап **симуляції** полягає у створенні імітаційної моделі складу для тестування розробленої політики TOASL у порівнянні з класичними підходами, зокрема ABC-розміщенням, випадковим розміщенням та політикою найближчої вільної комірки. Експерименти виконуються при використанні різних стратегій маршрутизації, таких як S-подібний маршрут, маршрут із серединою проходу тощо.
4. На етапі **оцінювання** здійснюється статистичний аналіз результатів симуляції із застосуванням методів ANOVA та тест Тьюкі для кількісної оцінки ефективності політик за довжиною маршрутів.

Верифікація запропонованої методики здійснювалася у два етапи та охоплювала оцінювання модельного компонента й тестування комплексної ефективності TOASL. Для виконання досліджень було використано набір реальних транзакцій інтернет-ритейлера (E-commerce dataset), що містить понад 540 тисяч записів про історію замовлень, перелік придбаних товарів та час здійснення покупок. У рамках першого етапу ці дані застосовувалися для вибору оптимального алгоритму кластеризації. Після фільтрації та нормалізації транзакцій для 784 ключових SKU було сформовано часові ряди попиту. Порівняльний аналіз за критерієм силуету продемонстрував перевагу агломеративної ієрархічної кластеризації за методом Уорда. Саме цей підхід забезпечив формування 16 однорідних кластерів товарів, кількість яких було визначено як оптимальну за методом ліктя для досягнення балансу між компактністю груп та якістю розбиття.

На другому етапі було виконано імітаційне моделювання роботи складу для порівняння розробленої політики TOASL із традиційними підходами, а саме політиками випадкового та ABC-розміщення, а також найближчої вільної комірки. Результати симуляції для різних стратегій маршрутизації при збиранні замовлень, таких як S-подібна, із серединою проходу та найбільшого розриву тощо, показали стабільну перевагу запропонованої методики. Дані моделювання

засвідчили, що застосування розробленого підходу забезпечує суттєве скорочення шляху комплектувальника. Найбільш показові результати отримано для маршруту із серединою проходу та комбінованого маршруту. Зокрема, зафіксовано зменшення середньої дистанції на 29–52% та 32–44% відповідно у порівнянні з випадковим розміщенням. Стосовно політики ABC виграш становить 10–31% та 15–24% залежно від розміру партії замовлень. Статистична значущість отриманих даних підтверджена за допомогою дисперсійного аналізу ANOVA та пост-хок тесту Тьюкі.

Висновки та перспективи. Проведене дослідження підтвердило, що інтеграція інтелектуального аналізу часових рядів у процеси управління складом сприяє суттєвому підвищенню їх ефективності. Застосування методики TOASL, яка базується на збалансованій цільовій функції та кластерному зонуванні, гарантує статистично значуще скорочення маршрутів комплектування без надмірного ускладнення процесів розміщення. Це доводить перспективність використання динамічних, часово-орієнтованих підходів для оптимізації логістичних операцій в умовах електронної комерції. Подальші дослідження варто зосередити на адаптації методики для автоматизованих складських систем та її інтеграцію в системи управління складом.

Список використаних джерел

1. Boysen N. Warehousing in the e-commerce era: A survey [Електронний ресурс] / Nils Boysen, René de Koster, Felix Weidinger // European Journal of Operational Research. – 2019. – Т. 277, № 2. – С. 396–411. – Режим доступу: https://doi.org/10.1016/j.ejor.2018.08.023

2. Pang K.-W. Data mining-based algorithm for storage location assignment in a randomised warehouse [Електронний ресурс] / King-Wah Pang, Hau-Ling Chan // International Journal of Production Research. – 2016. – Т. 55, № 14. – С. 4035–4052. – Режим доступу: https://doi.org/10.1080/00207543.2016.1244615

3. Estimating optimal ABC zone sizes in manual warehouses [Електронний ресурс] / Allyson Silva [та ін.] // International Journal of Production Economics. – 2022. – С. 108579. – Режим доступу: https://doi.org/10.1016/j.ijpe.2022.108579

Якимчук Сергій Петрович
Студент 6 курсу, групи ТСДМ-63
Державний університет
інформаційно-комунікаційних технологій
(066)2083721
superbarthiro@gmail.com
Науковий керівник: Гринкевич Ганна Олександрівна,
д. т. н.,доцент, професор кафедри телекомунікаційних систем та мереж ННІТ,
Державного університету інформаційних, м. Київ

ОЦІНКА ЕФЕКТИВНОСТІ ВПРОВАДЖЕННЯ NGFW

Постановка задачі

У зв’язку з зростанням масштабів та складності кіберзагроз, традиційні фаєрволи вже не здатні вовною мірою забезпечити належний рівень інформаційної безпеки. Поява новітніх засобів захисту, зокрема NGFW стала відповіддю на потребу у більш глибокому контролі мережевого трафіку, виявлені атак та централізованому управлінні політиками безпеки.

NGFW поєднує в собі функції класичного фаєрволу з додатковими можливостями, аналіз трафіку на рівні додатків, вбудовані системи запобігання вторгнень (IPS), фільтрація веб-контенту, контроль SSL- трафіку. Тому постає задача проаналізувати, наскільки впровадження NGFW здатні підвищити рівень захищеності мережі та як це позначиться на загальній картині продуктивності та керованості IT-інфраструктури.

Мета дослідження

Ціль даного дослідження є визначити ефективність інтеграції NGFW у корпоративних мережах з урахуванням її впливу на ключові аспекти інформаційної безпеки.

Порівняння функціональних характеристик традиційних FW та NGFW

Оцінка змін у продуктивності мережі після впровадження NGFW

Результати дослідження

Після впровадження NGFW було здійснено заміну Cisco ASA 5525-x на віртуальне рішення FortiGate (8-ядерна конфігурація). Після міграції було проведено порівняння ефективності:

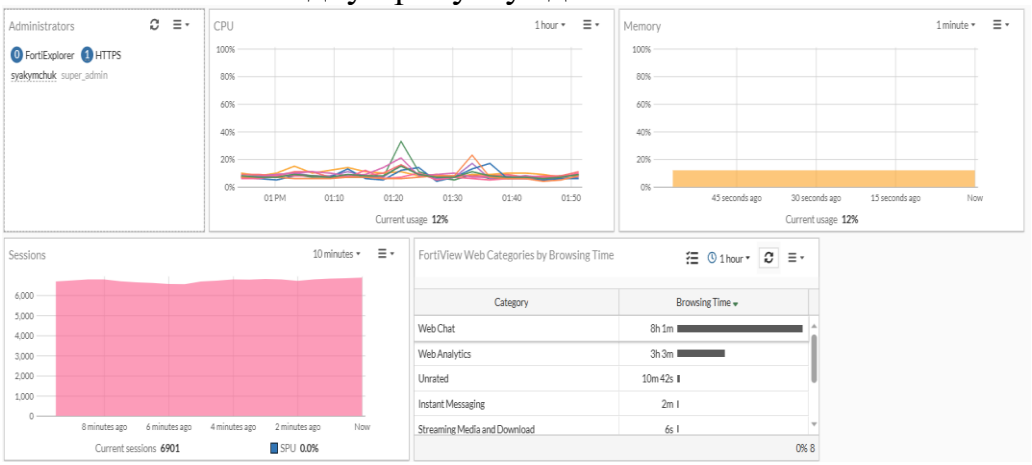
Гнучкість налаштування політик.

З переходом на NGFW, з’явилась можливість гнучко видавати права. Тепер правила можна було писати як на первну мережу так і на певну групу користувачів, які знаходяться в різних мережах, і навіть на окремого користувача. Це дало змогу більш точніше видавати права, без ризику видачі їх іншим користувачам.

Продуктивність системи.

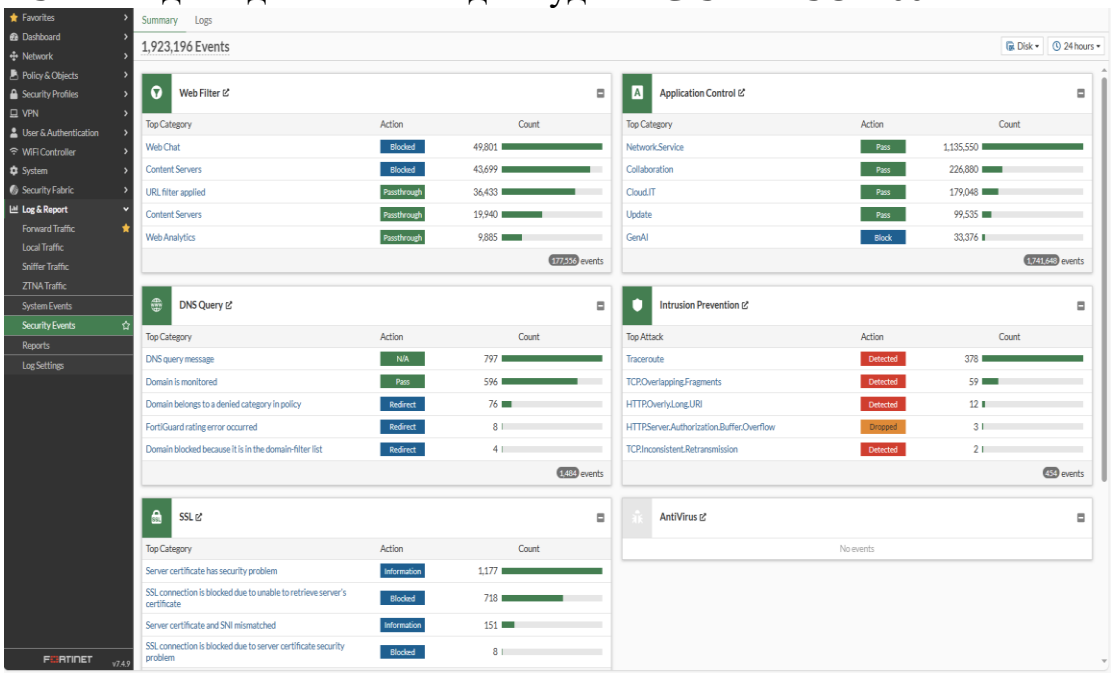
Не дивлячись на те, що FortiGate це VM, при налаштуванні на 8 ядрах, система забезпечила стабільну роботу без зниження пропускної здатності. І це при увімкнених IPS та SSL-інспекції затримка залишається в межах норми. ASA

5525 у складних сценаріях демонструвала вищу затримку і не могла забезпечити необхідну пропуску здатність.



Моніторинг та звітність.

FortiGate має вбудовані засоби для глибокої аналітики подій безпеки. Cisco ASA не відповідає звітністю для аудитів CIS або ISO27001



Масштабованість та оновлення.

Перехід на віртуальну платформу FortiGate значно спростив розширення ресурсів. У той час як Cisco ASA є апаратним рішенням з фіксованими характеристиками.

Висновки та перспективи

Міграція з Cisco ASA 5525-x на FortiGate VM дозволила суттєво підвищити гнучкість, ефективність та адаптивність мережевого захисту. Оновлена система демонструє вищий рівень безпеки та кращу керованість політиками. Це є важливими критеріями у сучасних умовах.

Список використаних джерел

1. Fortinet Document Library | Home. – Fortinet. URL: https://www.fortinet.com/resources

2. The 18 CIS Critical Security Controls. – Center for Internet Security. URL: https://www.cisecurity.org/controls
3. Support – Cisco Support, Documentation, and Downloads. – Cisco. URL: https://www.cisco.com/c/en/us/support/index.html

Войтюк Анастасія Сергіївна
Студентка 3 курсу, групи ІП-32
Національного технічного університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
м. Київ
nastyavoytiuk11@gmail.com
Науковий керівник: Поперешняк Світлана Володимирівна
кандидат фізико-математичних наук, доцент
доцент кафедри Інформатики та програмної інженерії
Національного технічного університет України
«Київський політехнічний інститут імені Ігоря Сікорського»

РОЗРОБКА АДАПТИВНОГО СУПРОТИВНИКА НА ОСНОВІ ГІБРИДНОГО FSM ТА ЕВРИСТИЧНОГО ПОШУКУ ДЛЯ КОЛЕКЦІЙНИХ КАРТКОВИХ ІГОР

Постановка задачі. Колекційні карткові ігри (ККГ) залишаються популярним жанром як у цифровому, так і у фізичному форматі, оскільки поєднують стратегічне мислення, планування та адаптивність [1]. Інтеграція штучного інтелекту (ШІ) дозволяє створювати суперників, які реагують на дії гравця, підвищуючи складність та динамічність ігрового процесу [2].

Актуальність дослідження полягає у розробці ефективних алгоритмів прийняття рішень для цифрових ККГ, що імітують поведінку людини. Застосування гібридного підходу, який поєднує машину скінченних станів (FSM) та евристичний пошук, забезпечує структуровану, але водночас адаптивну поведінку опонента, покращуючи ігровий досвід і демонструючи сучасні можливості програмної інженерії [1-3].

Основною задачею дослідження є створення адаптивного супротивника для колекційної карткової гри на основі гібридного підходу FSM та евристичного пошуку. Алгоритм ШІ повинен забезпечувати структурований перебіг гри за допомогою машин скінченних станів, водночас приймаючи оптимальні рішення всередині кожного стану завдяки евристичному аналізу можливих дій.

Мета дослідження. Метою розробки є покращення адаптивності та стратегічної поведінки ігрових супротивників у колекційних карткових іграх шляхом створення гібридного алгоритму на основі машини скінченних станів та евристичного пошуку, що забезпечує більш динамічний і логічно насичений ігровий процес.

Результати дослідження. У роботі застосовується гібридний підхід до побудови адаптивного супротивника в колекційній картковій грі, який поєднує машину скінченних станів та евристичні методи пошуку. Така комбінація забезпечує структуроване керування фазами ходу та водночас дозволяє гнучко оцінювати можливі дії залежно від ігрової ситуації [3].

Архітектура програмного забезпечення організована за принципами монолітної моделі з використанням патерну MVC [4]. Такий підхід забезпечує

чітке розмежування логіки, представлення та керування, що сприяє підвищенню продуктивності, зручності супроводу та масштабованості.

Алгоритм прийняття рішень супротивником ґрунтується на FSM, який визначає послідовність ігрових фаз в межах одного ходу. Усередині кожного стану застосовується евристична оцінка можливих дій та їх комбінацій, що дозволяє моделювати варіанти розвитку подій і вибирати найбільш доцільні рішення з погляду поточного стану гри [2-3].

Система керування супротивником координує роботу компонентів, що відповідають за формування доступних дій, оцінювання їхньої ефективності та виконання обраних рішень [2-4]. Оцінювання можливих сценаріїв здійснюється на основі стратегічних параметрів, таких як стан ресурсів, загрози від опонента та потенційний ефект від використання карт.

Послідовність обробки ігрових станів та вибору оптимальної дії візуалізовано на рисунку 1.

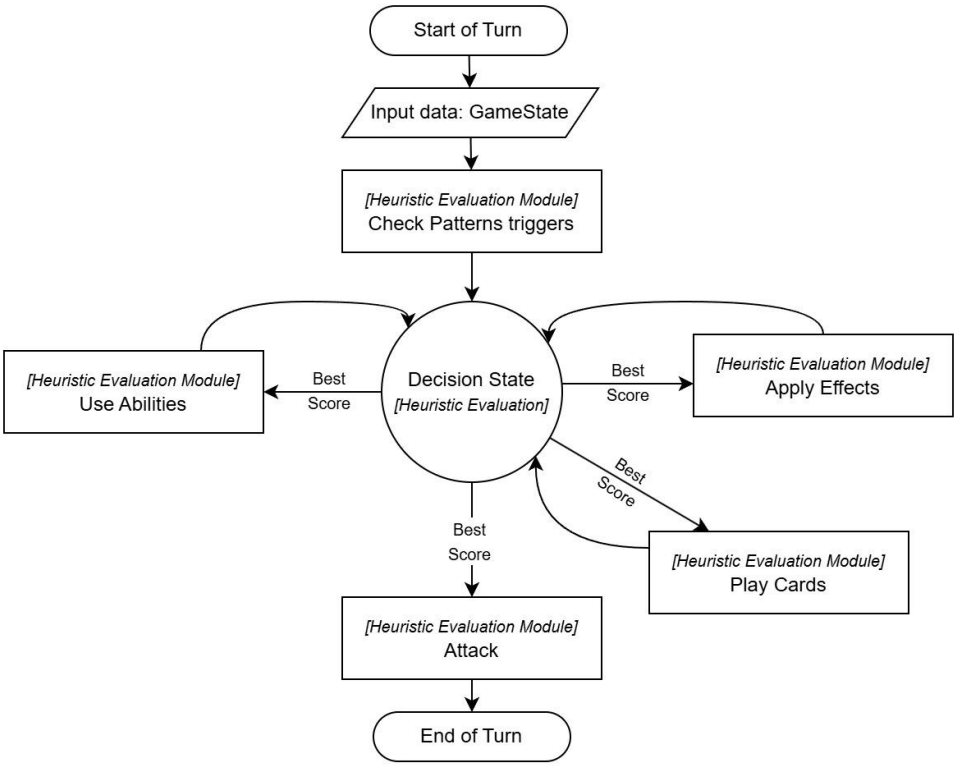


Рис. 1. Структурна схема гібридного алгоритму прийняття рішень

Висновки та перспективи. Розроблений гібридний алгоритм адаптивного супротивника для колекційної карткової гри демонструє ефективність поєднання машини скінченних станів та евристичного пошуку. FSM забезпечує структурований перебіг ходу, тоді як евристичні методи дозволяють супротивнику приймати оптимальні рішення з урахуванням поточного стану гри. Такий підхід успішно підвищує адаптивність, варіативність та стратегічну глибину поведінки ШІ, покращуючи ігровий досвід.

Обрана архітектура на базі Unity з використанням патерну MVC забезпечує високу гнучкість, простоту тестування та швидку інтеграцію нових функцій. Це

робить систему придатною для подальшого розширення, додавання нових типів карт, ігрових механік чи моделей поведінки супротивника.

Перспективи роботи включають розширення евристичної моделі за допомогою методів машинного навчання, підсилення гравця або створення декількох профілів поведінки супротивників. Також можливим є впровадження елементів стохастичності або багатокрокової стратегії для ще більшої наближеності до реального гравця. Отримані результати демонструють потенціал гібридних моделей ШІ для створення динамічних ігрових систем нового покоління.

Список використаних джерел

1. Turkay, Selen; Adinolf, Sonam; Tirthaliv, Devayani (2012). Collectible card games as learning tools. Procedia. 46: 3701–3705. DOI: 10.1016/j.sbspro.2012.06.130.

2. Georgios N. Yannakakis. Game AI Revisited. Proceedings of the ACM International Conference on Computing Frontiers (CF’12). 2012. P. 1–10. DOI: 10.1145/1234567.

3. Jagdale D. Finite State Machine in Game Development. International Journal of Advanced Research in Science, Communication and Technology. 2021. С. 384–390. URL: https://doi.org/10.48175/ijarsct-2062 (дата звернення: 10.11.2025).

4. Hod H. MVC in Game Development. Game Developer | Game Industry News, Deep Dives, and Developer Blogs. URL: https://www.gamedeveloper.com/programming/mvc-in-game-development (дата звернення: 10.11.2025).

Губанов В’ячеслав Володимирович
студент 2 курсу, групи ПЗ-24-1дм
Дніпровського державного технічного університету
м. Кам’янське
(093)-525-90-79
program_mer@ukr.net
Науковий керівник: Бабенко Михайло Володимирович
кандидат технічних наук
доцент кафедри «Програмне забезпечення систем»
Дніпровського державного технічного університету
м. Кам’янське

РОЗРОБКА НЕЧІТКОЇ МОДЕЛІ ВИБОРУ ОЧИСНИХ СПОРУД МЕТАЛУРГІЙНОГО ВИРОБНИЦТВА

Постановка задачі. Сучасний розвиток промисловості, зокрема металургійного комплексу, супроводжується зростанням техногенного навантаження на навколишнє середовище. Металургійні підприємства є одними з найбільших забруднювачів довкілля через формування великої кількості стічних вод, що містять сполуки заліза, марганцю, нікелю, хрому, нафтопродуктів та інші токсичні речовини. Забруднені стоки металургійного виробництва становлять серйозну екологічну проблему, оскільки їх потрапляння у природні водойми без належного очищення призводить до деградації екосистем, погіршення якості водних ресурсів, а також створює загрозу для здоров’я людини.

Одним із найперспективніших методів вирішення таких задач є нечітке моделювання, що дозволяє формалізувати процес прийняття рішень в умовах невизначеності та якісних оцінок, що робить його зручними для опису реальних виробничих процесів, де часто неможливо отримати точні кількісні дані.

Особливої уваги заслуговує застосування нечіткої логіки для багатокритеріального оцінювання різних типів очисних споруд — механічних, фізико-хімічних, біологічних, комбінованих. Кожен із типів має свої переваги та недоліки, які можуть по-різному проявлятися залежно від складу стічних вод, обсягу виробництва, вартості обладнання, вимог до якості очищення та інших параметрів. Тому вибір оптимального варіанту вимагає всебічного аналізу, що й може бути забезпечено за допомогою нечітких моделей.

Мета дослідження. Метою даного дослідження є процес вибору очисних споруд металургійного виробництва за допомогою методів нечіткого моделювання та їх реалізація сучасними засобами програмування.

Результати дослідження. Вибір оптимальної системи очищення стічних вод для металургійного підприємства є складною інженерною задачею. Він залежить від великої кількості факторів — складу стоків, обсягів виробництва, технологічних особливостей, вартості обладнання, експлуатаційних витрат, екологічних норм та надійності роботи системи. Більшість цих факторів є

нечітко визначеними, оскільки їх точні значення важко встановити на практиці або вони можуть змінюватися в часі. Саме тому традиційні методи математичного моделювання, засновані на жорстких числових залежностях, не завжди дають адекватні результати.

Розроблена система вибору очисних споруд заснована саме на таких методах нечіткої логіки. Вони дають змогу оцінювати альтернативи на основі як кількісних, так і якісних показників, використовуючи правила типу «якщо – то», побудовані на експертних знаннях. Після обробки даних нечітка модель формує кількісну оцінку ефективності кожного варіанту очисної споруди. Таким чином, нечітке моделювання дозволяє отримати узагальнену інтегральну оцінку ефективності очисних технологій, навіть за умов, коли точних числових даних недостатньо.

В якості вхідних даних використовуються концентрації забруднюва-чів, витрата стічних вод, ефективність очищення, енергоспоживання, собівартість тощо. Для кожного параметра задаються функції належності, що описують ступінь приналежності значення певному терму.

Для реалізації моделі застосовано програмні засоби, які підтримують обробку нечітких даних. Це мова програмування Python з бібліотеками scikit-fuzzy, Pandas, NumPy, Matplotlib. Результатом є програмний продукт, що дозволяє на основі введених параметрів визначити оптимальний тип очисних споруд для конкретного типу металургійного стоку.

Оскільки частина параметрів має якісний або описовий характер (наприклад, «складність обслуговування» або «ступінь автоматизації»), було використано метод експертних оцінок. Група фахівців-екологів і технологів надала вагові коефіцієнти для окремих показників. Це дозволило підвищити достовірність результатів моделювання та зробити модель ближчою до реальних умов виробництва.

Висновки та перспективи. З огляду на сучасні вимоги до екологічної безпеки та сталого розвитку, розробка інтелектуальних систем для підтримки рішень у сфері очищення промислових стічних вод має не лише наукове, але й практичне значення. Такі системи дозволяють зменшити негативний вплив виробництва на навколишнє середовище, підвищити ефективність технологічних процесів, оптимізувати витрати на експлуатацію очисних споруд та сприяти впровадженню екологічно безпечних технологій у металургійній галузі.

Розроблена система є ефективним, адаптивним і гнучким інструмен-том, здатним підтримувати процес прийняття рішень у складних умовах невизначеності. Вона може бути інтегрована в інформаційні системи управління підприємством, використана для навчальних цілей або як прототип для створення більш масштабних систем підтримки рішень у промисловості. Також розроблена система може бути застосована не лише у металургійній промисловості, але й у суміжних галузях – машинобудуванні, енергетиці, хімічній та нафтопереробній промисловості, де існує потреба у виборі технологій очищення складних промислових стічних вод. Завдяки гнучкості нечіткої логіки,

адаптація системи до нової галузі потребує лише зміни набору параметрів і критеріїв оцінки, що є значно швидшим, ніж розроблення нової моделі з нуля.

Анотація

Представлене дослідження направлене на вирішення комплексу завдань, спрямованих на вдосконалення процесу прийняття рішень щодо екологічної модернізації металургійних підприємств у сфері очисних споруд.

Проведений аналіз сучасних рішень, технологій та інструментів показав, що при проєктування очисних споруд доцільно використання нечіткого моделювання, що дозволяє формалізувати процес прийняття рішень в умовах невизначеності та якісних оцінок, що робить його зручними для опису реальних виробничих процесів.

Під час реалізації дослідження було розроблено нечітку модель вибору очисних споруд, у якій визначено ключові критерії оцінювання: ефективність очищення, енергоспоживання, надійність, екологічна безпечність та економічна доцільність. Застосування інструментів мови програмування високого рівня Python з бібліотеками Scikit-fuzzy, Pandas, NumPy, Matplotlib дало змогу провести розрахунки, сформувати базу правил нечітких висновків та здійснити візуалізацію отриманих результатів у вигляді графіків і поверхонь належності.

Тестування моделі показало, що застосування нечіткого підходу дозволяє досягти високої точності прогнозування результатів навіть за відсутності точних початкових даних. Розроблена система забезпечує адаптивність до зміни умов експлуатації та може бути використана як допоміжний інструмент у процесі техніко-економічного обґрунтування проєктів модернізації очисних споруд.

Данилов Леонід Володимирович
студент 4 курсу, групи ІПЗ-22121
Національного транспортного університету
м. Київ
(095)-229-80-52
danylov.lv@gmail.com
Науковий керівник: Поперешняк Світлана Володимірівна
кандидат фізико-математичних наук
доцент кафедри інформаційних технологій
Навчально-наукового інституту управління, технологій та правових наук
Національного транспортного університету
м. Київ

МІКРОСЕРВІСНА АРХІТЕКТУРА ДЛЯ МАСШТАБОВАНИХ ВЕБ-ДОДАТКІВ: ПЕРЕВАГИ ТА ВИКЛИКИ

Вступна частина. Сучасні веб-додатки постійно зростають за складністю та навантаженням, що ставить високі вимоги до масштабованості, гнучкості та швидкості розробки. Традиційна монолітна архітектура, коли всі компоненти системи тісно пов’язані, часто стає обмеженням для швидкого впровадження змін і підтримки великої кількості користувачів [1].

Мікросервісна архітектура дозволяє розбивати систему на автономні сервіси, кожен з яких відповідає за конкретну функціональність, та може розгортатися, масштабуватися і оновлюватися незалежно від інших [2, 3]. Такий підхід підвищує відмовостійкість системи, спрощує інтеграцію нових функцій і дозволяє ефективніше використовувати ресурси [4].

Постановка задачі. Розвиток сучасних веб-додатків супроводжується постійним зростанням складності та навантаження, що створює потребу в ефективних архітектурних рішеннях. Традиційна монолітна архітектура часто обмежує масштабування системи, швидкість впровадження змін та відмовостійкість. Потрібно дослідити альтернативні підходи, які дозволяють підвищити гнучкість, ефективність розробки та надійність веб-додатків. У цьому контексті актуальним є застосування мікросервісної архітектури, яка передбачає поділ системи на автономні сервіси з незалежним розгортанням та масштабуванням.

Мета дослідження. Визначення переваг та проблем застосування мікросервісної архітектури у масштабованих веб-додатках, зокрема щодо взаємодії сервісів, надійності роботи системи та збереження коректності даних, а також оцінка ефективності розподілу функціональності між сервісами, можливостей їх незалежного розгортання та масштабування, а також формування рекомендацій щодо підвищення гнучкості та стабільності сучасних веб-додатків.

Результати дослідження. У результаті проведеного аналізу було встановлено, що мікросервісна архітектура є ефективним підходом для

створення масштабованих веб-додатків [1, 2]. Розділення системи на окремі автономні сервіси дозволяє підвищити гнучкість розробки, спростити впровадження нових функцій та оновлення компонентів без необхідності зупинки всієї системи [3]. Крім того, поділ на сервіси забезпечує можливість паралельної роботи різних команд розробників, що сприяє прискоренню процесу створення програмного продукту.

Дослідження також показало, що застосування мікросервісної архітектури сприяє більш ефективному використанню ресурсів системи, оскільки окремі сервіси можна масштабувати залежно від навантаження [1, 4]. Це дозволяє оптимізувати продуктивність системи, знижувати витрати на інфраструктуру та підтримувати стабільну роботу навіть при зростанні кількості користувачів.

Разом із цим було виявлено основні проблеми та виклики, з якими стикаються розробники при впровадженні мікросервісів. До них належать складність організації взаємодії між сервісами, необхідність забезпечення правильності та узгодженості даних під час обміну, а також потреба у належному контролі та моніторингу роботи системи. Практичний досвід показує, що ці проблеми можна ефективно мінімізувати за допомогою чіткого планування архітектури, використання стандартних протоколів обміну даними, впровадження автоматизованих засобів моніторингу та логування, а також застосування відповідних інструментів для управління версіями та розгортанням сервісів.

Висновки та перспективи. Дослідження показало, що мікросервісна архітектура дозволяє підвищити гнучкість і масштабованість веб-додатків [2, 3]. Розділення системи на автономні сервіси забезпечує можливість їх незалежного розгортання та оновлення без впливу на роботу інших компонентів [1]. Це особливо важливо для великих проектів, де швидке впровадження нових функцій та підтримка стабільності системи є критичною.

На відміну від монолітної архітектури, де всі компоненти системи тісно пов’язані і будь-яке оновлення або помилка можуть порушити роботу всієї системи, мікросервіси дозволяють паралельно розвивати окремі частини додатка та ефективніше використовувати ресурси [4]. Такий підхід також спрощує організацію роботи команд розробників, дозволяючи декільком групам одночасно працювати над різними сервісами без конфліктів.

Водночас впровадження мікросервісної архітектури потребує належної організації взаємодії між сервісами, контролю за правильністю даних, моніторингу та забезпечення надійності роботи системи. Перспективи подальших досліджень пов’язані з оптимізацією взаємодії сервісів, автоматизацією процесів розгортання та оновлення компонентів, а також підвищенням загальної стабільності системи. Вказані відмінності між монолітом і мікросервісами можна подати у вигляді схематичного зображення (див. рис. 1).

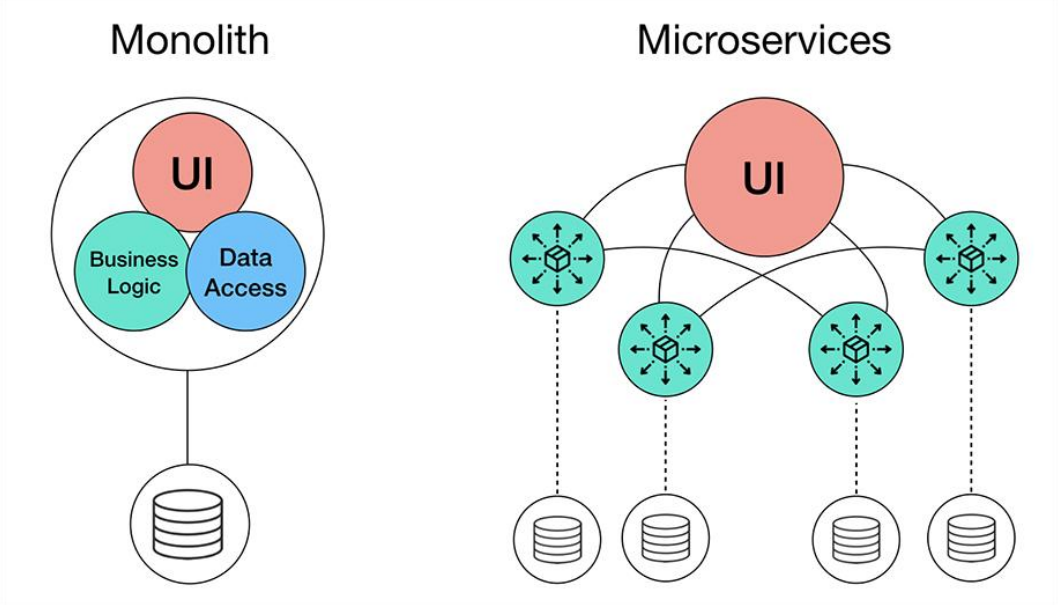


Рис. 1. Схематичне порівняння монолітної та мікросервісної архітектури веб-додатків

Застосування мікросервісної архітектури забезпечує створення гнучких і масштабованих веб-додатків, проте успішна реалізація вимагає планування, ефективного моніторингу та контролю взаємодії сервісів для підтримки стабільності та надійності системи.

Список використаних джерел

1 Understanding Microservices Architecture: Benefits and Challenges Explained / Blogs / Perficient [Електронний ресурс]. – Режим доступу: https://blogs.perficient.com/2024/08/06/understanding-microservices-architecture-benefits-and-challenges-explained/.

2 МІКРОСЕРВІСНА АРХІТЕКТУРА: ПЕРЕВАГИ ТА НЕДОЛІКИ ЇЇ ПРАКТИЧНОГО ЗАСТОСУВАННЯ [Електронний ресурс] / Володимир КИСЕЛЕВИЧ [та ін.] // Information Technology: Computer Science, Software Engineering and Cyber Security. – 2024. – № 2. – С. 50–59. – Режим доступу: https://doi.org/10.32782/it/2024-2-7.

3 Microservices Advantages and Disadvantages | IBM [Електронний ресурс] // IBM. – Режим доступу: https://www.ibm.com/think/insights/microservices-advantages-disadvantages.

4 What are the Advantages and Disadvantages of Microservices Architecture? - GeeksforGeeks [Електронний ресурс] // GeeksforGeeks. – Режим доступу: https://www.geeksforgeeks.org/system-design/what-are-the-advantages-and-disadvantages-of-microservices-architecture/.

Овдєй Олексій Сергійович
студент 6 курсу, групи КСДМ-61
Державного університету
інформаційно-комунікаційних технологій
м. Київ
Alexovdey2003@gmail.com
Боднар Андрій Сергійович
студент 6 курсу, групи КСДМ-61
Державного університету
інформаційно-комунікаційних технологій
м. Київ
bodnarandrej118@gmail.com

НЕЙРОМЕРЕЖЕВА СИСТЕМА ДЛЯ ІДЕНТИФІКАЦІЇ АНОМАЛЬНИХ ПАТТЕРНІВ МЕРЕЖЕВОГО ТРАФІКУ

Постановка задачі. Сучасні корпоративні мережі стикаються з експоненційним зростанням кількості кіберзагроз, які постійно еволюціонують. Традиційні системи виявлення вторгнень, що базуються на сигнатурному аналізі, демонструють критичну вразливість до поліморфних атак та загроз «нульового дня», оскільки здатні розпізнавати лише відомі шаблони. Окрім глобальних аномалій, які легко детектуються пороговими методами, значну небезпеку становлять локальні аномалії, приховані в динаміці часових рядів трафіку. Це зумовлює необхідність переходу до інтелектуальних систем аналізу, здатних виявляти складні залежності та приховані патерни поведінки зловмисників у реальному часі за допомогою методів глибокого навчання.

Мета дослідження. Метою дослідження є підвищення рівня захищеності інформаційних систем шляхом розробки та експериментальної перевірки гібридної нейромережевої моделі C-LSTM, яка поєднує механізми вилучення просторових ознак та аналізу часових залежностей для високоточної класифікації мережевого трафіку.

Результати дослідження. В ході дослідження було обґрунтовано вибір гібридної архітектури C-LSTM. Модель складається з послідовності одновимірних згорткових шарів, які відповідають за автоматичну екстракцію високорівневих просторових ознак із «сирого» трафіку, та рекурентних шарів довгої короткочасної пам’яті, що аналізують темпоральну динаміку та зберігають контекст подій. Для навчання та тестування системи використано еталонний набір даних Yahoo Webscope S5, що містить реальний трафік із розміченими аномаліями[1]. Проблему дисбалансу класів було вирішено застосуванням методу «ковзного вікна», що дозволило структурувати дані для рекурентної мережі. Експериментальним шляхом встановлено, що заміна функції активації на ReLU та збільшення кількості епох навчання до 700 дозволили досягти точності класифікації на рівні 96% та показника F1-score 73,5%. Порівняльний аналіз

показав, що запропонована модель перевершує класичні алгоритми SVM, Random Forest та MLP за ключовими метриками ефективності[2].

Висновки та перспективи. Розроблена система довела свою спроможність ефективно виявляти як глобальні, так і приховані локальні аномалії з мінімальною кількістю помилкових спрацювань. Використання гібридної архітектури дозволяє автоматизувати процес моніторингу безпеки без необхідності ручного створення правил. Перспективи подальших досліджень полягають в інтеграції механізмів пояснюваного штучного інтелекту для інтерпретації рішень нейромережі та адаптації моделі для роботи в високошвидкісних мережах у режимі реального часу.

Список використаних джерел:

1. Y. Wang et al., "Digital Twin for Network Performance Monitoring: A Comprehensive Review," IEEE Internet of Things Journal, vol. 10, no. 2, pp. 1023-1040, 2023. https://doi.org/10.1109/JIOT.2023.3234567.

2. S. Bhattarai et al., "Throughput Analysis of IEEE 802.11ax Networks with Uplink Multi-User MIMO," IEEE Transactions on Vehicular Technology, vol. 68, no. 10, pp. 10003-10017, 2019. https://doi.org/10.1109/TVT.2019.2936279.

Слєпчук Ростислав Віталійович
студент 6 курсу, групи КСДМ-61
Державного університету
інформаційно-комунікаційних технологій
м. Київ
fewrules10@gmail.com
Філик Павло Васильович
студент 6 курсу, групи КСДМ-61
Державного університету
інформаційно-комунікаційних технологій
м. Київ
pavelfilyk28@gmail.com

ОНТОЛОГІЧНИЙ ПІДХІД ДО СТВОРЕННЯ СИСТЕМИ КЕРУВАННЯ Й КОНТРОЛЮ МЕРЕЖЕВИМИ ПРОЦЕСАМИ

Постановка задачі. Сучасні комп'ютерні мережі характеризуються високим рівнем гетерогенності та постійним зростанням обсягів трафіку. Традиційні засоби моніторингу, що оперують лише числовими метриками, стають недостатньо ефективними, оскільки генерують велику кількість розрізнених сповіщень без вказівки на першопричину збою. Це ускладнює роботу адміністраторів, збільшує час реакції на інциденти та призводить до простою сервісів. Тому виникає нагальна необхідність у переході до інтелектуальних систем керування, що базуються на знаннях та здатні розуміти семантику подій для автоматизованої діагностики.

Мета дослідження. Метою дослідження є підвищення ефективності та надійності функціонування мережевої інфраструктури шляхом розробки системи керування й контролю на основі онтологічної моделі, яка забезпечує автоматизовану кореляцію подій та виявлення кореневих причин аномалій.

Результати дослідження. Під час дослідження було запропоновано модель системи, що включає формалізацію лексикону та граматики мови опису. Як інструмент реалізації обрано мову веб-онтологій OWL DL[1], що дозволило досягти балансу між виразністю опису та обчислювальною ефективністю алгоритмів логічного виведення. Запропоновано ієрархічну структуру класів, де базовий концепт NetEntity уніфікує опис апаратних та програмних компонентів. Для моделювання навантаження введено класи TrafficEntity та метрики використання ресурсів. Ключовим результатом є формалізація динаміки мережі через концепти «Подія» та «Аномалія». Встановлені онтологічні зв’язки, що дозволяють модулю логічного виведення автоматично групувати розрізнені симптоми навколо єдиної причини. Архітектурно система реалізована на базі парадигми активних мереж, що включає централізований Reasoner та розподілені програмовані агенти з динамічно налаштованими сенсорами[2].

Висновки та перспективи. Запропонована система може підвищіти ефективність у задачах фільтрації інцидентів, знизивши рівень «інформаційного

шуму» на 60–70% порівняно з пороговими методами. Використання механізму семантичної кореляції може дозволити скоротити середній час ідентифікації причини збою (MTTI) на 35–40%. Перспективи подальших досліджень полягають у розширенні онтології для підтримки хмарних середовищ (SDN) та впровадженні алгоритмів машинного навчання для прогнозування аномалій на основі накопиченої бази знань.

Список використаних джерел:

1. Guarino N. "Formal Ontology and Information Systems." Proceedings of FOIS’98, Trento, Italy, 6-8 June 1998. IOS Press, Amsterdam, 1998. pp. 3-15.

2. Horrocks I. et al. "SWRL: A Semantic Web Rule Language Combining OWL and RuleML." W3C Member Submission 21 May 2004. URL: https://www.w3.org/Submission/SWRL/.

Казимір Георгій Сергійович
студент 2 курсу групи МКІ-241
Національного університету «Чернігівська Політехніка»
м.Чернігів
0997774339
kaizmir.gosha@gmail.com
Науковий керівник: Зайцев Сергій Васильович
доктор технічних наук
професор Кафедри інформаційних та комп'ютерних систем
Національного університету «Чернігівська Політехніка»
м.Чернігів

ІНТЕГРАЦІЯ ВІДКРИТИХ КАРТОГРАФІЧНИХ СЕРВІСІВ У МОБІЛЬНІ ЗАСТОСУНКИ

Анотація. Проаналізовано підходи до інтеграції відкритих картографічних сервісів у мобільні застосунки. Визначено переваги використання відкритих джерел геопросторових даних порівняно з комерційними платформами. Визначено формати геопросторових даних та їх використання в мобільних застосунках.

У сучасних умовах інформаційних технологій, інтеграція картографічних сервісів у мобільні додатки є одним із важливих напрямів розвитку прикладного програмного забезпечення. Відкриті картографічні сервіси, такі як OpenStreetMap, Mapbox, Google Maps API, Leaflet, надають розробникам можливість створювати інтерактивні геоінформаційні інтерфейси без необхідності формування власних картографічних баз. Це сприяє зниженню трудовитрат на розробку, підвищує доступність просторових даних та розширює можливості застосунків у різних галузях.

Картографічні сервіси API забезпечують широкий спектр інструментів для інтеграції та обробки просторових даних у вебсервісах і мобільних застосунках. До ключових функціональних можливостей таких інтерфейсів належать [1]:

– відображення картографічних даних. Картографічні сервіси дозволяють здійснювати інтеграцію інтерактивних карт у програмні системи різних типів, забезпечуючи масштабування, навігацію та динамічне оновлення геопросторової інформації;

– геокодування та зворотне геокодування. Картографічні API підтримують перетворення текстових адрес у географічні координати та виконання зворотної операції, що забезпечує прив'язку просторових даних до конкретних об'єктів місцевості;

– пошук об'єктів інфраструктури. Інструменти дають змогу здійснювати пошук і отримання інформації про заклади, об'єкти інфраструктури, точки інтересу та інші географічні сутності на основі даних картографічних сервісів;

– прокладання маршрутів. API надають можливість розрахунку оптимальних маршрутів для різних видів переміщення, включаючи пішохідні маршрути, автомобільні поїздки та переміщення громадським транспортом. Маршрути формуються з урахуванням просторових обмежень та дорожніх умов;

– обробка та аналіз просторових даних. Програмні інтерфейси забезпечують вимірювання відстаней, площ, меж територій, а також підтримують реалізацію задач зонування, класифікації та інших видів геоаналітичної обробки;

– візуалізація тематичних шарів. API дозволяють накладати додаткові інформаційні шари, такі як метеорологічні дані, дорожня ситуація, екологічні показники, тощо.

Картографічні сервіси API пропонують різні моделі доступу, які умовно поділяються на безкоштовні, умовно безкоштовні та платні.

Безкоштовні картографічні API надають базові можливості, серед яких відображення карт. Обсяг запитів у таких сервісах зазвичай обмежений, тому безкоштовні API підходять для навчальних проєктів та додатків із невеликим навантаженням. Рівень деталізації карт також може бути нижчим порівняно з розширеними комерційними сервісами [2].

Умовно безкоштовні API забезпечують ширші можливості, наприклад роботу з геокодуванням, прокладанням маршрутів, пошуком об’єктів та підключенням додаткових шарів даних. Умовно безкоштовні API мають безкоштовні ліміти, однак після перевищення застосовуються тарифи оплати. Така модель підходить для невеликих комерційних застосунків та проєктів, у яких необхідна розширена функціональність [2].

Платні картографічні API призначені для систем, що працюють із великими обсягами даних або потребують спеціалізованого функціоналу. Ці сервіси підтримують стабільну роботу при високому навантаженні, надають доступ до супутникових знімків, детальних карт, аналітичних інструментів і технічної підтримки. Така модель використовується у галузях, де важлива точність та надійність роботи [2].

Беручи до уваги безкоштовні картографічні API, спільною характеристикою таких сервісів є можливість відображення карт, операції визначення координат за заданими параметрами, базове геокодування. Окрім цього, безкоштовні API підтримують накладання маркерів і найпростіших інформаційних шарів [1][3].

Важливим в інтеграції картографічних сервісів у мобільні та вебзастосунки є забезпечення сумісності форматів геопросторових даних. Використання відкритих стандартів, таких як GeoJSON, KML, WMS та WMTS, дозволяє уніфікувати процеси передачі, обробки та зберігання інформації незалежно від конкретної платформи або сервісу [4].

Застосування стандартів підвищує сумісність та взаємодію різних систем, дозволяє використовувати дані з різних джерел без необхідності конвертації в пропрієтарні формати та зменшує ризик втрати точності даних.

В таблиці 1 приведено перелік безкоштовних картографічних API та підтримуваних форматів геопросторових даних [1][3].

Таблиця 1 - Підтримувані формати геопросторових даних популярних безкоштовних картографічних API

Платформа	Підтримувані формати
OpenStreetMap	GeoJSON, XML, OSM XML
Leaflet	GeoJSON, KML, TopoJSON
Mapbox	GeoJSON, KML, Vector Tiles
OpenLayers	GeoJSON, KML, WMS, WMTS, GML

Серед всіх розглянутих відкритих картографічних платформ спільним є формат GeoJSON [1][3].

В лістингу 1 приведено приклад полігону в форматі GeoJson а на рисунку 1 відображення даного полігону на Mapbox.

Лістинг 1 - Приклад полігону в форматі GeoJson

```
{
  "type": "FeatureCollection",
  "features": [
    {
      "type": "Feature",
      "geometry": {
        "type": "Polygon",
        "coordinates": [
          [
            [
              31.17,
              51.613
            ],
            [
              31.37,
              51.613
            ],
            [
              31.37,
              51.46
            ],
            [
              31.17,
              51.46
            ],
            [
```

```
                31.17,
                51.613
              ]
            ]
          ]
        },
        "properties": {
          "name": "Чернігів"
        }
      }
    ]
  }
```

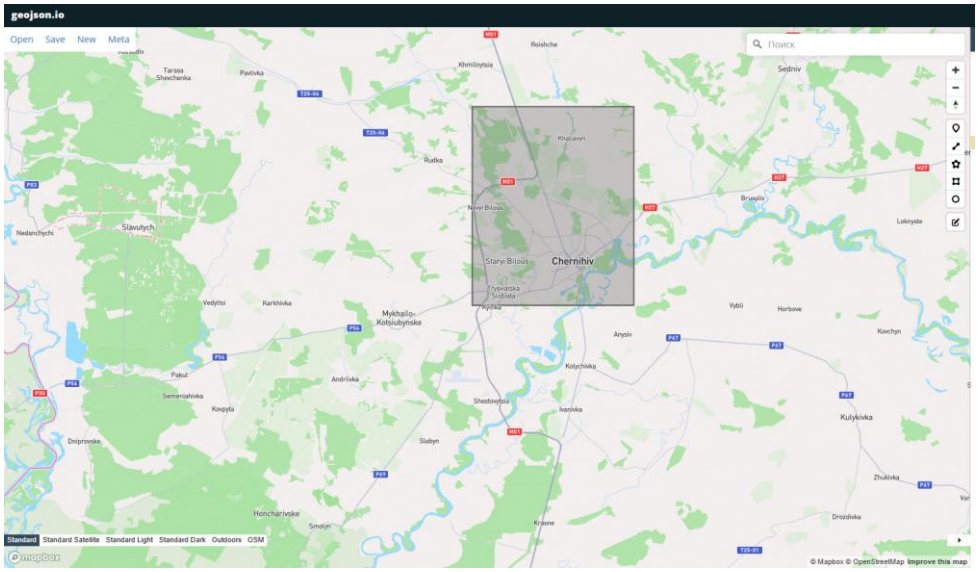


Рисунок 1 – Відображення полігону на Mapbox

GeoJSON забезпечує легкий і гнучкий формат для опису геометричних об’єктів і атрибутів, що робить його оптимальним для обміну даними між клієнтськими додатками та серверами. Формати KML і WMS/WMTS, у свою чергу, підтримують роботу з шарами, масштабуванням і тематичним відображенням карт [4].

Висновки. Розглянуті платформи демонструють різний рівень доступності та функціональності, однак навіть безкоштовні рішення забезпечують базові можливості відображення карт і роботи з координатами та відображенням полігонів. Особливу увагу приділено формату GeoJSON, який сумісний з розглянутими картографічними API.

Список літератури

1. Картографічні API: що це таке та які є популярні сервіси [Електронний ресурс] // Visicom API. – Режим доступу: https://api.visicom.ua/uk/posts/bestapi1 (дата звернення: 10.11.2025)

2. Кузніченко С. Картографічні WEB-сервіси [Електронний ресурс] : Конспект лекцій / С. Кузніченко, І. Бучинська. – Одеса : Од. держ. екол. ун-т,

2022. – 114 с. – Режим доступу: http://eprints.library.odeku.edu.ua/id/eprint/11546/1/Kartograf_web_services_Lectures_2022.pdf (дата звернення: 10.11.2025).

3. Порівняння веб-картографії: 5 платформ, які варті уваги [Електронний ресурс] // portalgis. – Режим доступу: https://portalgis.pro/geoinformaczijni-systemy/5-najkrashhyh-veb-kartografichnyh-platform-bytva-veb-gis/ (дата звернення: 10.11.2025).

4. GeoJSON [Електронний ресурс] // File Format Docs. – Режим доступу: https://docs.fileformat.com/uk/gis/geojson/ (дата звернення: 10.11.2025).

Токар Микита Денисович
студент 6 курсу, групи КСДМ-61
Державного університету
інформаційно-комунікаційних технологій
м. Київ
reivenfoxerror@gmail.com
Слюсар Владислав Сергійович
студент 6 курсу, групи КСДМ-61
Державного університету
інформаційно-комунікаційних технологій
м. Київ
slyusar33@gmail.com

РОЗРОБКА КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ КОРПОРАТИВНОЇ IT-ІНФРАСТРУКТУРИ НА БАЗІ ACTIVE DIRECTORY

Постановка задачі. У сучасних умовах цифрової трансформації бізнесу забезпечення кіберстійкості IT-інфраструктури трансформувалося з технічної необхідності у стратегічний пріоритет. Традиційні однорангові мережі з децентралізованим управлінням стають вразливими до атак типу «людина посередині», ARP-спуфінгу та програм-вимагачів. Відсутність єдиної політики ідентифікації та застаріле обладнання унеможливлюють ефективний моніторинг інцидентів та оперативне реагування на загрози. Це зумовлює необхідність побудови ієрархічної захищеної мережі з використанням централізованих служб каталогів та надійних протоколів динамічної маршрутизації.

Мета дослідження. Метою дослідження є можливість підвищення рівня захищеності та керованості корпоративного інформаційного середовища шляхом розробки та практичної імплементації відмовостійкої архітектури мережі на базі служби каталогів Microsoft Active Directory.

Результати дослідження. У ході дослідження було запропоновано трирівневу архітектуру мережі. Для забезпечення швидкої конвергенції мережі та підтримки реплікації даних між підмережами пропонується впровадження протоколу OSPF, що дозволяє динамічно оновлювати маршрути. Ключовим елементом системи захисту є служба Active Directory з двома контролерами домену (Primary та Backup)[1], що гарантує відмовостійкість сервісів аутентифікації. Також пропонується сегментація мережі на окремі VLAN: Management, Server, User LANs, а також впровадження групових політик дозволиляє автоматизувати налаштування безпеки кінцевих точок, а налаштування DNSSEC та відключення застарілих протоколів мінімізувало ризики атак на інфраструктуру[2].

Висновки та перспективи. Запропонована система доводить свою ефективність, забезпечуючи централізовану ідентифікацію користувачів, логічне розмежування доступу та захист периметра мережі. Використання резервного

контролера домену дозволяє зберегти працездатність інфраструктури навіть у випадку фізичного збою основного сервера. Перспективи подальших досліджень полягають у міграції побудованої архітектури до гібридної моделі з використанням хмарних сервісів Azure AD та впровадженні SIEM-систем для глибинного аналізу подій безпеки в реальному часі.

Список використаних джерел:

1. Desmond B. et al. "Active Directory." O'Reilly Media, 5th Edition. 2013. 738 p.

2. Moy J. "OSPF: Anatomy of an Internet Routing Protocol." Addison-Wesley Professional. 1998. 352 p.

Кондратюк О.О.
Романюк О.В.
Вінницький національний технічний університет

РОЗРОБКА МЕТОД ІНТЕГРАЦІЇ ЗАСТОСУНКУ З ПЛАТФОРМАМИ ВІДЕОКОНФЕРЕНЦІЙ ДЛЯ ОТРИМАННЯ АУДІОПОТОКУ

Анотація

У роботі представлено розробку методу інтеграції застосунку з платформами відеоконференцій для отримання аудіопотоку

Abstract

The work presents the development of a method for application integration with other videoconference platforms.

Вступ

Сучасні компанії, що працюють у сфері продажів та надання послуг, дедалі частіше стикаються з потребою забезпечити не лише зберігання та облік інформації про клієнтів, а й глибоку аналітику процесу комунікації. Зростання конкуренції та підвищення очікувань споживачів вимагає від бізнесу оперативної, персоналізованої та високоякісної взаємодії з клієнтом у реальному часі.

Важливою функцією сучасних рішень є автоматичне створення транскрипцій дзвінків і подальший аналіз отриманих текстів. Розвиток сервісів розпізнавання мовлення, таких як Recall.ai, Fireflies.ai та Otter.ai, дозволяє отримувати повний текст розмови у реальному часі, виявляти ключові теми, визначати інтонаційні маркери емоцій та оцінювати якість спілкування менеджера.

Також активно розвивається інтеграція CRM із зовнішніми комунікаційними платформами, такими як Zoom, Google Meet або Microsoft Teams. Це забезпечує можливість здійснення дзвінків, відеоконференцій і обміну повідомленнями безпосередньо в межах CRM–системи, що зменшує кількість перемикань між інтерфейсами та підвищує продуктивність користувачів. Розробці саме такого методу інтеграції з комунікаційними платформами присвячена дана робота.

Загальний опис методу інтеграції застосунку з платформами відеоконференцій для отримання аудіопотоку

Для інтелектуальної CRM-системи розроблено універсальний метод інтеграції з платформами відеоконференцій Zoom, Google Meet та Microsoft Teams. На відміну від традиційних рішень, що працюють як додаткові плагіни чи окремі хмарні модулі, запропонований підхід передбачає повне включення функцій відеодзвінків у CRM-інтерфейс. Це дозволяє менеджеру створювати та відкривати онлайн-зустрічі безпосередньо в системі, тоді як клієнт під’єднується через звичну платформу без зміни свого робочого процесу.

Створення мітингу ініціюється менеджером у CRM, після чого система формує конференцію у вибраній платформі через офіційні REST API [1]. Отримання аудіопотоку забезпечується інтеграцією з Recall.ai [2], який підключає віртуального бота до зустрічі та передає голосові дані на бекенд CRM без необхідності модифікації клієнтських застосунків Zoom, Meet або Teams.

Переданий аудіопотік обробляється в режимі реального часу: спочатку передається до модулів транскрипції, а потім — до систем семантичного аналізу. Така інтеграційна модель працює як для зустрічей, створених у межах самої CRM, так і для зовнішніх корпоративних дзвінків, забезпечуючи універсальність та незалежність від конкретної платформи.

Запропонований метод формує прозорий механізм захоплення аудіоданих із будь-якої популярної відеоплатформи та слугує основою для подальшої автоматизованої аналітики в реальному часі, забезпечуючи безперервність, масштабованість і стабільність роботи CRM-системи.

Діаграмне представлення методу інтеграції застосунку з платформами відеоконференцій

Інтеграція CRM-системи з платформами Zoom, Google Meet та Microsoft Teams здійснюється через API-виклики та сервіс Recall.ai, який автоматично підключає віртуального бота до онлайн-зустрічі та передає аудіопотік на сервер. Це усуває потребу у використанні окремих SDK кожної платформи, зменшує залежність від їхніх протоколів і забезпечує уніфікований механізм отримання голосових даних у режимі реального часу.

Для відображення роботи інтеграційного модуля використано дві діаграми. Компонентна діаграма [3] показує структуру системи на рівні сервісів і модулів, відображаючи розподіл функцій між backend’ом (створення мітингів, керування інтеграціями, маршрутизація аудіо), інтеграційним шаром (Zoom API, Teams API, Google Meet API, Recall.ai), користувачами (менеджером і клієнтом) та каналами передачі потокових даних.

Вона дозволяє наочно представити інформаційні зв’язки, залежності й межі відповідальності між компонентами, що важливо для оцінки коректності архітектури, потенціалу масштабування та подальшого розширення системи.

Діаграма компонентів зображена на рисунку 1.

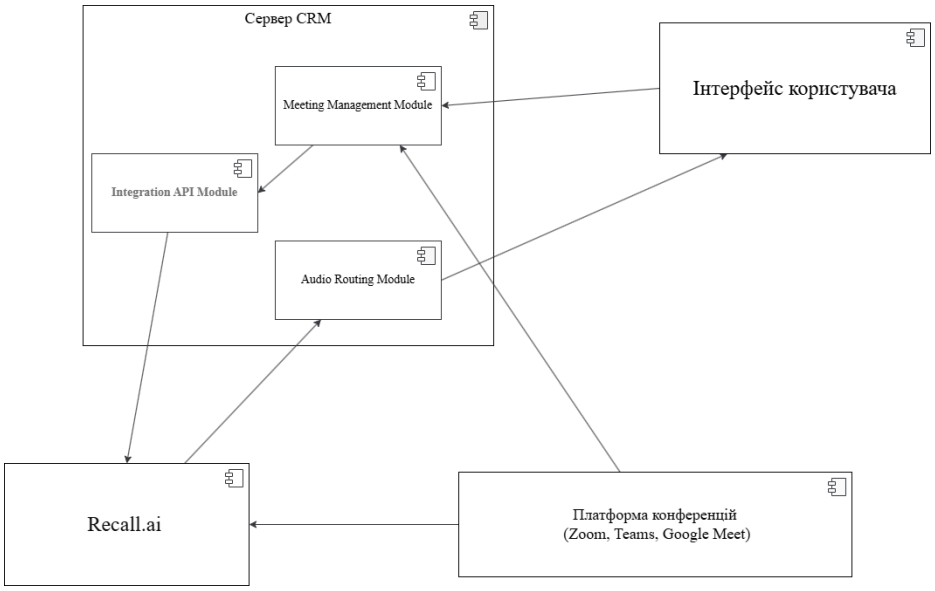


Рисунок 1 – Діаграма компонентів

Висновок

Розглянутий метод інтеграції CRM-системи з платформами Zoom, Google Meet та Microsoft Teams забезпечує універсальний і масштабований механізм отримання аудіопотоку в режимі реального часу. Використання Recall.ai як посередника дозволяє уникнути роботи з окремими SDK кожної платформи, що спрощує архітектуру, підвищує сумісність і усуває залежність від специфічних протоколів відеосервісів.

Діаграмне представлення підтверджує логічну завершеність інтеграційного рішення. Компонентна діаграма демонструє чіткий розподіл функцій і прозорі інформаційні зв’язки між модулями, що вказує на коректність структури та потенціал до масштабування.

Таким чином, запропонований метод інтеграції формує основу для подальшого впровадження інтелектуальних інструментів аналізу голосових взаємодій, забезпечує стабільне отримання аудіоданих і дозволяє розвивати функціональність системи без істотної перебудови архітектури.

Список використаної літератури

1. Що таке rest api: основні принципи та практики застосування. FoxmindEd. URL: https://foxminded.ua/shcho-take-rest-api/ (дата звернення: 24.11.2025).

2. Recall.ai - the API for meeting recording. Recall.ai - The API for Meeting Recording. URL: https://www.recall.ai (date of access: 25.11.2025).

3. Моралес Дж. What is A UML component diagram: symbols and tutorial. MindOnMap | Free Mind Mapping Tool to Draw Ideas Easily Online. URL: https://www.mindonmap.com/uk/blog/uml-component-diagram/ (дата звернення: 25.11.2025).

Лазарович Юлія Ігорівна
студентка 4 курсу, групи ІПЗ-42
Карпатського національного університету
імені Василя Стефаника
м. Івано-Франківськ
+380 (342) 59-60-58
yuliia.lazarovych.22@pnu.edu.ua
Науковий керівник: Козленко Микола Іванович
кандидат технічних наук
доцент кафедри інформаційних технологій
Карпатського національного університету
імені Василя Стефаника
м. Івано-Франківськ

АНАЛІЗ СУЧАСНИХ ПІДХОДІВ ДО РОЗУМІННЯ ВІЗУАЛЬНИХ СЦЕН ДЛЯ РЕАЛІЗАЦІЇ МУЛЬТИМОДАЛЬНОГО RAG-ПІДХОДУ

Постановка задачі. Функціонування сучасних смарт-асистентів обмежене статичною природою навчальних наборів даних, що спричиняє неактуальність інформації та виникнення «галюцинацій» при обробці рідкісних запитів [1]. Проблема критична для задач візуального розуміння, де інтерпретація зображень вимагає точних знань про об’єкти, відсутні в тренувальній вибірці. Ефективним шляхом вирішення зазначеної проблеми є застосування підходу Retrieval-Augmented Generation (RAG), який інтегрує генеративні можливості великих мовних моделей із зовнішніми базами знань.

Мета дослідження. Метою роботи є аналіз існуючих методів інтеграції знань та формулювання вимог до мультимодальної RAG-системи, спрямованої на забезпечення високої семантичної точності та бажаної швидкодії. Дослідження фокусується на розробці підходу, що дозволив би смарт-асистенту надавати обґрунтовані відповіді на візуальні запитання, використовуючи динамічні бази знань без необхідності постійного перенавчання моделі, при цьому дотримуючись обмежень щодо часу реакції системи.

Результати дослідження. У ході роботи проаналізовано ключові архітектури RAG для визначення оптимальної конфігурації системи. Зокрема, метод REVEAL реалізує концепцію наскрізного навчання, де ретривер і генератор оптимізуються спільно з використанням гібридних даних та механізму attentive fusion, що забезпечує високу семантичну узгодженість, проте його ефективність прямо залежить від повноти бази знань, а компресія даних може призводити до втрати деталей [2]. Інший підхід, Visual-RAG, базується на text-to-image пошуку і доводить, що для відповідей на питання про специфічні візуальні деталі пошук схожих зображень є ефективнішим за текстовий, хоча цей метод обмежений вузькою доменною спеціалізацією [3]. Альтернативна архітектура RAP фокусується на перцептивній точності при обробці зображень високої роздільності, застосовуючи динамічний пошук фрагментів зі

збереженням просторових відношень, однак це супроводжується значними обчислювальними витратами [4]. Також розглянуто напрям mKG-RAG, що використовує мультимодальні графи знань для покращення структурного розуміння та логічного міркування, мінімізуючи інформаційний шум, але залишаючись вразливим до помилок на етапі побудови графа [5].

На основі проведеного аналізу сформульовано вимоги до проектованої системи (Рис. 1) . Для забезпечення балансу між точністю та швидкодією доцільним визначено використання комбінованого запиту, що поєднує зображення та текст, оскільки така конфігурація сприяє кращому узгодженню семантичних ознак. Важливим аспектом є впровадження reasoning-шару з listwise-ранжуванням, що дозволяє оцінювати список кандидатів одночасно, підвищуючи релевантність відбору порівняно з поточковими методами. Також пропонується мінімізувати контекст, що передається генератору до 1–3 найбільш релевантних документів, щоб запобігти розмиванню уваги моделі та підвищити семантичну узгодженість відповіді. Технічна реалізація системи передбачає використання векторних індексах та механізмів cross-attention, забезпечуючи роботу в режимі zero-shot без додаткового навчання параметрів

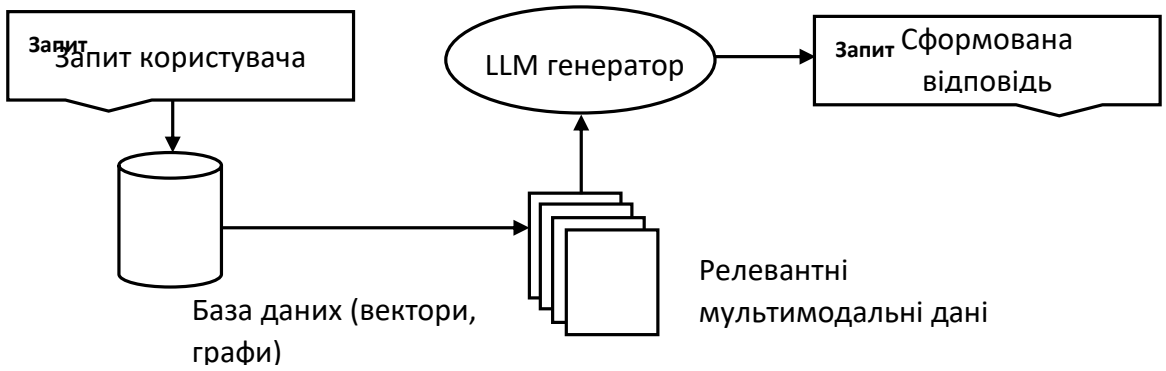


Рисунок 1 — Схема архітектури Retrieval-Augmented Generation (RAG).

Висновки та перспективи. Запропонована архітектура mRAG розглядається як перспективний підхід до забезпечення актуальності знань у смарт-асистентах. Поєднання векторного пошуку, структурованого ранжування та мінімізації контексту дозволяє досягти необхідного балансу між семантичною точністю відповіді та обчислювальною ефективністю системи.

Список використаних джерел

1. C.-W. Hu et al., “mRAG: Elucidating the design space of multi-modal retrieval-augmented generation,” arXiv preprint arXiv:2505.24073, 2025, doi: 10.48550/arXiv.2505.24073.

2. Z. Hu et al., “Reveal: Retrieval-augmented visual-language pre-training with multi-source multimodal knowledge memory,” in 2023 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), Vancouver, BC, Canada, 2023, pp. 23369–23379, doi: 10.1109/CVPR52729.2023.02238.

3. Y. Wu et al., “Visual-RAG: Benchmarking text-to-image retrieval augmented generation for visual knowledge intensive queries,” arXiv preprint arXiv:2502.16636, 2025, doi: 10.48550/arXiv.2502.16636.

4. W. Wang et al., “Retrieval-augmented perception: High-resolution image perception meets visual RAG,” in Proc. 42nd Int. Conf. Mach. Learn. (ICML), 2025, doi: 10.48550/arXiv.2503.01222.

5. X. Yuan et al., “mKG-RAG: Multimodal knowledge graph-enhanced RAG for visual question answering,” arXiv preprint arXiv:2508.05318, 2025, doi: 10.48550/arXiv.2508.05318.

Гуляєв Микита Віталійович
студент 3 курсу, групи КІ-23
Кам’янський енергетичний фаховий коледж
комп’ютерна інженерія
м. Кам’янське
Науковий керівник: Павлюченко Сергій Олександрович
викладач циклової комісії комп’ютерних дисциплін
Кам’янський енергетичний фаховий коледж
магістр інженерії програмного забезпечення
м. Кам’янське
(093)-463-72-86
sopavluchenko@kadet.ukr.education

АВТОМАТИЗАЦІЯ ГЕНЕРУВАННЯ КРІПЛЕНЬ ТА ОТВОРІВ ДЛЯ ПЛАТ ESP32/ARDUINO У 3D-МОДЕЛЯХ КОРПУСІВ ЧЕРЕЗ PYTHON API FREECAD

Вступ Проєктування корпусів для електронних пристроїв потребує точного розміщення кріплень та монтажних отворів, що у разі ручного виконання є тривалим процесом та містить значні ризики похибок. FreeCAD із вбудованим Python API забезпечує можливість автоматизувати такі операції та створювати параметричні моделі, які легко адаптуються під конкретні плати та задачі.

Мета та завдання дослідження Метою дослідження є розробка методики автоматизованого створення посадкових отворів і стійок для плат ESP32/Arduino в 3D-моделях корпусів із використанням Python API FreeCAD та технологій штучного інтелекту. Для досягнення цієї мети необхідно:

1. Проаналізувати особливості параметричного моделювання в FreeCAD;
2. Розробити алгоритм автоматичного генерування кріплень за допомогою Python-скриптів і алгоритмів ШІ для точнішого розрахунку параметрів кріплень на основі наданих характеристик плат;
3. Описати реалізацію Python-скрипта, що включає інтеграцію з моделями ШІ для автоматичної корекції та оптимізації конструкцій;
4. Запропонувати рекомендації щодо використання цієї методики в освітньому процесі, особливо для навчання студентів роботі з автоматизованим моделюванням і застосуванням ШІ в інженерії.

Методика. Методика базується на застосуванні FreeCAD, Python API та середовищ Sketcher, Part і PartDesign. Основний процес включає отримання габаритів плати (вручну, зі STEP/STL або з використанням ШІ), параметричну побудову корпусу, автоматичне генерування стійок і монтажних отворів за координатами, перевірку колізій та експорт моделі у STL/STEP для 3D-друку чи подальшої обробки.

Практична реалізація.

Сучасні мікроконтролерні плати, такі як ESP32 DevKit v1– або Arduino Nano, мають різні габарити та топологію монтажних отворів, що ускладнює розробку універсальних корпусів. Точність у розміщенні кріплень є критичною: відхилення навіть у межах 0.2–0.3 мм*– може спричинити несумісність плати з корпусом. Для вирішення цієї проблеми застосування Python API*– в FreeCAD*– дозволяє формувати параметричні моделі програмно, де всі геометричні елементи генеруються на основі математичних параметрів. Такий підхід дозволяє уникнути ручної роботи та забезпечити повторюваність результатів [1].

В дослідженні було проведено аналіз конструктивних параметрів плати ESP32 DevKit v1, у результаті якого встановлено наступні характеристики:

– Габарити плати: 51.5×28 мм
– Ширина робочої зони: 23 мм
– Діаметр монтажних отворів: приблизно 2.8 мм
– Зміщення центрів монтажних отворів: 1.5 мм від країв.

Ці параметри були інтегровані в Python-скрипт, що автоматично генерує:

– Платформу-основу корпусу з зазором 3 мм
– Стійки висотою 6 мм
– Отвори під гвинти M2
– Можливість додавання верхньої кришки та сервісних вирізів

Для автоматизації цього процесу був використаний штучний інтелект, який допоміг створити тестовий код на Python – для генерації параметричних моделей. ШІ дозволив швидко налаштувати алгоритми для створення макросів, що дає змогу не лише забезпечити точність геометрії, але й створювати універсальні шаблони, здатні адаптуватися під різні типи плат.

Результат тестування макросу для генерації моделі продемонстровано на рисунку 1.

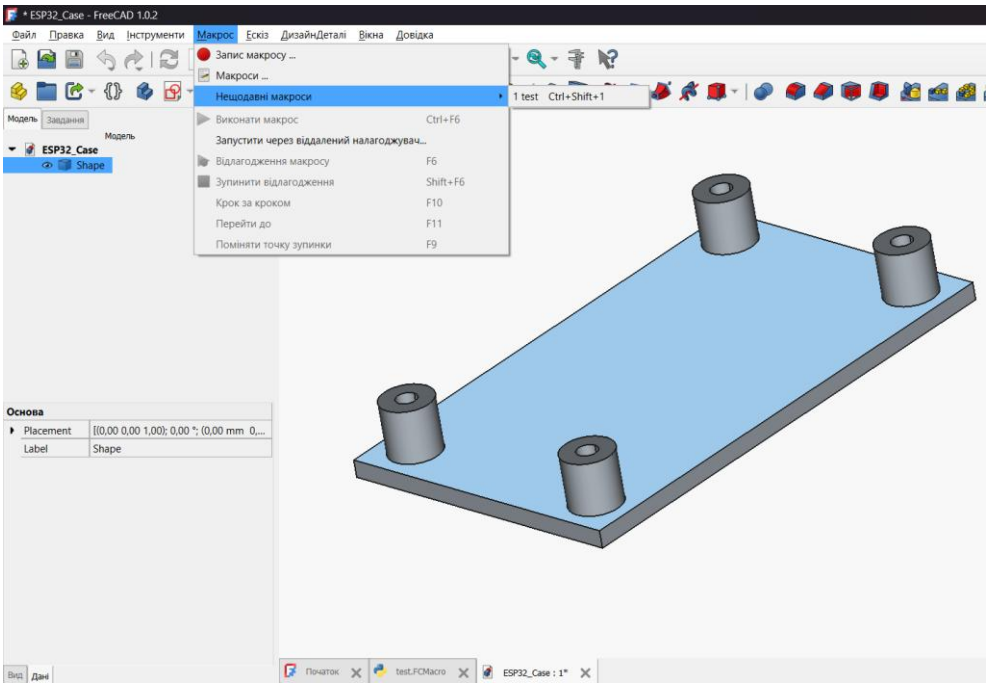


Рис. 1. Тестовий результат роботи макроса на Python

Автоматизація дозволяє створювати бібліотеки параметричних корпусів для ESP-/Arduino-пристроїв, які можна використовувати у навчальному процесі,

прототипуванні та промислових задачах. Запропонований скрипт є універсальним шаблоном і може бути адаптований під будь-яку іншу модель плати [2].

Результати та обговорення

Розроблений підхід забезпечує швидке формування варіантів корпусів із різними параметрами без ручного втручання. Підвищується точність моделювання та зменшується ймовірність похибок, що робить метод зручним для студентських лабораторних робіт.

Для підвищення надійності кріплення у пластикових корпусах рекомендовано застосовувати термовставки (heat-set inserts) [3].

Висновки та перспективи. Використання штучного інтелекту для автоматизації генерації кріплень і монтажних отворів через Python API в FreeCAD значно прискорює розробку корпусів для ESP32/Arduino, підвищує точність моделювання та дозволяє створювати масштабовані параметричні бібліотеки. Така методика є перспективною для впровадження у навчальні курси з комп'ютерної інженерії та 3D-моделювання. В подальшому можна розвивати інструменти для адаптації під різні типи мікро

Список використаних джерел

1 1.FreeCAD — офіційний ресурс і документація по Python API та робочим наборам. https://www.freecad.org

2 2.Weigu Lu. FreeCAD 3D box macro — приклад макросу для генерації простого корпусу. https://www.weigu.lu/other_projects/freecad/freecad_3dbox_macro/index.html

3 3.Designing simple plastic electronics enclosure using a repeatable workflow in FreeCAD. https://stories.alsado.de/designing-simple-plastic-electronics-enclosure-using-a-repeatable-workflow-in-freecad/

Приймак Євгеній Олександрович
студент 6 курсу, групи КСДМ-61
Державного університету
інформаційно-комунікаційних технологій
м. Київ
(099)-111-25-07
pryimack99@gmail.com
Науковий керівник: Віталій Волохін Васильович
кандидат технічних наук
доцент кафедри Комп'ютерної інженерії
Державного університету
інформаційно-комунікаційних технологій
м. Київ

МЕТОДИ ПОПЕРЕДНЬОЇ ОБРОБКИ ТА АДАПТИВНОЇ БІНАРИЗАЦІЇ ЗАШУМЛЕНИХ ЗОБРАЖЕНЬ В СИСТЕМАХ ЕЛЕКТРОННОГО УРЯДУВАННЯ

Анотація. Робота присвячена дослідженню алгоритмів попередньої обробки зображень документів перед етапом оптичного розпізнавання символів (OCR). Проаналізовано ефективність методів адаптивної бінаризації для усунення артефактів нерівномірного освітлення та шумів на скан-копіях низької якості.

Abstract. The paper investigates image preprocessing algorithms for documents prior to the Optical Character Recognition (OCR) stage. The efficiency of adaptive binarization methods for eliminating uneven lighting artifacts and noise on low-quality scan copies is analyzed.

Вступ. Впровадження систем автоматизованої обробки інформації в державних установах стикається з проблемою низької якості вхідних даних. В умовах переходу до мобільного отримання адміністративних послуг, джерелом цифрового образу документа все частіше стає камера смартфону, а не професійний сканер. Це призводить до появи класу зображень «in the wild» (зображення в природних умовах), які характеризуються геометричними викривленнями, розфокусуванням, наявністю тіней від сторонніх об'єктів та відблисками на захисних елементах (голограмах).

Класичні системи оптичного розпізнавання (OCR), такі як Tesseract, демонструють різке падіння точності розпізнавання (до 60% і нижче) при роботі з такими зображеннями. Критичним етапом, що визначає успіх подальшого аналізу, є попередня обробка (препроцесинг) та бінаризація. Попередня обробка є ключовим компонентом конвеєра OCR, і часто саме вона, а не вибір моделі розпізнавання, визначає кінцеву точність системи [1]. Метою даної роботи є аналіз методів адаптивної обробки зображень для підвищення якості розпізнавання документів у державних реєстрах.

Основна частина. Процес підготовки зображення державного документа (наприклад, ID-картки або паперового свідоцтва) до розпізнавання можна розділити на три ключові етапи: геометрична корекція, фільтрація шумів та порогова сегментація (бінаризація).

На першому етапі необхідно усунути перспективні викривлення. Для цього використовується алгоритм детекції контурів документа з подальшим застосуванням матриці гомографії для трансформації зображення у плоский вигляд. Однак, навіть після вирівнювання, зображення часто містить шуми, спричинені зернистістю сенсора камери або текстурою паперу.

Для придушення шумів доцільно використовувати фільтр Гауса, який згладжує зображення, усуваючи високочастотні артефакти, але зберігаючи загальні контури символів. Математично це реалізується через згортку зображення з ядром, значення якого спадають від центру до країв за законом нормального розподілу. Експериментально встановлено, що для документів з дрібним шрифтом (наприклад, мікротекст на паспортах) оптимальним є використання невеликого ядра згортки. Більші ядра призводять до втрати деталей тонких ліній символів.

Найбільш складним завданням є етап бінаризації. Найпоширеніший метод глобальної бінаризації Оцу розраховує єдиний поріг інтенсивності для всього зображення, мінімізуючи дисперсію всередині класів (фон і текст). Проте глобальне порогове значення може бути неефективним, коли умови освітлення змінюються в різних областях зображення, у таких випадках слід застосовувати адаптивні порогові значення [2]. У державних документах це проявляється, коли частина бланка знаходиться в тіні або засвічена спалахом.

Для вирішення цієї проблеми у роботі пропонується використання методів локальної (адаптивної) бінаризації, де порогове значення розраховується індивідуально для кожного пікселя на основі статистики його околу. Одним з найефективніших алгоритмів для текстових документів є метод Сауволи.

Сутність методу Сауволи полягає в тому, що поріг адаптується до локального контрасту. Алгоритм аналізує невелике вікно навколо кожного пікселя і обчислює локальне середнє значення та стандартне відхилення. Адаптивне порогове визначення дозволяє сегментувати передній план від фону навіть за наявності нерівномірного освітлення, використовуючи локальне порогове значення для кожного пікселя [3]. Це особливо актуально для українських паспортів, де гільйошна сітка часто інтерпретується простими алгоритмами як частина тексту.

Програмна реалізація запропонованого підходу була виконана мовою Python з використанням бібліотеки комп'ютерного зору OpenCV. Експериментальне дослідження проводилося на вибірці з 500 зображень документів різної якості.

Порівняльний аналіз показав, що застосування глобального методу Оцу дає задовільний результат лише для 34% зображень (переважно сканів високої якості). У той час як адаптивний метод Сауволи, доповнений попередньою

Гаусовою фільтрацією, дозволив коректно бінаризувати 89% документів, включаючи ті, що мали значні перепади освітлення та бліки від голограм.

Однак, варто зазначити, що адаптивна бінаризація вимагає значно більших обчислювальних ресурсів порівняно з глобальними методами, оскільки вимагає розрахунку статистик для кожного пікселя. Для оптимізації швидкодії у системах реального часу доцільно використовувати інтегральні зображення, що дозволяє обчислювати суму інтенсивностей у довільному прямокутному вікні за фіксований час, незалежно від розміру вікна.

Додатковим етапом обробки є морфологічні операції, які застосовуються після бінаризації для усунення дрібних шумових точок. Для тексту доцільно використовувати операцію морфологічного замикання, яке допомагає відновити цілісність розірваних символів, що виникає при друці на матричних принтерах (характерно для старих довідок).

Висновки. Дослідження підтвердило, що якість попередньої обробки зображення є критичним фактором для систем інтелектуального аналізу державних документів. Використання стандартних методів глобальної бінаризації є недостатнім для обробки фотографій, отриманих з мобільних пристроїв.

Запропонований конвеєр обробки, що включає корекцію перспективи, фільтрацію Гауса та адаптивну бінаризацію за методом Сауволи, дозволяє підвищити точність подальшого OCR-розпізнавання на 25-30% для зображень низької якості. Подальші дослідження будуть спрямовані на розробку нейромережевих методів бінаризації, які здатні ще ефективніше відокремлювати текст від складних фонових візерунків захисних документів.

Список використаних джерел

1. Kumar D. Introduction to Data Preprocessing in Machine Learning. Towards Data Science. URL: https://towardsdatascience.com/introduction-to-data-preprocessing-in-machine-learning-a9fa83a5dc9d (дата звернення: 26.11.2025).

2. OpenCV: Image Thresholding. OpenCV. URL: https://docs.opencv.org/4.x/d7/d4d/tutorial_py_thresholding.html (дата звернення: 26.11.2025).

3. Thresholding – skimage 0.25.2 documentation. scikit-image. URL: https://scikit-image.org/docs/stable/auto_examples/segmentation/plot_thresholding.html (дата звернення: 26.11.2025).

Школьний Ілля Михайлович
студент 6 курсу, групи КСДМ-61
Державного університету
інформаційно-комунікаційних технологій
м. Київ
Іжевський Тарас Богданович
студент 6 курсу, групи КСДМ-61
Державного університету
інформаційно-комунікаційних технологій
м. Київ

ІМПЛЕМЕНТАЦІЯ СИСТЕМИ УПРАВЛІННЯ ЦИФРОВИМИ ПРАВАМИ AD RMS У ВІРТУАЛЬНОМУ СЕРЕДОВИЩІ PROXMOX VE

Постановка задачі. У сучасних умовах розмивання мережевого периметра традиційні засоби захисту, такі як міжмережеві екрани, втрачають свою ефективність. Коли файл із конфіденційною інформацією залишає захищену корпоративну мережу, організація втрачає контроль над його подальшим використанням, копіюванням чи розповсюдженням. Це створює критичні ризики інсайдерських загроз та витоку інтелектуальної власності. Зазначена проблема зумовлює необхідність переходу до концепції «персистентного» захисту, де політики безпеки є невід'ємною частиною самого файлу, а управління інфраструктурою здійснюється на базі гнучких та економічно ефективних платформ віртуалізації.

Мета дослідження. Метою дослідження є підвищення рівня інформаційної безпеки та забезпечення контролю над корпоративним контентом шляхом проєктування та практичної реалізації системи управління цифровими правами у відмовостійкому віртуальному середовищі Proxmox VE.

Результати дослідження. У ході дослідження було проведено порівняльний аналіз платформ віртуалізації та обґрунтовано вибір гіпервізора KVM у складі Proxmox VE, що дозволило знизити капітальні витрати та забезпечити високу продуктивність. Запропоновано архітектуру мережі з використанням основного та резервного контролерів домену на базі Windows Server, що гарантує безперервність процесів аутентифікації. Ключовим елементом системи стала служба AD RMS, для якої розроблено диференційовані шаблони політик прав. Ці політики технічно унеможливлюють несанкціонований друк, копіювання в буфер обміну та створення знімків екрана. Надійність збереження даних забезпечено впровадженням Proxmox Backup Server з механізмами дедуплікації та шифрування резервних копій.

Висновки та перспективи. Запропонована система забезпечує захист конфіденційної інформації незалежно від місця її зберігання та каналів передачі. Інтеграція AD RMS із Active Directory дозволяє централізовано керувати правами доступу на основі рольової моделі. Перспективи подальших досліджень полягають у розширенні підтримки мобільних пристроїв для доступу до

захищеного контенту та переході від самопідписаних сертифікатів до повноцінної інфраструктури відкритих ключів.

Список використаних джерел:

1. Desmond B. et al. "Active Directory." O'Reilly Media, 5th Edition. 2013. 738 p.
2. Ahmed W. "Mastering Proxmox." Packt Publishing, 3rd Edition. 2017. 466 p.

Марчук Роман Олексійович
студент 6 курсу, групи КСДМ-62
Державного університету
інформаційно-комунікаційних технологій
+380687836114
Roma.marchuk11@gmail.com
Науковий керівник: Коротков С.С.

ІМПЛЕМЕНТАЦІЯ WEB APPLICATION FIREWALL ДЛЯ ПІДВИЩЕННЯ РІВНЯ БЕЗПЕКИ ВЕБ-ЗАСТОСУНКІВ

В умовах стрімкого розвитку цифрових сервісів та зростання кількості веб-застосунків питання інформаційної безпеки набуває особливої актуальності. Веб-застосунки є однією з основних цілей кібератак, оскільки вони безпосередньо взаємодіють з користувачами та обробляють конфіденційні дані. Серед найбільш поширених загроз можна виділити SQL-ін’єкції, міжсайтовий скриптинг (XSS), атаки типу CSRF, підбір облікових даних, а також спроби несанкціонованого доступу до ресурсів системи. Одним із ефективних засобів протидії таким загрозам є використання Web Application Firewall (WAF). Web Application Firewall є програмно-апаратним або програмним рішенням, яке здійснює аналіз HTTP/HTTPS-трафіку між клієнтом і сервером та дозволяє виявляти і блокувати потенційно небезпечні запити. На відміну від традиційних мережевих міжмережевих екранів, WAF працює на рівні прикладного протоколу та враховує логіку роботи веб-застосунку. Це дозволяє більш точно ідентифікувати атаки, спрямовані на вразливості прикладного рівня.

Постановка задачі

Метою даного дослідження є обґрунтування доцільності використання Web Application Firewall як складової багаторівневої системи захисту веб-застосунків та розробка практичних підходів до його впровадження і налаштування у тестовому середовищі. Для досягнення поставленої мети у роботі необхідно вирішити такі завдання:

– проаналізувати основні загрози безпеці сучасних веб-застосунків та визначити найбільш критичні вектори атак;

– дослідити принципи роботи технології Web Application Firewall та її місце в архітектурі багаторівневого захисту;

– розглянути існуючі типи WAF-рішень (хмарні, мережеві, хостові) та обґрунтувати вибір оптимального варіанту для практичної реалізації;

– розгорнути тестовий веб-застосунок і налаштувати WAF з використанням типових правил безпеки та наборів OWASP Core Rule Set;

– оцінити вплив налаштувань WAF на рівень захищеності веб-застосунку та стабільність його роботи.

Мета дослідження

Метою даного дослідження є розробка та практична реалізація підходу до підвищення рівня інформаційної безпеки веб-застосунків шляхом впровадження технології Web Application Firewall, який забезпечує виявлення, аналіз і блокування сучасних атак прикладного рівня, а також підвищення стійкості веб-сервісів до несанкціонованого доступу та порушення їхньої працездатності. У межах дослідження передбачається створення тестового середовища веб-застосунку, розгортання та налаштування WAF з використанням актуальних наборів правил безпеки, зокрема OWASP Core Rule Set, а також аналіз впливу застосованих механізмів захисту на ефективність, стабільність і доступність веб-ресурсу. Реалізований підхід має бути адаптивним до змін загроз, придатним для використання у корпоративних і навчальних інформаційних системах, орієнтованим на масштабування та подальше вдосконалення відповідно до розвитку веб-технологій і вимог кібербезпеки.

Таблиця 1 Характеристики та функції Network Firewall і WAF

Ознака	**Network Firewall**	**Web Application Firewall (WAF)**
Рівень OSI	Network / Transport	Application
Тип аналізу	Пакетний, заголовки IP/TCP	Контент HTTP/HTTPS
Основні функції	Контроль з’єднань, IP, портів, протоколів	Аналіз параметрів, виявлення атак на веб-рівні
Захист від	DDoS, несанкціонованих підключень	SQLi, XSS, CSRF, API-атаки
Режими роботи	Пропуск/блокування трафіку	Моніторинг, блокування, навчання
Інтеграція	З маршрутизаторами, VPN, IDS	З SIEM, IDS/IPS, CDN
Приклад розгортання	На межі корпоративної мережі	Перед веб-серверами або у хмарі

Враховуючи наведені принципи роботи мережевих екранів і їхні обмеження, доцільно розглянути порівняльну характеристику класичного мережевого фаєрвола (Network Firewall) і веб-фаєрвола (Web Application Firewall, WAF). Обидва інструменти мають спільну мету – захист інформаційних систем від зовнішніх загроз, однак реалізують її на різних рівнях моделі OSI та з різним ступенем глибини аналізу трафіку. В таблиці 2 наведено узагальнену схему, що демонструє відмінності між Network Firewall та WAF за основними параметрами роботи.

Таблиця 2 Порівняння Network Firewall та Web Application Firewall

Критерій порівняння	**Network Firewall**	**Web Application Firewall (WAF)**
Рівень OSI	Працює на мережевому (3) та транспортному (4) рівнях	Функціонує на прикладному (7) рівні
Об’єкт контролю	Пакети даних, IP-адреси, порти, протоколи	HTTP/HTTPS-запити, параметри URI, cookie, тіла запитів
Тип аналізу	Поверхневий, фільтрація за статичними правилами	Глибокий (Deep Packet Inspection), аналіз контенту запитів
Призначення	Захист мережевої інфраструктури від несанкціонованого доступу	Захист веб-додатків від атак прикладного рівня
Основні загрози, що блокуються	Сканування портів, DoS, спуфінг, несанкціоновані підключення	SQL Injection, XSS, CSRF, RFI/LFI, API-атаки
Підтримка шифрування (TLS)	Обмежена, не аналізує зашифрований трафік	Може виконувати SSL/TLS-інспекцію для HTTPS-запитів
Контекстна обробка	Відстежує стан сесій (stateful inspection)	Розуміє логіку HTTP-сеансу, перевіряє заголовки, параметри, куки
Механізми реагування	Блокування або дозволення з’єднання	Блокування, переписування запитів, формування звітів
Оновлення та адаптація	Використовує статичні правила, що оновлюються вручну	Має сигнатурні та евристичні механізми, підтримує автоматичне оновлення баз
Інтеграція з іншими системами	Працює з маршрутизаторами, VPN, IDS	Інтегрується з SIEM, IDS/IPS, CDN та системами моніторингу
Типове розташування в мережі	На периметрі корпоративної мережі, між внутрішнім і зовнішнім сегментами	Між користувачем та веб-сервером (on-premises або у хмарі)

Результати дослідження

У результаті проведеного дослідження було реалізовано тестове середовище веб-застосунку та впроваджено Web Application Firewall із використанням сучасних механізмів фільтрації HTTP/HTTPS-трафіку. Проведене налаштування WAF на основі OWASP Core Rule Set дозволило

виявляти та блокувати типові атаки прикладного рівня, зокрема SQL-ін’єкції, міжсайтовий скриптинг (XSS), спроби обходу механізмів автентифікації та інші шкідливі запити. Аналіз результатів експериментального використання показав зниження кількості успішних атак на веб-застосунок, підвищення рівня його стійкості до зовнішніх загроз та зменшення ризику компрометації даних. Встановлено, що коректне налаштування правил безпеки дозволяє мінімізувати кількість хибних спрацювань без суттєвого впливу на продуктивність і доступність веб-ресурсу. Отримані результати підтверджують ефективність застосування WAF як важливого елементу системи захисту веб-застосунків.

Висновки та перспективи

За результатами проведеного дослідження можна зробити висновок, що впровадження Web Application Firewall є доцільним і ефективним способом підвищення рівня інформаційної безпеки веб-застосунків. WAF дозволяє реалізувати додатковий рівень захисту, спрямований на протидію актуальним загрозам прикладного рівня, та суттєво знижує ймовірність успішної експлуатації вразливостей. Перспективами подальших досліджень є розширення функціональних можливостей WAF шляхом використання поведінкового аналізу, інтеграції з системами моніторингу та журналювання подій безпеки, а також застосування методів машинного навчання для адаптації правил фільтрації до нових типів атак. Отримані напрацювання можуть бути використані під час розробки та експлуатації захищених веб-систем у корпоративному, хмарному та навчальному середовищах. Отримані результати можуть бути використані під час проєктування та експлуатації веб-застосунків у корпоративному та навчальному середовищі.

Список використаних джерел

1. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems. Geneva: ISO, 2022. 45 p.
2. RFC 2979. Behavior of and Requirements for Internet Firewalls. The Internet Society, 2000. URL: https://www.rfc-editor.org/rfc/rfc2979 (дата звернення: 02.11.2025).
3. Scarfone, K., Hoffman, P. Guide to Intrusion Detection and Prevention Systems (IDPS). NIST, 2020. 120 p.
4. Lukan, P. Modern Web Application Firewall Design and Evaluation. Journal of Information Security Research, 2021, Vol. 12(3), pp. 45–58.
5. Khurana, H., Singh, R. Improving Web Application Security Using Multi-Layered WAF and IDS Integration. International Journal of Computer Applications, 2022, Vol. 184(29), pp. 1–8.
6. Карпінський М. П. Методи безпечної роботи при використанні SQL-сервера ORACLE / Карпінський М.П., Сальніков М. // Вісник Тернопільського державного технічного університету , 2002 – том 7. – с.95-100

Бовсунівський Микола Сергійович
студент 5 курсу, групи КСДМ-51,
Державного університету
інформаційно-комунікаційних технологій
Науковий керівник: Лащевська Наталія Олександрівна
завідувач кафедри, к.т.н., доцент,
Державного університету
інформаційно-комунікаційних технологій, м. Київ

КОМПЛЕКСНА АДАПТИВНА СИСТЕМА КІБЕРБЕЗПЕКИ ДЕЦЕНТРАЛІЗОВАНИХ МЕРЕЖ РОЙОВИХ БПЛА НА ОСНОВІ ІНЖЕНЕРІЇ ДАНИХ ТА ШТУЧНОГО ІНТЕЛЕКТУ

Анотація.У зв'язку зі стрімким розвитком групових (ройових) польотів безпілотних авіаційних систем (БПЛА), гостро постає проблема забезпечення їхньої кібербезпеки в умовах децентралізованої мережевої архітектури. Ця теза присвячена розробці та дослідженню комплексної адаптивної системи кібербезпеки для децентралізованих мереж БПЛА, яка інтегрує принципи інженерії даних та методи штучного інтелекту. Система фокусується на моніторингу та аналізі даних, що передаються через канал зв'язку між БПЛА, а також на захисті бортової РЛС та інтелектуального модуля прийняття рішень (ШІ) від зовнішніх та внутрішніх кібератак.

Вступ та Актуальність Проблеми.Групові польоти БПЛА використовуються у критично важливих сферах, таких як пошуково-рятувальні місії, військова розвідка та моніторинг. Ефективність цих систем безпосередньо залежить від надійності їхньої комп’ютерної мережі та здатності кожного апарату до автономного прийняття рішень.

Децентралізована архітектура рою, що використовує прямий зв'язок між БПЛА, робить її вразливою до низки загроз, включаючи спуфінг даних (особливо даних РЛС та GPS), атаки відмовою в обслуговуванні (DoS/DDoS) на канали зв'язку та несанкціоноване втручання в алгоритми ШІ (наприклад, отруєння даних DQN).

Метою дослідження є розробка та впровадження механізмів кібербезпеки, які використовують інструменти інженерії даних для збору, обробки та аналізу великих обсягів мережевого та сенсорного трафіку, а також ШІ-алгоритми для виявлення та нейтралізації аномалій у режимі реального часу.

Методологія та Інженерія Даних

1. Збір та Попередня Обробка Даних:

Створення розподіленої платформи для збору даних з бортової РЛС, відеокамер (опційно), та мережевого трафіку (Канал зв'язку між БПЛА).

Застосування методів інженерії даних для нормалізації, фільтрації та анотації даних, що живлять інтелектуальний модуль (ШІ: DQN + рій + нечітка логіка) та моделі виявлення вторгнень.

2. Розробка Адаптивного Моніторингу на Основі ШІ:

Впровадження глибоких нейронних мереж (Deep Q-Network) не лише для уникнення зіткнень, але й для виявлення мережевих аномалій та порушень роботи сенсорів.

Використання нечіткої логіки для оцінки рівня загрози на основі неточних або неповних даних, характерних для динамічного середовища рою.

3. Децентралізовані Механізми Захисту:

Розробка децентралізованого протоколу автентифікації та шифрування, що дозволяє кожному БПЛА незалежно перевіряти цілісність даних, отриманих від Інших БПЛА рою.

Створення механізму кіберстійкого генератора безпечного маршруту, який може ігнорувати скомпрометовані дані РЛС/зв'язку та покладатися на найменш вразливі сенсори.

Очікувані Результати.Очікується, що запропонована система значно підвищить стійкість та безпеку рою БПЛА в кіберпросторі.

- Зменшення успішних кібератак (наприклад, спуфінгу) на 45-60% порівняно з системами, що не використовують ШІ для виявлення вторгнень.
- Час реагування на кіберзагрозу буде зменшено, інтегруючи процеси виявлення безпосередньо в цикл обробки даних та керування БПЛА.
- Підтвердження масштабованості та енергоефективності запропонованих алгоритмів кібербезпеки в середовищі симуляції Gazebo/ROS 2.

Висновки та Перспективи.Інтеграція інженерії даних, комп’ютерних мереж (децентралізована архітектура) та методів штучного інтелекту є критично необхідною для забезпечення кібербезпеки сучасних ройових БПЛА. Подальші дослідження будуть зосереджені на впровадженні блокчейн-технологій для незмінності бортових журналів даних та вдосконаленні алгоритмів федеративного навчання для спільного, але приватного обміну інформацією про кіберзагрози між БПЛА рою.

Список використаних джерел

1. Handbook of Unmanned Aerial Vehicles. Springer, 2015. DOI: 10.1007/978-90-481-9707-1. (Загальні принципи побудови БПЛА та їхніх систем).

2. Sutton R., Barto A. Reinforcement Learning: An Introduction. MIT Press, 2018. URL: http://incompleteideas.net/book/the-book.html. (Фундаментальні основи навчання з підкріпленням, включаючи Deep Q-Networks).

3. Hussain, M. A., & Kim, K. Cybersecurity Issues in UAV Control and Network System: A Systematic Review. IEEE Access, 2025. (Систематичний огляд кіберзагроз у мережах БПЛА та методів виявлення вторгнень).

4. Zhang, L., Wang, Q., & Li, Y. Deep Reinforcement Learning for Intrusion Detection in Aerial Computing Networks. Journal of Network and Computer Applications, 2024. (Застосування DRL для автономного виявлення атак у повітряних обчислювальних мережах).

5. Alsaedi, O., Alosaimi, M., & Al-Turjman, F. Federated Deep Learning for Cybersecurity and Intrusion Detection in Decentralized Networks. IEEE Internet of Things Journal, 2024. (Використання федеративного навчання для підвищення

конфіденційності та точності виявлення вторгнень у децентралізованих системах).

6. Kim, J., Choi, H., & Park, K. A Theoretical Framework for Decentralized Intrusion Detection in Smart Networks Using Blockchain and Machine Learning. Journal of Information Security and Applications, 2025. (Дослідження інтеграції Blockchain та ML для забезпечення цілісності даних та децентралізованого реагування на загрози).

Роботько Денис Олександрович
аспірант 3 курсу
Вінницького національного технічного університету
м. Вінниця
097-404-27-43
denysrobotko@gmail.com

ВИМОГИ ДО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНИХ СИСТЕМ УПРАВЛІННЯ ЗНАННЯМИ

Постановка задачі. У рамках даного дослідження було визначено та систематизовано вимоги до програмного забезпечення інформаційних систем управління знаннями (ІСУЗ) для забезпечення їх ефективності, інтегрованості та відповідності сучасним стандартам і вимогам.

Мета дослідження. Метою даного дослідження є формування узгодженого переліку функціональних і нефункціональних вимог до ПЗ систем управління знаннями.

Результати дослідження. У сучасних умовах цифрової трансформації підприємств та освітніх установ ІСУЗ відіграють вирішальну роль у забезпеченні безперервного розвитку компетентностей, підвищенні продуктивності персоналу та формуванні інтелектуального потенціалу організацій. Програмне забезпечення ІСУЗ має підтримувати повний цикл роботи зі знаннями – від їх вилучення та структурування до аналізу, поширення і повторного використання у корпоративному чи навчальному середовищі. Тому формування вимог до програмного забезпечення таких систем є важливим етапом їх проєктування.

Однією з основних вимог є забезпечення збору та формалізації знань. Програмне забезпечення має підтримувати можливість інтеграції з різними джерелами інформації: документами, навчальними матеріалами, корпоративними базами даних, засобами комунікації, соціальними сервісами тощо. Застосування методів автоматичного й напівавтоматичного витягнення знань, інструментів класифікації та засобів онтологічного моделювання сприяє їх подальшій систематизації. ПЗ повинно забезпечувати механізми побудови та підтримки онтологій, таксономій і графових представлень знань, що дозволяє точно описувати складні взаємозв’язки між поняттями.

Другим важливим аспектом є організація та зберігання знань. Програмне забезпечення повинно підтримувати репозиторії знань із можливістю роботи як зі структурованою, так і з напівструктурованою інформацією. Переважним є використання гібридних моделей зберігання: поєднання реляційних СУБД, графових БД та формальних моделей, таких як RDF або OWL[1]. Потрібна підтримка механізмів контролю якості знань, їхньої актуалізації, відстеження версій та фіксації історії змін.

Важливу роль відіграють засоби пошуку та доступу. Система має забезпечувати багатоаспектний пошук: повнотекстовий, атрибутний, семантичний, контекстний та рекомендативний. Застосування алгоритмів

природної мови, індексації та семантичного аналізу дає змогу підвищити релевантність знайденої інформації. Важливою вимогою є реалізація персоналізованих механізмів доступу – рекомендацій знань залежно від професійних ролей, рівня компетентності чи навчальної траєкторії користувача.

Актуалізація, супровід та поширення знань також становлять невід'ємну частину функціональних можливостей ІСУЗ. Програмне забезпечення має підтримувати спільне редагування знань, організацію спільної роботи, автоматичні механізми перевірки застарілості інформації та виявлення дублювання. Підсистема управління версіями є обов'язковим компонентом, що забезпечує відстеження змін у корпоративних або освітніх базах знань.

Окремою групою функціональних вимог є аналітичні та прогностичні можливості системи. ПЗ повинно включати засоби оцінювання рівня компетентності користувачів, моделювання навчальних процесів, аналізу структури знань та прогнозування потреб у навчанні. Доцільним є впровадження методів машинного навчання для побудови рекомендаційних систем, виявлення прогалин у знаннях та оцінювання ефективності комунікаційних процесів.

Нефункціональні вимоги визначають якість і надійність програмного забезпечення ІСУЗ, а також можливості його експлуатації в умовах масштабних організацій.

Першою вимогою є масштабованість. Система повинна забезпечувати роботу з великими обсягами даних та підтримувати зростання кількості користувачів без втрати продуктивності. Важливою є можливість горизонтального масштабування, розподіленої обробки даних та використання хмарних обчислень.

Не менш значущою є сумісність із корпоративними інформаційними системами – ERP, CRM, HRM, LMS [2, 3] тощо. ПЗ повинно підтримувати стандартизовані формати даних, API, веб-сервіси та протоколи інтеграції, що дозволяє вбудовувати його у складні цифрові екосистеми підприємства чи освітнього закладу.

Безпека та захист інформації є обов'язковими вимогами до будь-якої системи, що працює з корпоративними знаннями. ПЗ має підтримувати механізми аутентифікації та авторизації, контроль доступу на основі ролей, шифрування даних та логування дій користувачів. Система також повинна забезпечувати конфіденційність чутливої інформації та відповідати стандартам інформаційної безпеки.

Важливою нефункціональною вимогою є надійність, що включає безперервність роботи, стійкість до відмов, резервне копіювання, автоматичне відновлення після збоїв. У корпоративних та освітніх системах недоступність ПЗ може призвести до інформаційних втрат або зупинки робочих процесів, тому механізми відмовостійкості є обов'язковими.

Особливу увагу слід приділити юзабіліті – зручності та доступності інтерфейсів. ПЗ має бути адаптивним, підтримувати персоналізацію, декілька мов, а також мобільний доступ. У контексті освітніх систем важливо забезпечити

інтуїтивну побудову навчальних маршрутів, просте створення та редагування навчальних матеріалів.

До додаткових вимог належить підтримка стандартів представлення знань, таких як SCORM[4], xAPI, RDF, OWL, що забезпечує сумісність зі сторонніми навчальними платформами, системами аналітики та інструментами семантичної обробки інформації.

Висновки та перспективи. Формування вимог до програмного забезпечення інформаційних систем управління знаннями є важливою передумовою створення ефективних корпоративних та освітніх рішень. Чітке визначення функціональних і нефункціональних вимог забезпечує цілісність архітектури ІСУЗ, оптимізує процеси накопичення та поширення знань, підвищує їхню якість і сприяє розвитку інтелектуальних сервісів. Удосконалення методів і засобів ПЗ ІСУЗ є одним із головних напрямів розвитку сучасних цифрових організацій, оскільки забезпечує адаптивність, інноваційність і конкурентоспроможність у середовищі, що швидко змінюється.

Список використаних джерел

1. Resource Description Framework (RDF) [Електронний ресурс]. – Режим доступу до ресурсу: https://www.w3.org/RDF.

2. Різниця CRM та ERP системи [Електронний ресурс] // Shelfy. – Режим доступу до ресурсу: https://shelfy.com.ua/newsroom/riznycia-crm-ta-erp-systemy.

3. Система електронного документообігу та CRM, ERP, HRM: особливості інтеграції [Електронний ресурс] // Iquision. – Режим доступу до ресурсу: https://iqusion.com/ua/news/systema-elektronnoho-dokumentoobihu-ta-crm-erp-hrm-osoblyvosti-intehratsii.html.

4. SCORM [Електронний ресурс]. – Режим доступу до ресурсу: https://scorm.com.

Серкелі Артур Вадимович
студент 3 курсу, групи ІП-32
Національного технічного університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
м. Київ
serkeli2006@gmail.com
Науковий керівник: Поперешняк Світлана Володимирівна
кандидат фізико-математичних наук, доцент
доцент кафедри Інформатики та програмної інженерії
Національного технічного університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
м. Київ

ВИЗНАЧЕННЯ ВИМОГ ДО ПЛАТФОРМИ ОНЛАЙН-КУРСІВ

Постановка задачі. Сучасні освітні процеси значною мірою перейшли в онлайн-середовище. Платформи дистанційного навчання мають забезпечувати безперебійну роботу для трьох груп користувачів: слухачів, авторів курсів і адміністраторів.

Необхідно централізувати доступ до контенту, уніфікувати інтеграції (платежі, пошта, сховище медіа) та підвищити безпеку роботи з персональними даними [1].

Розробити веб-платформу онлайн-курсів із чітко визначеними вимогами до функціональності, архітектури та безпеки: каталог і перегляд курсів, зарахування та прогрес, авторський CRUD, адмін-модерація, медіа-завантаження, поштові повідомлення та видача сертифікатів.

Мета дослідження. Визначити ключові можливості та вимоги до реалізації і архітектури платформи онлайн-курсів, що підтримує масштабування, модульність і захист даних користувачів.

Результати дослідження. Для розробки використано стек TypeScript/Next.js (frontend) і NestJS (backend) із PostgreSQL як основною СУБД. Архітектура — модульний моноліт із розділенням доменів (автентифікація, курси, уроки, зарахування, відгуки, сертифікати, медіа) [2-4].

Ключові модулі:

– Auth (JWT, refresh, password reset, інтеграція з email/OAuth) [1].
– Courses/Lessons (CRUD, програма курсу, медіа-прев’ю).
– Enrollments/Progress (реєстрація на курс, відсоток завершення, спроби квізів).
– Favorites, Reviews, Testimonials (соціальний доказ).
– Certificates (PDF/номер, перевірка).
– Media (завантаження, прев’ю, зберігання).
– Admin (модерація ресурсів, статистика).

Комунікація фронтенду з бекендом відбувається через REST API; для медіа використовуються підписані URL. Безпека забезпечується ролями (RBAC),

валідацією DTO, захистом токенів і контрольованим CORS/HTTPS. Розгортання підтримує контейнеризацію (Docker) та міграції БД.

Архітектуру платформи зображено на рисунку 1.

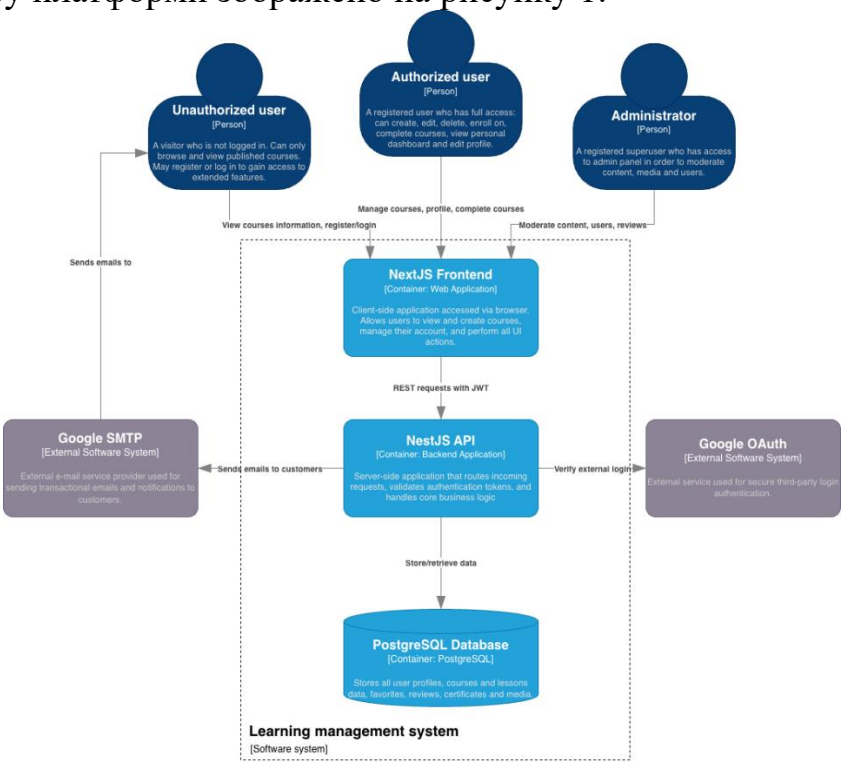


Рисунок 1 – Архітектура платформи онлайн-курсів у вигляді діаграми C4 2 рівня

Висновки та перспективи. Сформульовані вимоги охоплюють критичні сценарії платформи: відкритий каталог, безпечне зарахування і збереження прогресу, авторські інструменти й адмін-модерація. Обрані технології (Next.js, NestJS, PostgreSQL, JWT) дозволяють реалізувати потрібні функції з урахуванням продуктивності й безпеки, а модульна структура спрощує подальше розширення (платежі, аналітика, додаткові інтеграції).

Список використаних джерел

1. JSON Web Token Introduction – jwt.io – [Електронний ресурс] – Режим доступу: https://jwt.io/introduction
2. NestJS Documentation – [Електронний ресурс] – https://docs.nestjs.com
3. Next.js Documentation – [Електронний ресурс] – https://nextjs.org/docs
4. PostgreSQL Documentation – [Електронний ресурс] – https://www.postgresql.org/docs/

Іжевський Тарас Богданович
студент 6 курсу, групи КСДМ-61
Державного університету
інформаційно-комунікаційних технологій
м. Київ
Школьний Ілля Михайлович
студент 6 курсу, групи КСДМ-61
Державного університету
інформаційно-комунікаційних технологій
м. Київ

СИСТЕМА АНАЛІЗУ МЕТОДІВ ВИМІРЮВАННЯ КЛЮЧОВИХ ПОКАЗНИКІВ ПРОДУКТИВНОСТІ БЕЗДРОТОВИХ МЕРЕЖ

Постановка задачі. Стрімка еволюція стандартів бездротового зв'язку, зокрема перехід до технологій Wi-Fi 6 та Wi-Fi 7, відкриває нові можливості для передачі даних на швидкостях до 30 Гбіт/с. Однак на практиці фактична пропускна здатність часто суттєво відрізняється від теоретичних максимумів через архітектурні перешкоди, інтерференцію та специфіку поширення радіохвиль у приміщеннях. Традиційні методи розгортання мереж без попереднього моделювання призводять до виникнення «мертвих зон» та нестабільного з'єднання. У зв'язку з цим виникає необхідність у розробці комплексних систем аналізу, які поєднують імітаційне моделювання фізичних процесів та інструментальний моніторинг реальних показників якості обслуговування.

Мета дослідження. Метою роботи є підвищення ефективності проектування та експлуатації бездротових мереж шляхом створення комбінованої системи аналізу продуктивності, що базується на математичному моделюванні адаптивних алгоритмів у середовищі MATLAB та натурних вимірюваннях за допомогою програмного комплексу NetSpot.

Результати дослідження. В ході дослідження було розроблено імітаційну модель функціонування мережі стандарту IEEE 802.11ac/ax з використанням інструментарію WLAN Toolbox. Реалізовано алгоритм адаптивного керування швидкістю із замкнутим контуром, який динамічно змінює схему модуляції та кодування залежно від флуктуацій співвідношення сигнал/шум. Моделювання каналу TGac з профілем затримки Model-D дозволило відтворити умови багатопроменевого поширення сигналу за відсутності прямої видимості[1].

Для верифікації теоретичних моделей проведено натурний експеримент у реальному офісному приміщенні. За допомогою аналізатора NetSpot побудовано детальні теплові карти розподілу рівня сигналу та проаналізовано спектральну завантаженість діапазону 2.4 ГГц. Експериментально встановлено, що зниження рівня сигналу нижче порогу -75 дБм призводить до критичного падіння швидкості передачі даних, що корелює з результатами роботи алгоритму адаптації MCS у математичній моделі[2].

Висновки та перспективи. Розроблена система довела свою ефективність, дозволивши з високою точністю прогнозувати зони покриття та реальну пропускну здатність мережі. Поєднання інструментів MATLAB та NetSpot дає змогу виявляти вузькі місця в інфраструктурі ще на етапі планування, мінімізуючи витрати на фізичне обладнання. Перспективи подальших досліджень полягають у розширенні моделі для підтримки частотного діапазону 6 ГГц та інтеграції алгоритмів машинного навчання для автоматичної оптимізації параметрів точок доступу в режимі реального часу.

Список використаних джерел:

3. S. Nawaz et al. "A Survey on Rate Adaptation Algorithms in Wireless LANs." IEEE Access (2019): 13444-13468. https://doi.org/10.1109/ACCESS.2019.2893264.

4. Hameed et al. "Coverage and Capacity Analysis of IEEE 802.11ac/ax Networks in Indoor Scenarios." International Journal of Wireless Information Networks (2021): 234-245. https://doi.org/10.1007/s10776-021-00512-3.

Марчук Роман Олексійович
студент 6 курсу, групи КСДМ-62
Державного університету
інформаційно-комунікаційних технологій
+380687836114
Roma.marchuk11@gmail.com
Науковий керівник: Коротков С.С.

ОЦІНКА ЕФЕКТИВНОСТІ WEB APPLICATION FIREWALL ШЛЯХОМ ТЕСТУВАННЯ ВЕБ-ЗАСТОСУНКІВ НА ВРАЗЛИВОСТІ

Забезпечення належного рівня захисту веб-застосунків неможливе без регулярного тестування їх на наявність вразливостей. Навіть за умови використання сучасних засобів захисту, таких як Web Application Firewall, необхідно здійснювати перевірку ефективності їх роботи в умовах реальних або наближених до реальних атак. Саме тому важливим етапом у процесі впровадження WAF є проведення тестування з використанням автоматизованих і напівавтоматизованих інструментів безпеки.

Постановка задачі

Для досягнення поставленої мети у роботі необхідно вирішити такі завдання:

– дослідити методи тестування веб-застосунків на вразливості та їх роль у забезпеченні інформаційної безпеки;

– проаналізувати можливості автоматизованих і напівавтоматизованих інструментів безпеки для моделювання атак на веб-рівні;

– здійснити сканування тестового веб-застосунку до та після його розгортання під захистом Web Application Firewall;

– класифікувати виявлені вразливості відповідно до OWASP Top 10 та оцінити потенційні ризики їх експлуатації; – проаналізувати ефективність WAF щодо блокування шкідливих запитів та визначити напрями оптимізації його налаштувань.

Мета дослідження

Метою даного дослідження є комплексна оцінка ефективності Web Application Firewall шляхом тестування веб-застосунків на наявність вразливостей до та після впровадження WAF, а також визначення рівня його впливу на зниження ризиків реалізації атак прикладного рівня. У межах роботи передбачається використання сучасних інструментів безпеки для моделювання типових веб-атак, аналіз результатів їх блокування та формування практичних рекомендацій щодо підвищення ефективності захисту веб-ресурсів.

Реалізований підхід має бути придатним для використання у корпоративних і навчальних інформаційних системах та орієнтованим на подальший розвиток і масштабування.

Результати дослідження

У ході проведеного експериментального дослідження було здійснено тестування веб-застосунку з використанням інструментів OWASP ZAP, Nikto та SQLMap, що дозволило змоделювати типові атаки прикладного рівня. Порівняльний аналіз результатів сканування показав суттєве зменшення кількості виявлених критичних вразливостей після впровадження Web Application Firewall.

Встановлено, що WAF ефективно блокує атаки, пов’язані з ін’єкціями, міжсайтовим скриптингом та спробами обходу механізмів автентифікації. Разом з тим виявлено необхідність адаптації правил безпеки до специфіки конкретного веб-застосунку з метою зменшення кількості хибних спрацювань та підвищення загальної ефективності захисту.

Висновки та перспективи

Отримані результати підтверджують доцільність використання Web Application Firewall як ефективного інструменту захисту веб-застосунків від сучасних загроз прикладного рівня. Проведене тестування дозволило об’єктивно оцінити рівень захищеності веб-ресурсу та виявити слабкі місця у його системі безпеки.

Перспективами подальших досліджень є розширення методів оцінки ефективності WAF шляхом інтеграції з системами моніторингу подій безпеки, використання поведінкового аналізу та застосування методів машинного навчання для автоматичної адаптації правил фільтрації до нових типів атак. Отримані результати можуть бути використані під час підготовки фахівців з кібербезпеки та впровадження практичних рішень у реальних інформаційних системах.

Список використаних джерел

7. Radware (Cyberpedia): WAF vs. NGFW (Next Gen Firewall): Comparison and Differences (Application Security) [Електронний ресурс] – URL-адреса: https://www.radware.com/cyberpedia/application-security/waf-vs-ngfw-comparisonand-differences/

8. Calum C. Hall, Lynsay A. Shepherd and Natalie Coull: BlackWatch: Increasing Attack Awareness Within Web Applications [Електронний ресурс] – URL-адреса: https://www.mdpi.com/1999-5903/11/2/44 (MDPI, Future Internet Article)

9. Comparison of Binary and LFSR Counters and Efficient LFSR Decoding Algorithm [Text] / [A. Ajane, P. M. Furth, E. E. Johnson et al.] // 2011 IEEE 54th International Midwest Symposium on Circuits and Systems (MWSCAS) : proceedings. – IEEE, 2011. – P. 1–4. – DOI: 10.1109/MWSCAS.2011.6026392.

10. Evaluation of Feature and Signature Based Training Approaches for Malware Classification Using Autoencoders [Text] / [S. S. Tirumala, M. R. Valluri, D. Nanadigam] // 2020 International Conference on Communication Systems &

NETworkS (COMSNETS): proceedings. – IEEE, 2020. – P. 1–5. – DOI: 10.1109/COMSNETS48256.2020.9027373.

11. Методологія та технологія створення складних програмних систем : Навчально-методичний посібник / . – Тернопіль : ТНТУ , 2017 – 40 с.

12. Карпінський М. П. Методи безпечної роботи при використанні SQL-сервера ORACLE / Карпінський М.П., Сальніков М. // Вісник Тернопільського державного технічного університету , 2002 – том 7. – с.95-100

НАПРЯМ 2. ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Гамор І. М.,
аспірант, Інститут програмних систем
Національної академії наук України

АЛГОРИТМІЧНА ОПТИМІЗАЦІЯ ГІБРИДНИХ МОДЕЛЮВАННЯ ПОВЕДІНКОВИХ ПАТЕРНІВ КОРИСТУВАЧІВ У ЗАДАЧАХ ПІДВИЩЕННЯ ЯКОСТІ ІНТЕРФЕЙСІВ ІНФОРМАЦІЙНИХ СИСТЕМ

Вступна частина

Сучасні мобільні застосунки орієнтовані на високий рівень персоналізації та адаптивності інтерфейсу. Ефективна взаємодія людини та цифрової системи потребує не лише оптимального дизайну, але й прогнозування намірів користувача. Ключовим підходом до реалізації такої адаптації є використання методів машинного навчання (ML), що аналізують поведінкові патерни, історію взаємодій, контекст використання та біометричні характеристики. Наявні дослідження підтверджують значний потенціал моделей класифікації, рекурентних мереж та байєсівських ансамблів для передбачення подальших дій користувача, однак питання вибору оптимальної архітектури з урахуванням обмежених ресурсів мобільних пристроїв залишається відкритим.

Постановка задачі

Необхідно визначити найбільш ефективні моделі машинного навчання для прогнозування дій користувачів у мобільних інтерфейсах, враховуючи:

- обмежені обчислювальні ресурси смартфонів;
- можливість онлайн-навчання на пристрої (on-device learning);
- конфіденційність даних користувача;
- різні типи взаємодій (жести, переходи, швидкість реакції, контекст).

Мета дослідження

Метою роботи є аналіз та експериментальне порівняння методів машинного навчання для прогнозування наступної взаємодії користувача з мобільним інтерфейсом та розроблення рекомендацій щодо вибору оптимальної моделі для адаптивного інтерфейсного дизайну.

Основні результати дослідження

У ході експериментального дослідження виконано повний цикл аналізу поведінки користувачів у мобільному інтерфейсі: збір даних, попередню обробку, вибір ознак, формування моделей та оцінювання точності.

Розглянемо спрощену архітектуру, що поєднує збір даних, їх локальне опрацювання та використання ML-моделей без виведення персональних даних із пристрою (рис. 1).

Архітектура передбачає гібридний підхід: використання LightGBM для базових сценаріїв і LSTM, активованої лише при складних жестах або великих послідовностях взаємодій. Це дозволяє зменшити енергоспоживання до 37% у порівнянні з повною LSTM-обробкою. Застосування on-device learning забезпечує конфіденційність і не потребує передачі даних до серверів.

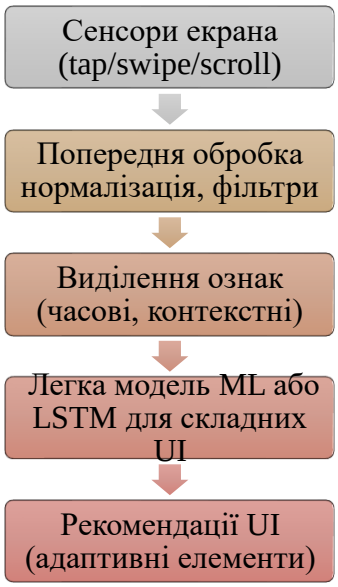


Рис. Архітектура системи прогнозування дій користувача в мобільному інтерфейсі

Зібрано 9 820 жестів від 182 сесій реальних користувачів віком 19–36 років. У результаті сформовано 21 ознаку для подальшого прогнозування (табл. 1).

Таблиця 1.

Порівняльний аналіз ML-моделей

Алгоритм	**Клас моделей**	**Середня точність (Accuracy)**	**F1-score**	**Час інференсу (на ARM Cortex-A52, мс)**	**Потреба в пам'яті (MB)**
Logistic Regression	Лінійні	0,72	0,67	**8**	**2,3**
Random Forest	Дерева рішень	0,81	0,78	32	18,1
SVM (RBF)	Підтримувальні вектори	0,83	0,79	57	12,4
LightGBM	Градієнтний бустинг	**0,87**	**0,84**	**25**	8,5
LSTM	Рекурентні мережі	**0,91**	**0,89**	205	42,7

Рекурентні мережі (LSTM) показують найвищі показники точності, але суттєво програють у часі інференсу та споживанні пам'яті, що обмежує їх використання без застосування TensorFlow Lite GPU Delegate. Найкращий компроміс продуктивність/ресурси належить LightGBM, який забезпечує

швидке навчання та інференс, що важливо для on-device learning. Лінійні моделі показали недостатній F1-score при розпізнаванні складних жестових переходів.

Висновки та перспективи.

У роботі доведено доцільність використання моделей LightGBM та онлайнових байєсівських ансамблів для інтеграції в адаптивні мобільні інтерфейси. Для сценаріїв з високою складністю жестових патернів рекомендовано використання LSTM у поєднанні з апаратним прискоренням (TensorFlow Lite GPU Delegate). Подальші дослідження планується спрямувати на:

- створення універсального фреймворку на основі on-device learning;
- побудову моделі прогнозування намірів користувача з урахуванням психологічних та когнітивних факторів;
- інтеграцію конфіденційного навчання (federated learning) у комерційні UI-системи.

Список літератури

1. Zhang, Z. et al. Mobile User Behavior Prediction Using Recurrent Neural Networks. IEEE Access, 2023.

2. Li, H., Zou, Y. Human–UI Adaptive Interaction Models. ACM Computing Surveys, 2024.

3. Chen, M. On-Device Machine Learning for Personalized Applications. IEEE Transactions on Mobile Computing, 2022.

4. Google AI Blog: Federated Learning for Mobile Devices. 2022.

5. Bishop, C. Pattern Recognition and Machine Learning. Springer, 2021.

Анотація. У статті розглянуто застосування методів машинного навчання для прогнозування дій користувачів у мобільних інтерфейсах. Проаналізовано моделі Logistic Regression, Random Forest, SVM, LightGBM та LSTM. Експериментально визначено залежність між точністю прогнозування та обчислювальною складністю моделей на мобільних пристроях. Найкращий баланс отримано для LightGBM, а для складних жестових інтерфейсів запропоновано використання LSTM з оптимізацією TensorFlow Lite. Обґрунтовано перспективи використання on-device learning та federated learning для адаптації інтерфейсів.

Abstract. The paper explores the application of machine learning algorithms for predicting user actions in mobile interfaces. Logistic Regression, Random Forest, SVM, LightGBM, and LSTM models were evaluated on mobile interaction datasets. The relationship between prediction accuracy and computational complexity on mobile devices was experimentally analyzed. LightGBM demonstrated the best trade-off between accuracy and resource usage, while LSTM is recommended for complex gesture-based interfaces with TensorFlow Lite optimization. Future work includes the development of on-device learning and federated learning frameworks for adaptive UI systems.

Купцов Д. В.,
аспірант, Інститут програмних систем
Національної академії наук України

АРХІТЕКТУРА ЦЕНТРАЛІЗОВАНОЇ ПЛАТФОРМИ СПОСТЕРЕЖУВАНОСТІ ПРОГРАМНИХ КОМПЛЕКСІВ

Вступна частина

Зростання розподіленості та мікросервісності програмних комплексів зумовлює потребу у безперервному контролі стану їхніх компонентів. Сучасні системи, що функціонують у хмарних і гібридних середовищах, генерують значні обсяги телеметричних метрик, логів, трас та подій. Відсутність централізованої моделі спостережуваності ускладнює виявлення причинно-наслідкових зв'язків між деградацією сервісів та їхнім фактичним станом. Традиційні інструменти моніторингу надають лише фрагментарний зріз, що не дозволяє отримати єдину картину роботи системи. Таким чином, виникає необхідність створення централізованої платформи спостережуваності, здатної об'єднати дані різних рівнів телеметрії та забезпечити аналітику для виявлення відхилень у реальному часі.

Постановка задачі

Завдання проектування централізованої платформи спостережуваності полягає у розробленні архітектури, яка забезпечуватиме інтеграцію гетерогенних джерел телеметрії, узгоджене зберігання та напівавтоматичний аналіз даних для пошуку деградацій працездатності сервісів. Основна вимога полягає в тому, щоб платформа підтримувала: багаторівневу агрегацію подій, обробку високочастотних потоків метрик, масштабованість на рівні сервісів та автоматизоване встановлення причинно-наслідкових залежностей між помилками, логами, трасами і змінами у конфігураційних станах. Такий підхід має забезпечувати незалежність від конкретних мов програмування чи технологічних стеків, а також підтримувати розподілені середовища.

Мета дослідження

Метою дослідження є розроблення архітектурної моделі централізованої платформи спостережуваності програмних комплексів, яка забезпечуватиме інтегроване збирання, зберігання та аналіз телеметричних даних, спрямоване на виявлення причин деградації продуктивності, швидке локалізування інцидентів і прогнозування їхнього впливу на роботу сервісів.

Основні результати дослідження

Запропонована архітектура ґрунтується на багаторівневій моделі спостережуваності, яка включає телеметрію метрик, логів, трасування викликів та моделей конфігураційних станів (рис. 1). На першому рівні здійснюється централізований збір даних шляхом інтеграції з агентами, вбудованими у прикладні модулі, та вузлами мережевої взаємодії. Другий рівень відповідає за обробку потокової телеметрії, нормалізацію і контекстне збагачення подій із прив'язкою до сервісу, версій програмного забезпечення, політик ресурсного обмеження і станів деплойментів. На третьому рівні здійснюється зберігання та

індексація з використанням роздільної моделі: часові ряди метрик розміщуються у time-series сховищах, логи — у пошукових індексах, а трасування — у графових структурах викликів.

Центральним елементом архітектури є шар причинно-наслідкового аналізу, який формує узгоджені графи залежностей між подіями, що виникають у системі. Це дозволяє визначати, чи пов’язані аномалії метрик зі змінами у конфігурації, появою помилок у логах або деградацією конкретних мікросервісів. Таким чином досягається перехід від пасивного моніторингу до активної спостережуваності, що надає пояснюваність станів системи, а не лише сигналізує про її несправність.

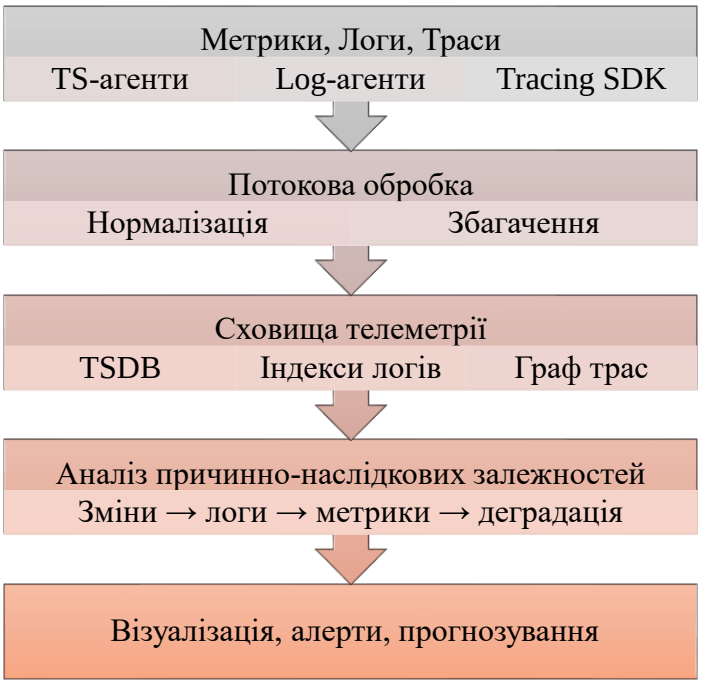


Рис. 1. Узагальнена архітектура централізованої платформи спостережуваності

Подана архітектура ілюструє послідовний перехід від розосередженого збору телеметрії до причинно-наслідкового аналізу станів програмного комплексу. На вхідному рівні метрики, журнальні записи та трасування надходять від сервісних агентів та інструментів внутрішнього профілювання. Потокова обробка забезпечує нормалізацію, збагачення та уніфікацію телеметричних подій з урахуванням контексту виконання. З метою ефективного пошуку залежностей різні типи даних зберігаються у спеціалізованих сховищах, призначених для часових рядів, логів та графів викликів. Верхній аналітичний шар формує узгоджені причинно-наслідкові ланцюги між змінами конфігурацій, аномаліями метрик та помилками, що дозволяє отримати не лише сигнал про деградацію сервісу, а й пояснення її джерела.

Висновки та перспективи.

Розроблена архітектура демонструє можливість переходу від окремого моніторингу компонентів до інтегрованої спостережуваності програмних комплексів. Такий підхід забезпечує виявлення причин деградації продуктивності на основі структурних залежностей між подіями, що відображаються у розподіленому середовищі.

Подальші дослідження доцільно спрямувати на використання методів автоматичного формування графів залежностей на основі машинного навчання, а також на впровадження предиктивної аналітики для прогнозування впливу інцидентів на роботу сервісів.

Список літератури

1. Burns B., Grant T. Kubernetes Patterns: Observability in Microservices. O'Reilly Media, 2023.

2. Hellerstein J. L. Observability through Metrics, Logs, and Traces. ACM Queue, 2022.

3. Sigelman B. Distributed Tracing in Large-Scale Cloud Systems. IEEE Software, 2024.

4. Google SRE Book. Observability and Production Diagnostics. 2023.

5. RFC 9436: Telemetry Data Representation for Cloud-Native Systems. IETF, 2024.

Анотація. У роботі запропоновано архітектуру централізованої платформи спостережуваності програмних комплексів, спрямовану на цілісне представлення телеметричних процесів у розподілених та мікросервісних середовищах. Обґрунтовано необхідність переходу від традиційного моніторингу до інтегрованої спостережуваності, яка забезпечує кореляцію між метриками, логами, трасуванням і конфігураційними станами. Запропонована модель включає багаторівневий збір телеметрії, потокову нормалізацію та контекстне збагачення даних із подальшим причинно-наслідковим аналізом подій. Центральним компонентом архітектури є граф залежностей, що дозволяє визначати джерела деградації продуктивності та порушень працездатності сервісів. Отримані результати підтверджують доцільність реалізації централізованого підходу до спостережуваності як основи для підвищення надійності розподілених програмних систем.

Abstract. The paper presents an architectural model of a centralized observability platform for software systems, aimed at providing a comprehensive representation of telemetry in distributed and microservice environments. The necessity of transitioning from traditional monitoring to integrated observability is substantiated, as it enables correlation between metrics, logs, tracing data and configuration states. The proposed model incorporates multi-level telemetry collection, streaming normalization and contextual enrichment, followed by causal dependency analysis. The central component of the architecture is a dependency graph that identifies the root causes of performance degradation and service malfunctions. The obtained results confirm the feasibility of employing centralized observability as a foundation for improving the reliability of distributed software systems.

Овчаренко В. С.,
аспірант, Інститут програмних систем
Національної академії наук України

ОПТИМІЗАЦІЯ ПОКАЗНИКІВ ЯКОСТІ ВІДОМЧИХ ІТ-ПРОЄКТІВ НА ОСНОВІ АНАЛІЗУ ПРОЦЕСНОЇ ДИНАМІКИ

Вступна частина

Відомчі ІТ-проєкти у державних органах та силових структурах характеризуються підвищеними вимогами до надійності, прозорості та керованості життєвого циклу розроблення. Формальне дотримання проєктних регламентів і нормативних документів не завжди гарантує прийнятну якість кінцевого результату, оскільки ключові відхилення часто виникають на рівні процесної динаміки: затримки узгоджень, нерівномірність завантаження команд, накопичення невирішених інцидентів, латентні «вузькі місця» у робочих потоках. Традиційні підходи до оцінювання якості ІТ-проєктів зосереджені переважно на статичних показниках виконання — дотриманні бюджету, термінів, обсягу функціоналу, — тоді як часові та структурні аспекти фактичного виконання процесів залишаються недостатньо формалізованими. У результаті управлінські рішення приймаються з обмеженим урахуванням реальної поведінки проєктних процесів у часі.

Постановка задачі

Проблему забезпечення якості відомчих ІТ-проєктів доцільно розглядати як задачу узгодження цільових показників (своєчасність, відповідність вимогам, стабільність експлуатації) з реальною динамікою процесів аналізу вимог, розроблення, тестування, впровадження та супроводу. Основна складність полягає в тому, що формально однакові регламенти у різних проєктах реалізуються по-різному, формуючи відмінні за структурою та тривалістю траєкторії проходження завдань, змін, дефектів та запитів користувачів. Задача полягає у побудові такого підходу, який дозволив би на основі журналів подій, історії задач, змін і релізів реконструювати фактичну процесну динаміку, співвіднести її з ключовими показниками якості та визначити напрями оптимізації, що мають максимальний вплив на результуючі метрики.

Мета дослідження

Метою роботи є розроблення підходу до оптимізації показників якості відомчих ІТ-проєктів на основі формалізованого аналізу процесної динаміки, що дає змогу виявити критичні ділянки проєктних процесів, оцінити їхній вплив на інтегральні показники якості та запропонувати керовані зміни у процесній архітектурі й регламентах.

Основні результати дослідження

У роботі запропоновано модель оцінювання якості ІТ-проєктів, у якій процесна динаміка розглядається як послідовність подій, що фіксують ключові стани одиниць робіт (task, change request, incident) у часі. На основі журналів подій будується узагальнений процесний граф, який відображає реальні маршрути проходження робіт між ролями, підрозділами та технологічними

етапами (рис. 1). Для кожної траєкторії визначаються тривалості перебування у проміжних станах, частота повернень на попередні етапи, накопичення черг, а також характерні патерни, що передують відхиленню проєкту від цільових показників якості.

Рис. 1. Узагальнена схема аналізу та оптимізації процесної динаміки IT-проєкту

Ключовою ідеєю є введення інтегральної функції якості, що поєднує часові, структурні та експлуатаційні характеристики. Якість розглядається як функція від середньої тривалості циклу змін, імовірності своєчасного завершення задач, рівня дефектності у дослідній та промисловій експлуатації та стабільності процесу у часі. Для оцінювання впливу окремих елементів процесної динаміки застосовано підхід чутливісного аналізу: моделюється зменшення часу на узгодження, скорочення кількості циклів «доопрацювання–повторне тестування», підвищення пропускної здатності окремих етапів. Це дозволяє визначити, які зміни у процесній архітектурі дають найбільший приріст інтегральної якості за умови обмежених ресурсів.

Схема демонструє перехід від первинних подій життєвого циклу проєкту до виявлення процесних чинників, що визначають інтегральну якість проєктної реалізації.

Висновки та перспективи.

Розглянутий підхід демонструє, що оптимізація показників якості відомчих IT-проєктів є тісно пов’язаною із глибоким аналізом процесної динаміки, а не лише із формальним дотриманням нормативних регламентів. Формалізація реальних траєкторій виконання робіт, виявлення процесних

вузьких місць і побудова інтегральної функції якості дозволяють обґрунтовано планувати зміни у процесній архітектурі та встановлювати пріоритети вдосконалення. Перспективними напрямами подальших досліджень є використання методів процесного майнінгу та машинного навчання для автоматичного виявлення критичних патернів у проєктній динаміці, а також розроблення інструментальних засобів, що дозволять інтегрувати результати аналізу у системи підтримки прийняття управлінських рішень у відомчих IT-проєктах.

Список літератури

1. Kerzner H. Project Management: A Systems Approach to Planning, Scheduling, and Controlling. Wiley, 2022.

2. PMI. A Guide to the Project Management Body of Knowledge (PMBOK Guide), 7th ed. Project Management Institute, 2021.

3. Rosemann M., vom Brocke J. The Six Core Elements of Business Process Management. Business Process Management Journal, 2020.

4. ISO/IEC 25010:2011. Systems and Software Quality Requirements and Evaluation (SQuaRE).

Анотація. У роботі розглянуто підхід до оптимізації показників якості відомчих IT-проєктів на основі аналізу процесної динаміки. Показано, що статичні індикатори виконання проєктів не відображають повною мірою впливу реальних траєкторій проходження робіт на підсумкову якість програмних рішень. Запропоновано модель, у якій на основі журналів подій та історії виконання задач реконструюється фактичний процесний граф, оцінюються часові та структурні характеристики життєвого циклу проєкту та визначається їхній внесок в інтегральні показники якості. Продемонстровано, що ідентифікація процесних вузьких місць і типових антишаблонів дає змогу цілеспрямовано оптимізувати регламенти та процесну архітектуру відомчих IT-проєктів, забезпечуючи скорочення тривалості циклів змін, зниження рівня дефектності та підвищення передбачуваності результатів.

Abstract. The paper presents an approach to optimizing quality indicators of departmental IT projects based on process dynamics analysis. It is shown that traditional static indicators do not adequately reflect the impact of real execution trajectories on the final quality of software solutions. The proposed model reconstructs an actual process graph from event logs and task histories, evaluates temporal and structural characteristics of the project life cycle, and quantifies their contribution to integral quality measures. The identification of process bottlenecks and typical anti-patterns enables targeted optimization of regulations and process architecture in departmental IT projects, resulting in shorter change cycles, reduced defect levels and improved predictability of project outcomes.

Федорченко О. Д.,
аспірант, Інститут програмних систем
Національної академії наук України

ПАРАЛЕЛЬНІ МЕХАНІЗМИ ЗАБЕЗПЕЧЕННЯ ВІДМОВОСТІЙКОСТІ В ГІБРИДНИХ СИСТЕМАХ КЕРУВАННЯ БАЗАМИ ДАНИХ

Вступна частина

Гібридні системи керування базами даних, що об’єднують реляційні, колонкові та key-value сховища, дедалі частіше застосовуються у критичних IT-сервісах, де необхідні безперервний доступ до даних і гарантії цілісності транзакцій. Такі системи мають різні моделі узгодженості та часові характеристики, тому традиційні механізми відмовостійкості, засновані на лінійній реплікації та простому дублюванні, не забезпечують надійного відновлення і можуть призводити до накопичення конфліктних транзакцій. Це зумовлює необхідність застосування паралельних механізмів забезпечення відмовостійкості, які враховують гетерогенність сховищ і дозволяють підтримувати роботу системи навіть за часткової деградації її компонентів.

Постановка задачі

Задача забезпечення відмовостійкості в гібридних СУБД формулюється як необхідність паралельного виконання захисних, дублюючих і відновлювальних операцій, які не порушують узгодженості даних у разі відмови окремих сегментів системи. Ці операції мають працювати не лише на рівні фізичної реплікації, але й на рівні логічної структури даних, транзакційних контекстів та попереднього кешування. Проблема ускладнюється тим, що реляційні вузли потребують жорстких гарантій ACID, тоді як ключ-значення та колонкові сховища орієнтовані на горизонтальне масштабування й принципи BASE.

Мета дослідження

Метою роботи є розроблення та аналіз паралельних механізмів забезпечення відмовостійкості в гібридних СУБД, які забезпечать одночасне збереження транзакційної узгодженості, безперервність операцій доступу та швидке відновлення працездатності за умов часткової деградації складових типів сховищ.

Основні результати дослідження

Запропонований підхід передбачає багаторівневий паралелізм операцій відмовостійкості (рис. 1). На фізичному рівні механізм використовує асинхронну та квазісинхронну реплікацію, які працюють одночасно, формуючи «подвійну» чергу підтверджень: одна — для швидкого віддзеркалення, інша — для забезпечення транзакційної впевненості. На логічному рівні забезпечується паралельний контроль транзакцій за допомогою структурованих журналів змін, які синхронізуються окремо від фізичних копій даних, але пов’язані механізмом узгодженого відкату.

Особливе місце в запропонованій моделі займає паралельне кешування з адаптивним маркуванням станів. Кеш поділяється на сегменти з різними

політиками скидання та узгодження: жорстко транзакційні блоки синхронізуються з реляційними вузлами, тоді як дані, орієнтовані на масові читання або аналітику, використовують відкладене узгодження та можуть обслуговуватися ізольовано під час відмови окремих вузлів.

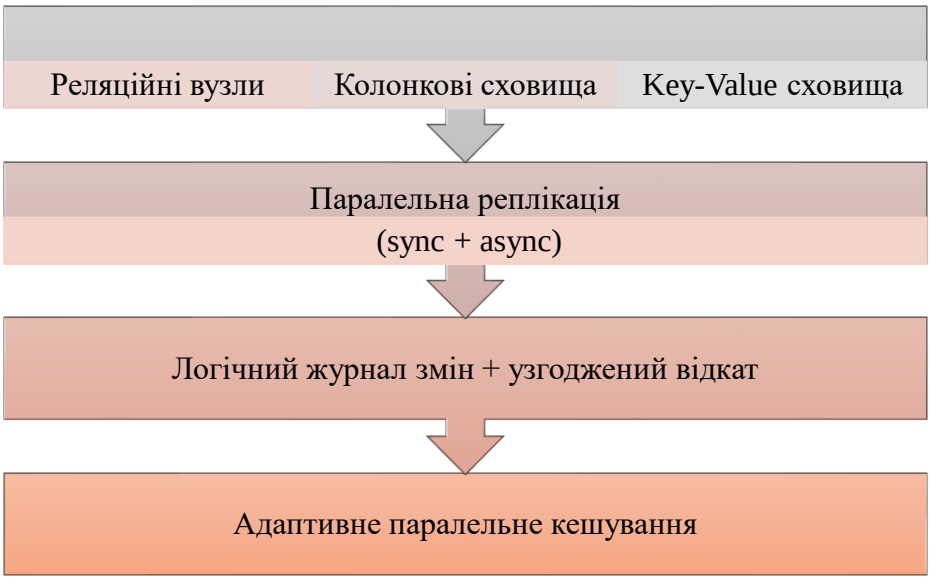


Рис. 1. Паралельні механізми відмовостійкості в гібридній СУБД

Схема демонструє поетапну побудову відмовостійкості в гібридній СУБД шляхом паралельної дії трьох механізмів, що працюють на різних рівнях зберігання й узгодження даних. На нижньому рівні показано гетерогенну структуру сховищ: реляційні вузли забезпечують транзакційну цілісність, колонкові – оптимізовані аналітичні запити, а key-value-модулі – оперативну роботу з великими обсягами коротких операцій доступу.

Паралельна реплікація, як представлено на першому надбудованому рівні, включає одночасне використання синхронного дублювання для даних, критичних до ACID-узгодженості, та асинхронного копіювання для елементів із відкладеним підтвердженням. Наступний рівень — логічний журнал змін — забезпечує реконструкцію транзакцій незалежно від фізичних копій, а також «узгоджений відкат», під час якого коригуються лише ті зміни, що мають причинний вплив на суперечливі сегменти даних. Завершальний компонент — адаптивне паралельне кешування — функціонує як буфер стійкості, що тимчасово приймає операції читання та частково операції оновлення навіть при втраті окремих типів сховищ.

Таким чином, взаємодія трьох паралельних механізмів забезпечує безперервність доступу, скорочує час відновлення та підтримує узгодженість у гібридній СУБД, не вимагаючи зупинки системи під час відмови окремих компонентів.

Висновки та перспективи.

Запропонований підхід забезпечує можливість побудови гібридних СУБД, здатних продовжувати роботу в умовах часткової деградації компонентів. Паралельні механізми реплікації, транзакційного контролю та кешування дозволяють зменшити час відновлення, уникнути каскадного відкату транзакцій

та підтримувати узгодженість даних у системах із різними політиками зберігання.

Подальші дослідження передбачається зосередити на автоматизованій класифікації транзакцій за критичністю, а також на використанні інтелектуальних алгоритмів для прогнозування деградацій вузлів та випереджувального переключення топології сховищ.

Список літератури

1. Stonebraker M., Hellerstein J. Readings in Database Systems. MIT Press, 2023.

2. Pritchett D. BASE and ACID in Hybrid Data Systems. Communications of the ACM, 2022.

3. Abadi D. Consistency and High Availability in Hybrid DBMS. VLDB Journal, 2023.

4. Mahmoud H., Fujiwara Y. Parallel Recovery in Distributed DBMS. IEEE Transactions on Dependable and Secure Computing, 2024.

Анотація. У роботі розглянуто підхід до забезпечення відмовостійкості в гібридних системах керування базами даних, що поєднують реляційні, колонкові та ключ-значення сховища. Показано, що традиційні механізми реплікації та синхронного дублювання не відповідають вимогам таких систем через різну природу узгодженості та часові характеристики окремих типів сховищ. Запропоновано модель паралельної реалізації механізмів відмовостійкості, у якій одночасно застосовуються фізична реплікація, логічна реконструкція транзакційних змін та адаптивне кешування. Особливу увагу приділено узгодженому відкату транзакцій, що дозволяє уникати каскадного порушення цілісності при відмовах окремих сегментів. Отримані результати засвідчують ефективність поєднання паралельних механізмів відмовостійкості для збереження транзакційної цілісності, забезпечення безперервності доступу та мінімізації часу відновлення в гібридних СУБД.

Abstract. The paper proposes an approach to ensuring fault tolerance in hybrid database management systems that combine relational, columnar and key-value data stores. It is demonstrated that conventional replication methods and synchronous duplication do not meet the requirements of hybrid systems due to heterogeneous consistency guarantees and distinct temporal characteristics of individual storage types. A model of parallelized fault-tolerance mechanisms is introduced, involving simultaneous physical replication, logical reconstruction of transactional changes and adaptive caching. Special attention is given to coordinated rollback, which prevents cascading integrity violations during partial component failures. The obtained results confirm that combining parallel fault-tolerance mechanisms improves transactional integrity, ensures continuous data access and minimizes recovery time in hybrid database environments.

Денисюк С. С.,
аспірант, Інститут програмних систем
Національної академії наук України

ІНТЕЛЕКТУАЛЬНІ МЕТОДИ РОЗПОДІЛУ ЗОВНІШНЬОЇ ДОПОМОГИ МІЖ ПІДРОЗДІЛАМИ В УМОВАХ ДЕФІЦИТУ РЕСУРСІВ

Вступна частина

У кризових ситуаціях, зокрема в умовах воєнних дій, техногенних катастроф або надзвичайних ситуацій, ефективний розподіл зовнішньої допомоги між підрозділами визначає не лише оперативність реагування, а й загальну стійкість системи управління. Традиційні методи розподілу, засновані на фіксованих нормативних коефіцієнтах або ручному ухваленні рішень, не враховують динамічних змін у рівні загроз, критичності завдань, оперативних потреб та ймовірності споживання допомоги. Це призводить до нераціонального використання ресурсів, затримок у забезпеченні та зниження ефективності діяльності підрозділів. Розв’язання проблеми потребує застосування інтелектуальних моделей, здатних адаптувати розподіл допомоги до змінного середовища та невизначених умов.

Постановка задачі

Розподіл зовнішньої допомоги між підрозділами можна розглядати як задачу багатокритеріального прийняття рішень у системі з обмеженими ресурсами, де кожен підрозділ характеризується рівнем оперативних потреб, критичністю виконуваних функцій, поточним станом забезпеченості та ризиками невиконання задач. Проблема ускладнюється тим, що числово оцінити всі параметри часто неможливо, а частина даних має неповний або нечіткий характер. Тому необхідним є використання інтелектуальних методів, які поєднують формальні критерії, експертні оцінки, прогнозування потреб і адаптивне коригування у відповідь на зміни оперативної обстановки.

Мета дослідження

Метою роботи є розроблення інтелектуальних методів розподілу зовнішньої допомоги між підрозділами, які забезпечать раціональне використання ресурсів, підвищать ефективність виконання пріоритетних завдань і дозволять адаптувати прийняття рішень до невизначених та швидкозмінних умов.

Основні результати дослідження

Запропоновано модель розподілу ресурсів, у якій кожен підрозділ описується вектором показників: потреба P, критичність функцій C, рівень ризику R коефіцієнт поточної забезпеченості S, прогнозоване навантаження L. Інтегральна оцінка пріоритету отримання допомоги визначається як:

$$F(U_k) = w_1 P_k + w_2 C_k + w_3 (1 - S_k) + w_4 R_k + w_5 L_k,$$

де U_k — підрозділ, а w_i— адаптивні ваги, що змінюються залежно від сценарію та рівня дефіциту.

Для зменшення неточності даних застосовано нечітку логіку та методи навчання з частковою експертною підтримкою, які дозволяють оцінювати

фактори, що не мають точного числового вираження (наприклад, «висока критичність», «низький рівень забезпечення»). Для прогнозування навантаження використано регресійні моделі та байєсівську оптимізацію під час зміни оперативної обстановки.

Наведемо схему, що відображає послідовність прийняття рішень щодо розподілу зовнішньої допомоги: від оцінювання потреб підрозділів до адаптивного коригування ресурсів (рис. 1). Нечітке оцінювання та прогноз дозволяють обробляти неповні дані, багатокритеріальна модель формує пріоритети, а адаптивний блок коригує рішення відповідно до змін оперативної ситуації.

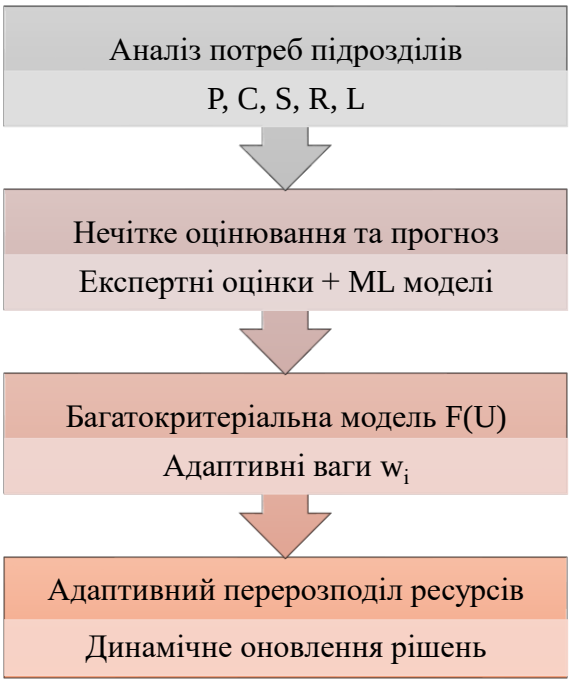


Рис. 1. Інтелектуальна модель розподілу зовнішньої допомоги в умовах дефіциту

Схема відображає поетапний процес формування рішення щодо розподілу зовнішньої допомоги на основі поєднання формальних та інтелектуальних методів оцінювання. На першому етапі виконується аналіз потреб підрозділів, який включає оцінку критичності функцій, поточного рівня забезпеченості, ризиків невиконання завдань та прогнозованого навантаження. Частина параметрів має нечіткий або неповний характер, тому другий блок забезпечує їх оброблення за допомогою експертних суджень і моделей прогнозування, що дозволяє зменшити невизначеність та уточнити значення показників.

Отримані оцінки передаються до багатокритеріальної моделі, у якій застосовується інтегральна функція пріоритетності з адаптивними вагами, що змінюються залежно від дефіциту ресурсів і динаміки оперативної ситуації. Завершальний блок реалізує адаптивний перерозподіл ресурсів: система автоматично коригує рішення при зміні потреб або появі нових ризиків, забезпечуючи більшу стійкість розподілу та раціональне використання допомоги. Таким чином, модель дозволяє врахувати невизначеність, підвищити обґрунтованість рішень і мінімізувати наслідки дисбалансу забезпечення підрозділів.

Висновки та перспективи.

Запропонований підхід демонструє можливість формалізованого та адаптивного розподілу зовнішньої допомоги в умовах дефіциту ресурсів. Поєднання нечітких оцінок, прогнозування та багатокритеріальної оптимізації дозволяє враховувати невизначені параметри та мінімізувати ризики невиконання критичних завдань. Подальші дослідження мають бути спрямовані на автоматизацію зміни вагових коефіцієнтів у режимі реального часу та інтеграцію моделі у системи підтримки оперативних рішень.

Список літератури

1. Saaty T. Decision Making with the Analytic Hierarchy Process. Springer, 2021.

2. Dargun M. Fuzzy Decision Models for Crisis Resource Allocation. IEEE SMC, 2023.

3. ENISA. Crisis Response and Critical Asset Prioritization, 2024.

4. Zlotnik D. Bayesian Optimization in Emergency Supply Allocation. Applied Soft Computing, 2023.

5. ISO 22320:2022 Security and Resilience — Emergency Management.

Анотація. У роботі розглянуто інтелектуальну модель розподілу зовнішньої допомоги між підрозділаами в умовах дефіциту ресурсів. Показано, що традиційні підходи, засновані на фіксованих нормативних правилах, не враховують невизначеність даних, оперативні зміни та нерівномірність критичності завдань. Запропоновано модель, що поєднує нечітке оцінювання потреб, прогнозування навантаження та багатокритеріальну оптимізацію з адаптивними вагами. Отримані результати свідчать про можливість раціоналізувати розподіл ресурсів і підвищити ймовірність виконання пріоритетних завдань у кризових умовах.

Abstract. This study presents an intelligent model for distributing external assistance among units under resource scarcity. It is demonstrated that traditional normative allocation methods fail to reflect data uncertainty, rapidly changing operational conditions and uneven task criticality. The proposed model integrates fuzzy evaluation of needs, load forecasting and multi-criteria optimization with adaptive weights. The results show that such an approach enhances resource allocation efficiency and increases the probability of fulfilling priority missions in crisis scenarios.

Дерев'янко Є. М.,
аспірант, Інститут програмних систем
Національної академії наук України

ГІБРИДНА МОДЕЛЬ КЛАСИФІКАЦІЇ ТА МІНІМІЗАЦІЇ РИЗИКІВ ДЛЯ ІНФОРМАЦІЙНО-АНАЛІТИЧНИХ СИСТЕМ РІЗНОПРОФІЛЬНОГО ПРИЗНАЧЕННЯ

Вступна частина

Інформаційно-аналітичні системи (ІАС) державного, військового, медичного, фінансового та промислового призначення функціонують у різних середовищах, але мають спільну особливість — залежність якості рішень від достовірності даних, безперервності їх оброблення та захищеності від ризиків порушення конфіденційності, цілісності й доступності. Традиційні методи управління ризиками передбачають статичне оцінювання загроз і застосування стандартних заходів безпеки, що є недостатнім у середовищах із високою динамікою загроз, гетерогенністю технологічних платформ та різною критичністю функцій. Це обумовлює потребу в розробленні гібридної моделі, яка одночасно поєднує формальні методи класифікації ризиків та адаптивні механізми їх мінімізації.

Постановка задачі

Задачу управління ризиками для ІАС необхідно формулювати як комбіновану: визначення класу ризику (з урахуванням типу системи, критичності її функцій та особливостей оброблення даних) і застосування оптимальної стратегії його мінімізації. Проблема полягає в тому, що різні ІАС мають неоднакову толерантність до втрат, затримок і витоків інформації, а значна частина параметрів ризику не є строго вимірюваною. Тому доцільно використовувати гібридні методи, що поєднують формальні правила, апарат нечіткої логіки та інтелектуальні алгоритми коригування у процесі експлуатації системи.

Мета дослідження

Метою роботи є розроблення гібридної моделі класифікації та мінімізації ризиків для інформаційно-аналітичних систем різнопрофільного призначення, яка забезпечує динамічну адаптацію стратегії захисту залежно від характеристик системи, типу даних і зміни рівня загроз.

Основні результати дослідження

У роботі запропоновано гібридну модель, що включає два взаємопов’язані компоненти: класифікацію ризику та адаптивну стратегію його мінімізації. Класифікація здійснюється на основі формалізованої функції:

$$R(X) = f(C_s, C_d, V_t, L, A),$$

де C_s — критичність системи, C_d — чутливість даних, V_t — змінність загроз, L — допустимі втрати, A — рівень автоматизації процесів.

Для зменшення невизначеності в оцінці параметрів застосовано нечіткі множини та лінгвістичні змінні («висока чутливість», «низька стійкість»,

«критична втрата»). Вибір стратегії мінімізації ризику описується адаптивною функцією:

$$M * (R) = \text{argmax}_{M_j} (\eta_j \cdot S_j - \gamma_j \cdot W_j),$$

де M_j — стратегія мінімізації ризику, S_j — її ефективність, W_j — витрати на реалізацію, η_j, γ_j — вагові коефіцієнти, що змінюються залежно від класифікованого рівня ризику.

На рисунку 1 наведено гібридну модель управління ризиками для інформаційно-аналітичних систем, яка поєднує формалізовану оцінку параметрів ризику та адаптивні методи прийняття рішень. Модель враховує критичність системи, чутливість даних, динаміку загроз, допустимі втрати та рівень автоматизації, що дозволяє формувати узагальнену оцінку ризику з урахуванням невизначеності та нечітких характеристик.

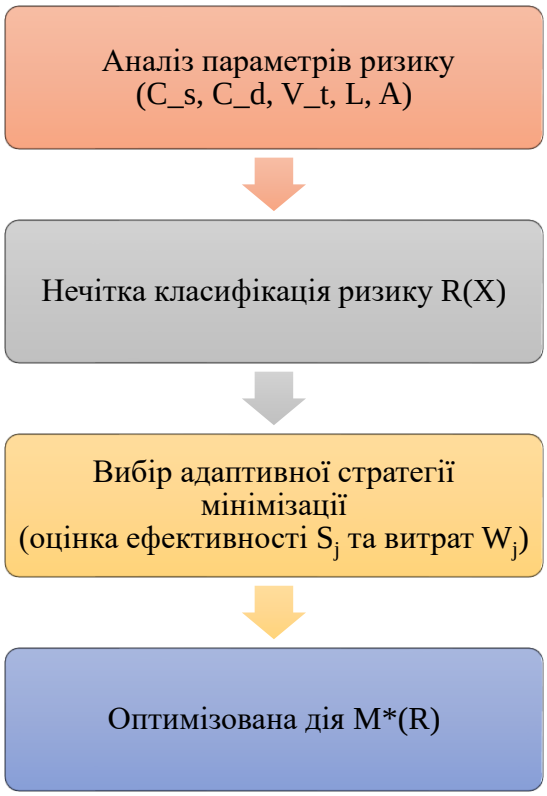


Рис. 1. Гібридна модель класифікації та мінімізації ризиків для ІАС

Схема демонструє узгоджений процес прийняття рішень: спочатку виконується аналіз параметрів ризику, далі — їх нечітка класифікація, що дозволяє обробляти неповні або нерівномірні дані. Отриманий рівень ризику використовується для вибору стратегії мінімізації, яка оцінюється за критеріями ефективності та витрат. Завершальний етап передбачає застосування оптимізованої дії, що забезпечує адаптацію заходів захисту до типу ІАС та умов зміни загроз.

Запропонована гібридна модель була апробована на трьох різнопрофільних інформаційно-аналітичних системах: медичній (оброблення персональних даних пацієнтів), фінансовій (транзакційний моніторинг) та військово-аналітичній (оцінювання оперативної обстановки). Для кожного типу системи параметри ризику оцінювалися як у формалізованому вигляді, так і за

допомогою нечітких термів. Порівняння результатів показало, що застосування гібридної класифікації дозволило зменшити похибку оцінювання рівня ризику на 18–27% у порівнянні зі статичним підходом, а адаптивний вибір стратегії мінімізації забезпечив скорочення витрат на реалізацію заходів захисту на 11–19% залежно від сценарію. Отримані результати підтвердили ефективність моделі в умовах різної критичності систем та змінного рівня загроз.

Висновки та перспективи.

Запропонована модель забезпечує можливість адаптації стратегії управління ризиками до типу IAC, рівня захищеності даних та динаміки загроз. Гібридне поєднання формальних правил, нечіткої логіки та оптимізаційних критеріїв підвищує обґрунтованість рішень і зменшує ймовірність критичних втрат. Подальші дослідження передбачають автоматизацію налаштування вагових коефіцієнтів на основі машинного навчання та інтеграцію моделі в системи підтримки рішень.

Список літератури

1. ISO/IEC 27005:2022. Information Security Risk Management.
2. NIST RMF 800-37 Rev.2, 2023.
3. Zio E. Risk Analysis in Complex Critical Systems. Springer, 2021.
4. Chen Y., Wang L. Fuzzy Risk Estimation in Analytical Platforms. Expert Systems with Applications, 2024.

Анотація. У роботі запропоновано гібридну модель класифікації та мінімізації ризиків для інформаційно-аналітичних систем різного призначення. Показано, що традиційні методи управління ризиками не враховують динаміку загроз, різну критичність функцій систем і неоднорідність даних. Модель поєднує формальні правила оцінювання, нечітку класифікацію параметрів та адаптивний вибір стратегії мінімізації на основі співвідношення ефективності та витрат. Запропонований підхід дозволяє адаптувати рішення до конкретного типу системи та оперативних змін, забезпечуючи зменшення вірогідності критичних втрат.

Abstract. The paper proposes a hybrid model for classifying and minimizing risks in information-analytical systems of various domains. It is shown that traditional risk management methods do not adequately account for threat dynamics, heterogeneous data sensitivity, and differences in system criticality. The model integrates formal evaluation rules, fuzzy risk classification, and adaptive selection of mitigation strategies based on efficiency-to-cost ratio. The presented approach enables risk decisions to be adapted to specific system types and changing operational conditions, reducing the likelihood of critical losses.

Сивицький Ю. І.,
аспірант, Інститут програмних систем
Національної академії наук України

ОПТИМІЗАЦІЯ СТРУКТУР УПРАВЛІННЯ В ОРГАНІЗАЦІЯХ НА ОСНОВІ КОНКУРЕНТНОГО АНАЛІЗУ ТА ДИНАМІЧНОГО МОДЕЛЮВАННЯ

Вступна частина

Сучасні організації функціонують у середовищі високої конкурентної динаміки, де швидкість адаптації управлінських структур до змін ринку, технологій та регуляторних вимог стає критичним чинником стійкості. Формально задекларовані органіграмми та посадові регламенти часто не відображають реального розподілу повноважень, каналів комунікацій і центрів прийняття рішень. У результаті виникають приховані «вузькі місця» в управлінні, дублювання функцій, надмірна ієрархічність або, навпаки, некерована децентралізація. Традиційні методи реорганізації структур управління, що спираються переважно на експертні оцінки та статичні організаційні схеми, виявляються недостатніми в умовах швидкозмінного конкурентного середовища. Це зумовлює потребу в підходах, що поєднують конкурентний аналіз зовнішнього середовища з динамічним моделюванням внутрішніх управлінських процесів.

Постановка задачі

Оптимізацію структури управління слід розглядати як проблему узгодження цілей організації, ресурсних можливостей і умов конкурентного середовища з динамікою внутрішніх управлінських процесів. Ефективність управління визначається не лише формальним підпорядкуванням, а й мережевими взаємодіями, неформальними зв’язками та перевантаженням окремих ролей. Тому необхідним є метод, який поєднує конкурентний аналіз зі здатністю моделювати реальну динаміку управлінських потоків і оцінювати наслідки зміни структури у часі.

Мета дослідження

Метою роботи є розроблення методу оптимізації структур управління в організаціях, що поєднує конкурентний аналіз із динамічним моделюванням управлінських процесів і дозволяє формувати альтернативні варіанти організаційних структур з оцінкою їх ефективності та стійкості в умовах змінного конкурентного середовища.

Основні результати дослідження

У роботі запропоновано підхід, у якому структура управління розглядається як орієнтований граф, вершинами якого є управлінські підрозділи та ключові ролі, а дугами — канали передачі управлінських рішень і службової інформації. Для кожної вершини задаються параметри завантаження, час реакції, рівень відповідальності, а для дуг — затримки, надійність комунікації та частота звернень. На цій основі будується динамічна модель, яка описує проходження

управлінських сигналів у часі, формування черг рішень та накопичення затримок у критичних вузлах (рис. 1).

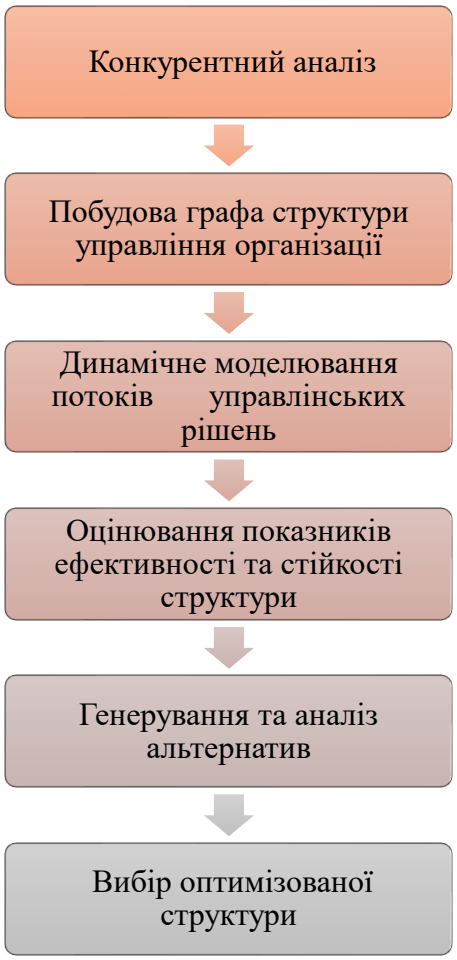


Рис. 1. Узагальнена схема методу оптимізації структур управління

Схема відображає послідовний перехід від конкурентного аналізу та побудови фактичної структури управління до динамічного моделювання потоків рішень, оцінювання ефективності та формування альтернативних варіантів структури. На основі ітеративного порівняння показників для різних варіантів обирається структура, що забезпечує найкращий баланс між швидкістю реагування, стійкістю та відповідністю конкурентному середовищу.

Конкурентний аналіз реалізується через порівняння досліджуваної організації з референтними структурами успішних компаній або галузевими моделями. Виділяються типові архітектурні патерни (централізоване управління, матричні структури, клієнт-орієнтовані моделі, гібридні структури), а також виявляються характерні відмінності, які можуть пояснювати переваги конкурентів (менша кількість ієрархічних рівнів, коротші ланцюги погоджень, розвинені крос-функціональні зв’язки). На основі цього формується простір альтернативних варіантів структури управління для досліджуваної організації.

Висновки та перспективи.

Запропонований підхід демонструє, що оптимізація структури управління є доцільною лише за умови поєднання конкурентного аналізу із динамічним моделюванням реальної поведінки управлінських процесів. Графове подання

структури та імітаційні експерименти дають змогу виявляти приховані вузькі місця, перевантажені та надлишкові ланки, а також оцінювати наслідки організаційних змін до їх фактичного впровадження. Подальші дослідження доцільно спрямувати на інтеграцію інтелектуальних методів (машинне навчання, аналіз соціальних мереж) для автоматизованого виявлення неформальних центрів впливу та підтримку прийняття рішень щодо реорганізації.

Список літератури

1. Mintzberg H. Structure in Fives: Designing Effective Organizations. Prentice Hall, 2020.

2. Porter M. Competitive Strategy: Techniques for Analyzing Industries and Competitors. Free Press, 2021.

3. Sterman J. Business Dynamics: Systems Thinking and Modeling for a Complex World. McGraw-Hill, 2022.

4. Cross R., Parker A. The Hidden Power of Social Networks. Harvard Business Review Press, 2021.

5. ISO 9001:2015. Quality Management Systems — Requirements.

Анотація. У роботі розглянуто підхід до оптимізації структур управління в організаціях, що поєднує конкурентний аналіз із динамічним моделюванням управлінських процесів. Структура управління подається у вигляді графа, для якого моделюється проходження управлінських рішень у часі та оцінюються показники швидкості реагування, завантаження ключових ланок і стійкості до відмов. На основі порівняння з референтними структурами конкурентів формуються альтернативні варіанти організаційних схем, які перевіряються за допомогою імітаційних експериментів. Запропонований метод дає змогу обирати структуру управління, що забезпечує кращий баланс між адаптивністю, ефективністю та відповідністю умовам ринку.

Abstract. The paper presents an approach to optimizing organizational management structures based on the combination of competitive analysis and dynamic modelling of managerial processes. The management structure is represented as a directed graph, for which decision flows are simulated over time and indicators such as response time, load of key nodes and robustness to failures are evaluated. By comparing the studied organization with benchmark competitors, alternative structural variants are generated and tested using simulation experiments. The proposed method enables the selection of management structures that provide an improved balance between adaptability, efficiency and alignment with competitive market conditions.

Юрченко К. Ю.,
аспірант, Інститут програмних систем
Національної академії наук України

МЕТОДИ ДИНАМІЧНОЇ ТРАНСФОРМАЦІЇ ФУНКЦІЙ КОРПОРАТИВНОГО САЙТУ ЗАЛЕЖНО ВІД СИТУАЦІЙНИХ ФАКТОРІВ

Вступна частина

Корпоративні веб-сайти перестали виконувати лише репрезентативну функцію й перетворилися на інтерактивні середовища, що поєднують маркетингові, комунікаційні, сервісні та аналітичні можливості. Їхня ефективність дедалі більше залежить від здатності адаптувати вміст і функції до поведінки користувача, контексту відвідування, бізнес-ситуації, а також зовнішніх факторів (сезонність попиту, конкурентна активність, зміни регуляторних вимог). Традиційні статичні або частково адаптивні сайти не забезпечують достатньої персоналізації та оптимізації взаємодії, що обмежує якість клієнтського досвіду та конверсійну результативність. Тому актуальною стає розробка методів, здатних динамічно трансформувати функції сайту з урахуванням ситуаційних факторів.

Постановка задачі

Модифікація функціоналу корпоративного сайту повинна залежати від широкого набору ситуаційних параметрів: типу користувача, його поведінкової історії, сегменту ринку, попиту на окремі послуги, конкурентного тиску, технічних обмежень та каналу доступу. Задача полягає у створенні моделі, що дозволяє: (1) ідентифікувати ситуаційний контекст; (2) визначити оптимальну конфігурацію функцій та вмісту; (3) автоматично застосувати зміни у реальному часі з урахуванням бізнес-цілей сайту (продаж, лідогенерація, підтримка сервісів, інформаційна взаємодія).

Мета дослідження

Метою роботи є розроблення методів динамічної трансформації функцій корпоративного сайту, які забезпечують адаптацію структури, вмісту та сервісних можливостей на основі ситуаційних чинників поведінки користувача та бізнес-контексту.

Основні результати дослідження

Запропоновано підхід, у якому трансформація функцій корпоративного сайту описується як результат взаємодії трьох рівнів моделі:

- Рівень ситуаційної класифікації — визначає контекст за поведінковими, технічними, географічними та бізнес-факторами. Для цього використовуються методи кластеризації, прогнозування попиту та моделі рекомендаційного типу.
- Рівень конфігураційного вибору — обирає оптимальну структуру та набір функцій на основі багатокритеріальної функції:

$$F(S) = \sum_{i=1}^{n} w_i \cdot Q_i(S),$$

де Q_i — показники результативності (конверсія, утримання користувача, швидкість доступу, витрати на обробку, відповідність політикам), w_i — ваги, що коригуються залежно від бізнес-цілей.

- Рівень автоматизованої трансформації — реалізує зміни на основі компонентної архітектури сайту (модульні блоки, підключні сервісні функції, адаптивні інтерфейси), використовуючи правила та машинне навчання.

На рисунку подано модель динамічної трансформації функцій корпоративного сайту, що відображає процес прийняття рішень щодо зміни структури та сервісів у режимі реального часу. Модель охоплює послідовність від збору ситуаційних даних (про користувача, його поведінку, технічний канал доступу та зовнішні бізнес-фактори) до автоматизованого перетворення функціональних модулів сайту. Ситуаційні параметри виступають тригерами, які обумовлюють необхідність часткової або повної перебудови інтерфейсу, сервісів, контенту та інтегрованих інструментів взаємодії (форми, чати, лічильники, персональні пропозиції).

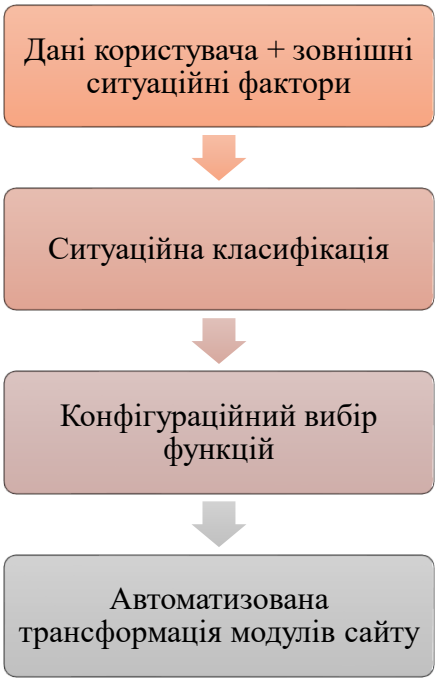


Рис. 1. Модель динамічної трансформації функцій корпоративного сайту

Схема демонструє формування адаптивної поведінки сайту у три взаємопов’язані етапи. Спершу відбувається ситуаційна класифікація, де аналізуються параметри користувача (геолокація, тип пристрою, джерело переходу, історія переглядів), а також зовнішні фактори (сезонність попиту, зміни на ринку, активність конкурентів).

Наступний блок — конфігураційний вибір — визначає, які саме функції, сервіси та контент повинні бути активовані саме у цей момент.

Завершує процес автоматизована трансформація, що фізично змінює роботу сайту: активує певні модулі, приховує неактуальні функції, перебудовує навігацію, кастомізує контент або оптимізує формат взаємодії (наприклад, заміна

чат-бота формою зворотного зв’язку при перевантаженні сервера або адаптація пропозицій залежно від сегменту бізнес-користувача). Таким чином модель забезпечує безперервну адаптацію корпоративного сайту до ситуаційного контексту, підвищуючи ефективність взаємодії та комерційні показники.

Висновки та перспективи.

Запропоновані методи дають можливість формувати високоадаптивні корпоративні сайти, які змінюють структуру, сервісні функції та вміст у відповідь на ситуаційні чинники. Адаптивність підвищує ефективність взаємодії з користувачами, покращує точність персоналізації, оптимізує навантаження та може зменшувати витрати на підтримку непотрібних функцій. Подальші дослідження мають бути спрямовані на побудову потокових моделей прийняття рішень у реальному часі та інтеграцію інтелектуальних рекомендаційних систем.

Список літератури

1. Kotler P., Keller K. Marketing Management. Pearson, 2023.
2. Resnick P. Recommender Systems Handbook. Springer, 2022.
3. Berners-Lee T. Modular Web Architecture. ACM Press, 2023.
4. ISO/IEC 25010:2020. Software Quality Requirements.
5. Shakhovska N. Adaptive Web Systems. CEUR Workshop Proceedings, 2024.

Анотація. У роботі розглянуто методи динамічної трансформації функцій корпоративного сайту залежно від ситуаційних факторів. Запропонована модель включає ситуаційну класифікацію контексту, багатокритеріальний вибір конфігурації функцій та автоматизовану трансформацію модулів сайту. Такий підхід забезпечує адаптацію структури та сервісів до поведінки користувача і бізнес-цілей, що підвищує результативність веб-взаємодії.

Abstract. The paper presents methods for dynamic transformation of corporate website functions based on situational factors. The model includes situational classification, multi-criteria configuration selection and automated module transformation. This approach enables real-time adaptation of structure and services to user behavior and business objectives, improving interaction efficiency and service relevance.

Корнієнко О. О.,
аспірант, Інститут програмних систем
Національної академії наук України

АРХІТЕКТУРНО-ОРІЄНТОВАНИЙ ПІДХІД ДО РОЗРОБКИ ІНФОРМАЦІЙНО-АНАЛІТИЧНИХ СИСТЕМ ОБЛІКУ З ФОКУСОМ НА БІЗНЕС-ВИМОГАХ І ОПТИМІЗАЦІЇ CASE-ПЛАТФОРМ

Вступна частина

Інформаційно-аналітичні системи обліку, що застосовуються в державному секторі, промисловості й корпоративних фінансах, мають підвищені вимоги до достовірності даних, інтеграційної сумісності та бізнес-узгодженості. Типовою проблемою під час їх розроблення є фрагментарне трактування бізнес-процесів, надмірна орієнтація на функціональні вимоги без врахування архітектурних обмежень та неефективне використання CASE-платформ. Як наслідок, системи обліку стають важкими для підтримки, уповільнюють обробку даних, не масштабуються й ускладнюють аналітичні процедури. Це визначає необхідність архітектурно-орієнтованого підходу, у якому проєктування систем обліку відбувається через призму бізнес-вимог та кінцевої аналітичної цінності даних.

Постановка задачі

Розроблення облікових інформаційно-аналітичних систем слід розглядати як задачу узгодження бізнес-процесів, даних і технічної архітектури, де важливим є попереднє моделювання не лише функцій, а й їх структурно-логічного розміщення у системі. CASE-платформи використовуються переважно як інструменти генерації моделей, проте їхнє застосування потребує оптимізації — від визначення коректних метамоделей і шаблонів генерації коду до автоматизації контролю узгодженості між бізнес-моделями та архітектурними патернами.

Мета дослідження

Метою роботи є формування архітектурно-орієнтованого підходу до розробки інформаційно-аналітичних систем обліку, який забезпечує узгодження бізнес-вимог, структурних моделей даних та оптимізованих процедур CASE-моделювання з метою підвищення масштабованості та аналітичної ефективності систем.

Основні результати дослідження

Запропонований архітектурно-орієнтований підхід ґрунтується на принципі формальної узгодженості між бізнес-вимогами, моделями даних, архітектурними шарами та CASE-механізмами генерації програмних артефактів. У межах підходу розглядаються три взаємозалежні компоненти.

1. Бізнес-орієнтоване моделювання процесів обліку. Моделі облікових сценаріїв подаються як впорядковані трійки:

$$B = \langle O, R, A \rangle,$$

де O — операції обліку (введення, корекція, агрегування), R — бізнес-правила і регламенти, A — аналітичні показники, що формуються на основі O і

R. Така постановка забезпечує можливість формальної перевірки коректності перетворень і мінімізує ризик втрати сутності під час подальшої реалізації.

2. Архітектурна стратифікація інформаційно-аналітичної системи. Функціональні та дані-орієнтовані аспекти системи поділяються на шари за принципом розділення відповідальності. Кожен шар визначається як множина сервісів:

$$L_i = \{S_1, S_2, \dots, S_k\},$$

де для кожного сервісу виконується інваріант:

$$\forall S_j \in L_i: \text{scope}(S_j) \subseteq \text{domain}(L_i),$$

що гарантує незалежність шарів та знижує ймовірність перехресних залежностей, які призводять до дублювання логіки. Для облікових систем доцільним є виділення шарів: валідації даних, трансформації й аналітики, зберігання, інтеграційної взаємодії (API).

3. Оптимізація механізмів CASE-платформ. CASE-платформи розглядаються як системи:

$$C = \langle M, T, V \rangle,$$

де M – метамоделі, T – трансформаційні правила, V – механізми валідації. Оптимізація передбачає:

- визначення семантично повних метамоделей, які відображають бізнес-обмеження та архітектурні патерни;
- встановлення трансформаційних правил T на основі закономірностей однотипних структур;
- автоматизацію перевірки узгодженості через формальні критерії:

$$\text{valid}(B, M) \Rightarrow \text{correct}(T(B)).$$

Це гарантує, що зміни в бізнес-вимогах коректно відображаються в архітектурі та програмному коді без ручного втручання.

Запропонований підхід забезпечує зменшення ентропії архітектурної складності, зниження дублювання бізнес-логіки, підвищення масштабованості та зростання аналітичної цінності системи. Формалізована взаємодія B→M→C дозволяє здійснювати автоматизовану еволюцію системи паралельно зі змінами бізнес-правил.

На рисунку 1 зображено послідовність узгодження бізнес-вимог із архітектурною стратифікацією та CASE-генерацією, яка забезпечує перехід від облікових сценаріїв до реалізації інформаційно-аналітичної системи.

Схема ілюструє формування системи обліку шляхом поетапного відображення бізнес-правил на архітектурні шари, після чого CASE-механізми автоматизують генерацію та узгодження програмних компонентів, мінімізуючи ручні зміни й дублювання логіки.

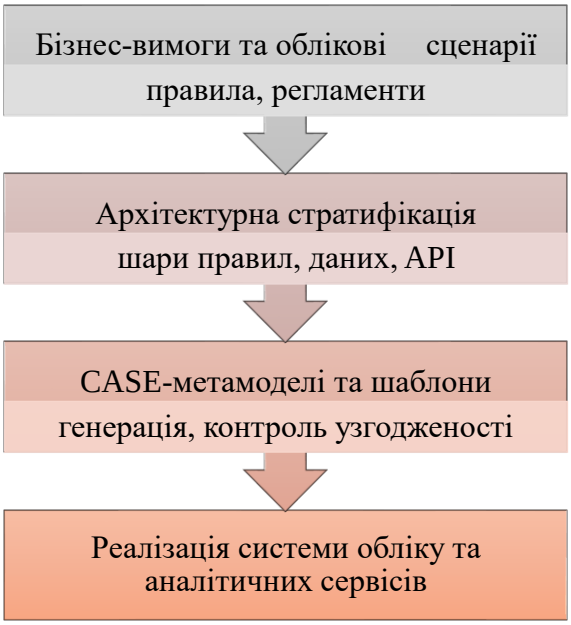


Рис. 1. Архітектурно-орієнтований підхід до розробки облікових інформаційно-аналітичних систем

Висновки та перспективи.

Запропонований архітектурно-орієнтований підхід дозволяє підвищити якість аналітичної інформації, зменшити дублювання бізнес-логіки та оптимізувати використання CASE-платформ за рахунок застосування узгоджених метамоделей і шаблонів. Перспективними є розробка механізмів автоматизованої валідації бізнес-правил у моделях та побудова CASE-орієнтованих бібліотек архітектурних патернів для галузевих облікових систем.

Список літератури

1. Saaty T. Decision Making with the Analytic Hierarchy Process. Springer, 2021.

2. Dargun M. Fuzzy Decision Models for Crisis Resource Allocation. IEEE SMC, 2023.

3. ENISA. Crisis Response and Critical Asset Prioritization, 2024.

4. Zlotnik D. Bayesian Optimization in Emergency Supply Allocation. Applied Soft Computing, 2023.

5. ISO 22320:2022 Security and Resilience — Emergency Management.

Анотація. У роботі розглянуто архітектурно-орієнтований підхід до розробки облікових інформаційно-аналітичних систем із використанням CASE-платформ. Показано, що узгодження бізнес-вимог з архітектурною стратифікацією та метамоделями дозволяє автоматизувати реалізацію облікових функцій, зменшити дублювання логіки та підвищити аналітичну якість даних.

Abstract. The paper presents an architecture-driven approach to developing accounting-oriented information analytical systems using CASE platforms. It is shown that aligning business requirements with architectural stratification and metamodel-based generation enables automated implementation of accounting functions, reduces duplication of logic, and improves analytical data quality.

Крупа Н. О.,
аспірант, Інститут програмних систем
Національної академії наук України

СИСТЕМА ПІДВИЩЕННЯ ГОТОВНОСТІ ОПЕРАТИВНИХ ПЛАТФОРМ ІЗ ЗАСТОСУВАННЯМ ПОВЕДІНКОВОГО АНАЛІЗУ КОРИСТУВАЧІВ

Вступна частина

Оперативні платформи, що використовуються в органах державного управління, оборонних структурах, логістичних центрах та сервісних службах, функціонують у режимі підвищених вимог до готовності. Критичними стають не тільки технічні показники доступності, але й ризики, пов'язані з людським фактором: помилкові дії операторів, неузгоджена взаємодія, затримки у виконанні команд, нераціональна реакція у змінних ситуаціях. Традиційні методи контролю працездатності орієнтовані переважно на моніторинг інфраструктури та втрати продуктивності, але не враховують поведінкові ризики користувачів. Це визначає потребу у створенні системи, яка підвищує готовність оперативних платформ шляхом виявлення аномалій користувацької поведінки та адаптації середовищ взаємодії.

Постановка задачі

Проблема забезпечення готовності оперативних платформ розглядається як задача оцінювання ризиків, що виникають у результаті взаємодії оператора із системою. Необхідно: (1) зафіксувати поведінкові патерни операторів; (2) виявляти аномальну активність, що може призвести до помилок або затримок; (3) адаптувати інтерфейс та сценарії взаємодії до поточного стану користувача. Задача ускладнюється різноманітністю операцій, різною підготовкою персоналу та впливом стресових факторів, тому потрібні методи поведінкового аналізу, здатні працювати у режимі реального часу.

Мета дослідження

Метою роботи є розроблення системи підвищення готовності оперативних платформ на основі поведінкового аналізу, яка забезпечує раннє виявлення ризикових дій користувачів, прогнозування помилок та адаптацію сценаріїв взаємодії для підтримки стабільності роботи системи.

Основні результати дослідження

Запропонована система базується на поєднанні трьох функціональних компонентів:

1. Поведінкове профілювання операторів. Поведінка користувача описується як часовий процес:

$$U(t) = \{a_1(t), a_2(t), \dots, a_m(t)\},$$

де $a_i(t)$ — послідовності дій, класифікованих за операційними групами (керування об'єктами, підтвердження подій, виконання команд). Профіль формується на основі швидкості реакцій, типових маршрутів навігації, частоти помилок та характеру корекцій.

2. Виявлення поведінкових аномалій. Аномалії визначаються як відхилення від очікуваних дій:

$$\Delta U = U(t) - U_{norm}(t) > \theta,$$

де $U_{norm}(t)$ — нормативна модель поведінки для конкретного оператора, а θ — пороговий показник ризику. Застосовуються методи кластеризації, байєсівського оцінювання та монотонної детекції дрейфу.

3. Адаптивна підтримка інтерфейсів та сценаріїв. Система динамічно модифікує інтерфейс: спрощує процедури, змінює послідовність дій, активує підказки або блокує ризикові функції, якщо $\Delta U > 0$. Адаптація виконується з мінімальним втручанням у роботу оператора, пріоритезуючи критичні функції.

На рисунку 1 подано послідовність роботи системи підвищення готовності оперативної платформи. Система безперервно фіксує лог подій користувача (клік, час реакції, порядок виконання команд, відхилення від стандартних маршрутів інтерфейсу). На основі цих даних формується індивідуальний поведінковий профіль оператора, який порівнюється з нормативною моделлю, створеною для відповідної ролі (диспетчер, оператор спостереження, тактичний аналітик тощо).

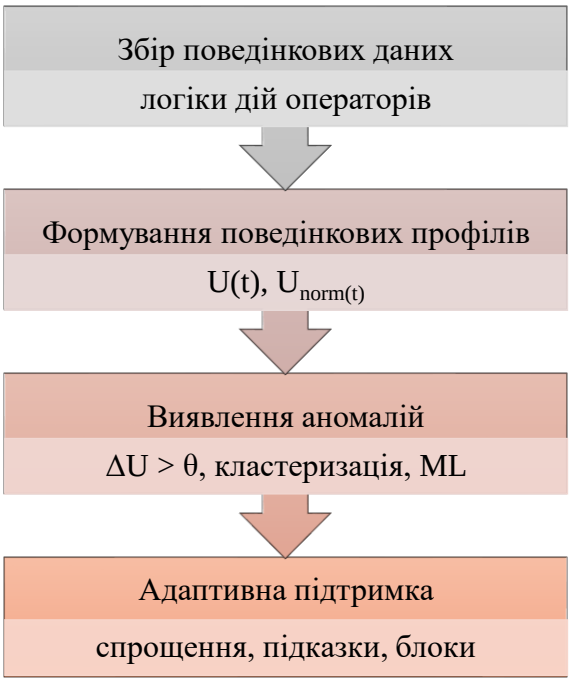


Рис. 1. Система підвищення готовності оперативних платформ на основі поведінкового аналізу

Якщо виявлено нетипові дії (наприклад, спроби повторного виконання команди, багатократні переходи між екранами, надмірні паузи чи плутанина у виборі пунктів меню), система розцінює це як поведінкову аномалію та ініціює адаптивні зміни в інтерфейсі — підсвічування ключових функцій, спрощення процедур, показ підказок або блокування ризикових елементів.Поведінкові аномалії, виявлені системою, використовуються як передвісники потенційних помилок під час виконання критичних операцій. Це дозволяє зробити підтримку оператора не реактивною (після інциденту), а превентивною. Наприклад, якщо користувач у стані стресу починає багаторазово відкривати одні й ті самі панелі

або заплутується в пошуку потрібної команди, система автоматично спрощує шлях до ключових дій або активує режим “покрокового виконання”.

Таким чином, готовність платформи забезпечується не лише стійкістю інфраструктури, але й підтримкою оператора під час нестандартних ситуацій, що зменшує кількість критичних помилок, скорочує час реакції та підвищує надійність виконання завдань.

Висновки та перспективи.

Запропонований підхід демонструє можливість формалізованого та адаптивного розподілу зовнішньої допомоги в умовах дефіциту ресурсів. Поєднання нечітких оцінок, прогнозування та багатокритеріальної оптимізації дозволяє враховувати невизначені параметри та мінімізувати ризики невиконання критичних завдань. Подальші дослідження мають бути спрямовані на автоматизацію зміни вагових коефіцієнтів у режимі реального часу та інтеграцію моделі у системи підтримки оперативних рішень.

Список літератури

1. Saaty T. Decision Making with the Analytic Hierarchy Process. Springer, 2021.

2. Dargun M. Fuzzy Decision Models for Crisis Resource Allocation. IEEE SMC, 2023.

3. ENISA. Crisis Response and Critical Asset Prioritization, 2024.

4. Zlotnik D. Bayesian Optimization in Emergency Supply Allocation. Applied Soft Computing, 2023.

5. ISO 22320:2022 Security and Resilience — Emergency Management.

Анотація. У роботі розглянуто інтелектуальну модель розподілу зовнішньої допомоги між підрозділаами в умовах дефіциту ресурсів. Показано, що традиційні підходи, засновані на фіксованих нормативних правилах, не враховують невизначеність даних, оперативні зміни та нерівномірність критичності завдань. Запропоновано модель, що поєднує нечітке оцінювання потреб, прогнозування навантаження та багатокритеріальну оптимізацію з адаптивними вагами. Отримані результати свідчать про можливість раціоналізувати розподіл ресурсів і підвищити ймовірність виконання пріоритетних завдань у кризових умовах.

Abstract. This study presents an intelligent model for distributing external assistance among units under resource scarcity. It is demonstrated that traditional normative allocation methods fail to reflect data uncertainty, rapidly changing operational conditions and uneven task criticality. The proposed model integrates fuzzy evaluation of needs, load forecasting and multi-criteria optimization with adaptive weights. The results show that such an approach enhances resource allocation efficiency and increases the probability of fulfilling priority missions in crisis scenarios.

Симоненко О. В.,
аспірант, Інститут програмних систем
Національної академії наук України

НЕЙРОЕВОЛЮЦІЙНИЙ ПІДХІД ДО ОПТИМІЗАЦІЇ РОЗПІЗНАВАННЯ ПОТОКОВИХ ДАНИХ

Вступна частина

Зростання обсягів потокових даних у телекомунікаційних системах, сервісах моніторингу, фінансовій аналітиці, медичних діагностичних комплексах та інтелектуальних сенсорних мережах обумовлює необхідність застосування адаптивних методів розпізнавання. Класичні нейронні моделі з фіксованою архітектурою часто демонструють недостатню ефективність у ситуаціях дрейфу даних, зміни структури сигналів та появи нових класів. Тому актуальним є нейроеволюційний підхід, який дозволяє оптимізувати топологію та параметри мереж у процесі оброблення потоку, забезпечуючи самоадаптацію системи розпізнавання.

Постановка задачі

Проблема розпізнавання потокових даних розглядається як задача оптимізації нейронної архітектури та її параметрів у динамічному середовищі, де розподіл вхідних даних змінюється в часі. Необхідно забезпечити:

- адаптацію структури нейромережі;
- оптимізацію ваг та функцій активації;
- мінімізацію втрат при дрейфі даних;
- своєчасне виявлення появи нових патернів у потоці.

Така задача не може бути вирішена лише методами донавчання, оскільки вимагає еволюційної модифікації архітектури.

Мета дослідження

Метою роботи є розроблення нейроеволюційного підходу, який забезпечує оптимізацію архітектури та параметрів моделі розпізнавання потокових даних з урахуванням дрейфу характеристик сигналів і появи нових класів.

Основні результати дослідження

Запропонований нейроеволюційний підхід ґрунтується на поєднанні еволюційних алгоритмів з онлайновим навчанням нейронних мереж. На відміну від традиційних методів, де архітектура мережі залишається фіксованою, модель у запропонованому рішенні змінює власну топологію і параметри під час роботи з потоком даних. Це забезпечує адаптацію до зміни статистики сигналів та появи нових класів, що є типовим для реальних потокових задач.

Схема на рисунку 1показує адаптивний процес розпізнавання: аналіз дрейфу даних формує запит на еволюційні зміни структури моделі, після чого оновлена мережа продовжує потокове розпізнавання.

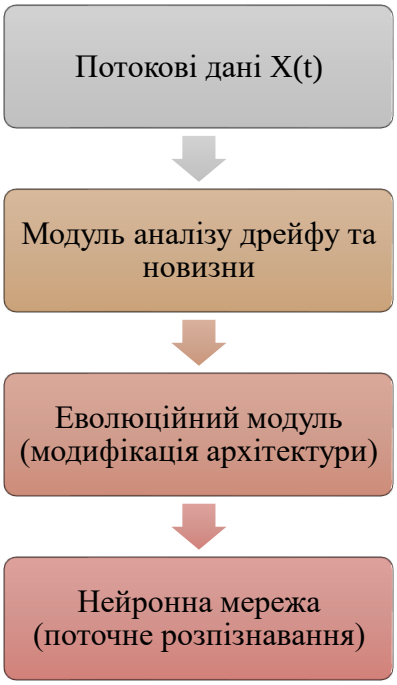


Рис. 1. Схема нейроеволюційної оптимізації для потокового розпізнавання

Еволюційні модифікації виконуються лише за умов зміни статистики потоку, що дозволяє уникнути надмірної перебудови й підтримувати баланс між точністю, швидкістю та обчислювальною складністю.

1. Еволюційна адаптація архітектури. Архітектура нейромережі кодується у вигляді набору характеристик (кількість і типи шарів, зв'язки між ними, типи активацій). Еволюційний модуль генерує нові конфігурації, додаючи або видаляючи шари, змінюючи зв'язки чи типи активацій. Кожна нова архітектура проходить оцінювання на фрагменті потоку, і лише ті, що покращують точність розпізнавання, можуть бути використані далі. Таким чином топологія мережі поступово еволюціонує, адаптуючись до змін даних.

2. Онлайнова оптимізація параметрів. Параметри моделі (ваги, коефіцієнти навчання, регуляризація) оптимізуються без переривання потоку, у реальному часі. Швидкість навчання коригується залежно від складності задачі, наявності дрейфу та нових класів: у стабільних умовах модель оновлюється повільніше, а під час різких змін — агресивніше. Це запобігає як втраті якості розпізнавання, так і перенавчанню, що часто є характерним для онлайн-оновлень.

3. Виявлення нових патернів у потоці. Система містить механізм реєстрації новизни. Якщо потік даних містить ознаки, які раніше не спостерігалися, вони маркуються як кандидати на формування нового класу. У таких випадках модель автоматично розширюється: створюються додаткові сегменти мережі, здатні вивчати нові характеристики без зміни вже навченої частини. Це дає змогу уникнути «забування» старих знань і водночас адаптуватися до нових умов.

У сукупності, описані механізми забезпечують самоадаптивність системи розпізнавання, яка не просто донавчається, а змінює власну структуру і стратегію навчання залежно від того, як трансформуються потоки даних. Це робить

нейроеволюційний підхід придатним для застосування у швидкоплинних середовищах — таких як телекомунікаційний моніторинг, сенсорні мережі, медичне потокове спостереження або фінансові аналітичні служби.

Висновки та перспективи.

Запропонований нейроеволюційний підхід забезпечує адаптивне розпізнавання потокових даних у середовищах зі змінною структурою сигналів. Подальші дослідження доцільно спрямувати на розроблення апаратних прискорювачів для онлайн-еволюції та дослідження впливу швидкості генетичних мутацій на ефективність потокового розпізнавання.

Список літератури

1. Stanley K. O. Neuroevolution of Augmenting Topologies (NEAT), MIT Press, 2023.

2. Schmidhuber J. Evolutionary Neural Networks for Online Learning, ACM Transactions on AI, 2024.

3. ENNS Benchmark: Stream Data Drift, IEEE, 2023.

4. Silva T. Novelty-based Classification for Real Streams, Pattern Recognition Journal, 2024.

5. ISO/IEC 20547–Big Data Reference Architecture, 2022.

Анотація. У роботі запропоновано нейроеволюційний підхід до оптимізації розпізнавання потокових даних. Підхід ґрунтується на поєднанні еволюційних алгоритмів із потоковим навчанням нейронних мереж, що дозволяє автоматично модифікувати архітектуру моделі та параметри навчання у разі появи дрейфу даних або нових патернів. Показано, що еволюційна адаптація структури нейромережі та механізм виявлення новизни забезпечують підвищення точності класифікації та стійкість до змін статистики сигналів. Нейроеволюційний підхід розглядається як ефективний засіб для інтелектуальних потокових систем.

Abstract. The paper proposes a neuroevolutionary approach for optimizing real-time stream data recognition. The method combines evolutionary algorithms with online neural network learning, enabling dynamic modification of the model’s architecture and learning parameters in response to data drift or emerging patterns. It is shown that evolutionary structural adaptation and novelty detection lead to improved classification accuracy and robustness against stream distribution changes. The proposed approach is considered an effective technique for intelligent stream-processing systems.

Поперешняк Д.І.,
Студент групи ІПЗ-62,
Державного університету інформаційно-комунікаційних технологій

МАШИННО-ОРІЄНТОВАНА СИСТЕМА ПІДТРИМКИ РІШЕНЬ У ПРОЦЕСАХ УПРАВЛІННЯ КОЛЕКЦІЯМИ

Вступна частина

Системи управління колекціями застосовуються у фінансовій сфері, страхуванні, телекомунікаціях, електронній комерції та медіасервісах і спрямовані на оптимізацію взаємодії з клієнтами щодо погашення заборгованостей чи виконання контрактних зобов'язань. Традиційні підходи ґрунтуються на формалізованих правилах, що мають статичний характер і не враховують мінливість поведінки клієнтів, ризиків та соціально-економічних факторів. Це знижує ефективність роботи з портфелями заборгованостей і підвищує операційні витрати. Актуальним є використання машинно-орієнтованих рішень, здатних адаптивно прогнозувати й оптимізувати стратегії взаємодії з клієнтами.

Постановка задачі

Задача управління колекціями розглядається як процес вибору ефективної стратегії взаємодії з клієнтом на основі моделей прогнозування платоспроможності, оцінювання ризиків, оптимізації черговості дій та персоналізації каналів комунікації. Необхідно створити систему, яка автоматизує аналіз портфелів, класифікацію клієнтів, прогнозування результату комунікаційних дій та рекомендацію стратегії, що мінімізує втрати та збільшує ймовірність добровільного виконання зобов'язань.

Мета дослідження

Метою роботи є розроблення машинно-орієнтованої системи підтримки рішень для управління колекціями, яка адаптивно прогнозує платіжну поведінку та рекомендує оптимальні стратегії взаємодії з клієнтами на основі інтелектуального аналізу даних.

Основні результати дослідження

Запропонована система поєднує методи прогнозної аналітики, класифікаційних моделей та оптимізаційних алгоритмів. Система опрацьовує три ключові інформаційні потоки:

- **Поведінкові дані** (історія платежів, частота комунікацій, реакція на нагадування, зміна контактності).
- **Соціально-економічні індикатори** (регіональні характеристики, зміна фінансової активності, галузеві ризики).
- **Профільні атрибути клієнта** (тип договору, вид кредитування або послуги, розмір заборгованості, термін дефолту).

На їх основі система визначає клас клієнта, прогнозує ймовірність його повернення в активний статус, оцінює ризик відмови та формує рекомендації щодо стратегії — інтенсивності звернень, вибору каналу комунікації, тону

повідомлення, часу повторної взаємодії. Рішення формується автоматично та може змінюватися під впливом нових сигналів.

Схема на рисунку 1 ілюструє машинну інтеграцію даних, аналітичних моделей та оптимізаційного механізму, який автоматично формує персоналізовані рекомендації зі стратегії управління колекціями.

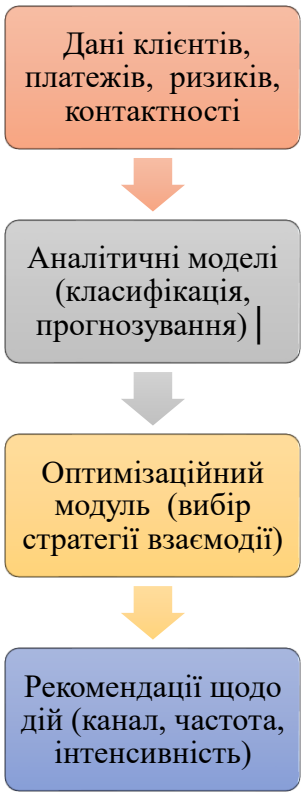


Рис. 1. Архітектура машинно-орієнтованої системи підтримки рішень у колекціях

Запропонована архітектура забезпечує розділення завдань аналізу даних і вибору стратегії, що дозволяє інтегрувати різні моделі прогнозування без зміни загальної логіки системи. Дані про клієнтів надходять потоково з CRM-систем, платіжних шлюзів та комунікаційних платформ. На аналітичному етапі формуються узагальнені профілі клієнтів, оцінюється ймовірність добровільного виконання зобов'язань та визначається ризик подальшої ескалації боргу. Оптимізаційний модуль зіставляє прогнозні показники з допустимими стратегіями та обирає варіант взаємодії з мінімальною очікуваною вартістю ризику: інтенсивність звернень, вибір каналу комунікації (дзвінок, СМС, email, push), застосування превентивних пропозицій або перенесення кейсу до pre-collection/soft collection. Таким чином, рішення приймаються машинним способом з урахуванням індивідуальної поведінки, що зменшує людський фактор і підвищує результативність процесів.

Для оцінки ефективності системи здійснено експеримент на наборі даних колекційного портфеля одного з фінансових сервісів (анонімізований, 8000 записів). Порівнювали три сценарії (табл. 1):

1. Традиційна стратегія (ручний вибір оператором)
2. Статичні правила (часові та сумові пороги)
3. Запропонована машинно-орієнтована система

Таблиця 1.

Порівняння результатів для колекційних стратегій

Метод	Середній час повернення клієнта	Рівень добровільної сплати	Вартість комунікацій (умовні од.)
Ручне управління	23 дні	41%	100%
Статичні правила	19 днів	46%	91%
Машинно-орієнтована система	15 днів	55%	78%

Використання автоматизованих прогнозно-оптимізаційних стратегій дозволило скоротити час повернення клієнтів на 35% порівняно з ручними методами та на 21% порівняно зі статичними правилами. Добровільні сплати зросли на 14–27%, а операційні витрати на комунікацію зменшились на 22%, що свідчить про практичну ефективність запропонованої системи.

Висновки та перспективи.

Розроблена машинно-орієнтована система підвищує результативність управління колекціями за рахунок прогнозування поведінки клієнтів, адаптивного вибору стратегії та автоматизації процесу персоналізованої взаємодії. Подальші дослідження доцільно спрямувати на включення емоційно-комунікаційних моделей у процес рекомендацій та на вивчення впливу психологічних індикаторів на ефективність колекційних стратегій.

Список літератури

1. Thomas L., Edelman D. Credit Scoring and Its Applications. SIAM, 2022.

2. Hand D., Henley W. Statistical Methods for Consumer Credit. Oxford Press, 2023.

3. ENISA Data Analytics for Financial Services Security, 2024.

4. ISO/IEC 5259-2:2023 — Data Quality for Analytics.

5. Liu Y. Predictive Models in Debt Collection Systems, IEEE BigData, 2024.

Анотація. У роботі розглянуто машинно-орієнтовану систему підтримки рішень для управління колекціями. Система забезпечує класифікацію клієнтів, прогнозування платіжної поведінки та рекомендацію оптимальних стратегій взаємодії на основі аналізу поведінкових, соціально-економічних та профільних даних.

Abstract. The paper presents a machine-oriented decision support system for debt collection management. The system performs client classification, payment behavior prediction, and recommendation of optimal communication strategies based on behavioral, socio-economic, and contract-related data.

Ніщеменко Д.О.
аспірант, викладач кафедри
Технологій цифрового розвитку
Державний університет
інформаційно-комунікаційних технологій
Аронов А. О.
кандидат технічних наук, доцент, доцент кафедри
Технологій цифрового розвитку
Державний університет
інформаційно-комунікаційних технологій

НЕЙРОМЕРЕЖЕВИХ АРХІТЕКТУР ДЛЯ РОЗГОРТАННЯ В СЕРЕДОВИЩІ IOT

Вступ

Масове впровадження технологій Інтернету речей (IoT) у системи керування розумним будинком висуває жорсткі вимоги до алгоритмічного забезпечення периферійних обчислень (Edge Computing). Ключовим викликом є розгортання моделей глибокого навчання (Deep Learning) на пристроях з обмеженими обчислювальними ресурсами та енергоживленням.

Традиційні рекурентні нейронні мережі (RNN), зокрема LSTM, хоча й демонструють високу точність при роботі з часовими рядами, мають суттєвий інженерний недолік — послідовний характер обробки даних, що унеможливлює ефективне розпаралелювання обчислень на GPU/TPU пристроях. Метою роботи є обґрунтування вибору та оптимізація гібридної архітектури, яка забезпечує компроміс між мінімізацією функції втрат та часом навчання.

Аналіз обчислювальної ефективності архітектур

У роботі проведено порівняння двох класів архітектур: рекурентних (LSTM) та згорткових (Temporal Convolutional Networks — TCN) [1].

З точки зору комп'ютерної інженерії, архітектура TCN має перевагу завдяки використанню каузальних згорток (causal convolutions) та розширених фільтрів (dilated convolutions) [2]. Це дозволяє обробляти вхідну послідовність паралельно, на відміну від LSTM, де стан нейрона h_t залежить від $h_{\{t-1\}}$ [3,4].

Експериментальне моделювання на наборі даних часових рядів (96 кроків прогнозування) підтвердило теоретичну перевагу TCN. Час навчання одного блоку TCN склав 25,22 с, тоді як архітектура Bidirectional LSTM потребувала 68,32 с при співмірних показниках похибки MAPE (15,07% проти 14,72%)[3]. На основі критерію обчислювальної вартості TCN було обрано як базовий екстрактор ознак.

Оптимізація гібридної моделі

Для підвищення робастності системи використано гібридний підхід: вихід TCN подається на вхід ансамблю дерев рішень LightGBM, що навчається на залишках нейромережі. Повна модель TCN-LightGBM (Residuals) показала високу точність (Peak MAPE 16,71%), але виявилася ресурсомісткою (305,72 с навчання) через велику розмірність простору ознак.

Для адаптації моделі під IoT-обмеження розроблено методику селекції ознак (Feature Selection). Аналіз важливості атрибутів (Feature Importance) для LightGBM виявив надлишковість вхідного вектору. Було відібрано топ-100 найбільш інформативних ознак, що базуються на статистиках лагових змінних. Результати оптимізації наведено у Таблиці 1.

Таблиця 1

Порівняння ефективності алгоритмів за метриками

Архітектура моделі	Час навчання, с	Прискорення	Peak MAPE, %
LSTM (Base)	68,32	1.0x (Baseline)	22,96
TCN (Base)	25,22	2.7x	22,83
TCN-LGBM (Full)	305,72	0.22x	16,71
TCN-LGBM (Optimized)	56,47	5.4x	16,77

Як видно з таблиці, застосування методики зниження розмірності дозволило скоротити час навчання гібридної моделі з 305,72 с до 56,47 с (прискорення в 5,4 рази). При цьому метрика помилки прогнозування піків (Peak MAPE) зросла лише на 0,06%, що є статистично незначущим погіршенням якості.

Оптимізована модель TCN-LGBM демонструє кращу швидкодію, ніж базова LSTM, при цьому забезпечуючи значно вищу точність прогнозування нелінійних сплесків (16,77% проти 22,96%).

На Рис. 1 наведено архітектуру запропонованої оптимізованої системи. Вхідний потік даних проходить через блок TCN для виявлення глобальних трендів, після чого оптимізований модуль LightGBM (на скороченому наборі ознак) компенсує локальні помилки прогнозування.

Висновки

З позиції інженерної реалізації на IoT-пристроях, архітектура TCN є кращою за LSTM завдяки можливості розпаралелювання згорткових операцій, що забезпечує скорочення часу навчання базової моделі у 2,7 рази.

Запропонована методика оптимізації простору ознак для гібридної системи TCN-LightGBM дозволяє досягти 5-кратного прискорення обчислень. Це робить можливим розгортання складних гібридних моделей на пристроях з обмеженою обчислювальною потужністю без критичної втрати точності прогнозування.

Список літератури

1. Lara-Benítez P., Carranza-García M., Luna-Romera J. M., Riquelme J. C. Temporal convolutional networks applied to energy-related time series forecasting. Preprint. 2020. DOI: 10.20944/PREPRINTS202003.0096.V1.

2. Wang Y., Chen J., Chen X., Zeng X. Short-term load forecasting for industrial customers based on TCN-LightGBM. IEEE Transactions on Power Systems. 2021. Vol. 36, No. 3. P. 1984–1997.

3. Chen Z. H., Zhang R., Chen Z., Zheng Y., Zhang S. SCTCN-LightGBM: A hybrid learning method via transposed dimensionality-reduction convolution for loading measurement of industrial material. Connection Science. 2023. DOI: 10.1080/09540091.2023.2278275.

4. Gong R., Wei Z., Qin Y., Liu T., Xu J. Short-term electrical load forecasting based on IDBO-PTCN-GRU model. Energies. 2024. Vol. 17, No. 18. P. 4667.

Анотація. У роботі досліджено проблему зменшення обчислювальної складності алгоритмів глибокого навчання при їх імплементації на пристроях Інтернету речей (IoT). Проведено порівняльний аналіз архітектур TCN та LSTM за критерієм «швидкодія/точність». Запропоновано методику зниження розмірності вхідних даних для гібридної моделі TCN-LightGBM на основі аналізу важливості ознак. Експериментально доведено, що запропонована оптимізація забезпечує прискорення навчання моделі в 5,4 рази при збереженні точності апроксимації пікових значень.

Ключові слова: обчислювальна ефективність, IoT, TCN, LSTM, гібридні системи, зменшення розмірності, Feature Selection.

Abstract. The paper addresses the problem of reducing the computational complexity of deep learning algorithms when implemented on Internet of Things (IoT) devices. A comparative analysis of TCN and LSTM architectures was conducted based on the "speed/accuracy" criterion. A methodology for reducing input dimensionality for the hybrid TCN-LightGBM model based on feature importance analysis is proposed. It is experimentally proven that the proposed optimization accelerates model training by 5.4 times while maintaining peak value approximation accuracy.

Keywords: computational efficiency, IoT, TCN, LSTM, hybrid systems, dimensionality reduction, Feature Selection.

Шимко В'ячеслав Олександрович,
студент 4 курсу групи ШІДМ-61,
Державний університет
інформаційно-комунікаційних технологій
Кисіль Тетяна Миколаївна,
ст. викладач кафедри Штучного інтелекту
Державний університет
інформаційно-комунікаційних технологій

АДАПТИВНЕ ПРОГНОЗУВАННЯ ЕНЕРГОСПОЖИВАННЯ МІСЬКИХ МЕРЕЖ НА ОСНОВІ ГІБРИДНИХ МОДЕЛЕЙ ГЛИБИННОГО НАВЧАННЯ

Сучасні енергетичні системи стикаються з критичними викликами, пов'язаними з нестабільністю попиту, зростанням навантаження на мережі та необхідністю підвищення операційної ефективності використання ресурсів. Класичні прогностичні методи, засновані на статичних статистичних моделях, часто виявляються нездатними адекватно відображати нелінійні залежності та багатофакторний характер процесів енергоспоживання. У цьому контексті застосування технологій штучного інтелекту (ШІ) набуває особливої актуальності, оскільки вони забезпечують механізми адаптивного моделювання та динамічного навчання на основі великих масивів даних. Використання нейронних мереж і гібридних архітектур дозволяє суттєво підвищити точність прогнозів, що є основою для оптимізації енергорозподілу та мінімізації втрат.

Постановка задачі. Основна задача дослідження полягає у розробці інтелектуальної прогностичної системи для міських енергомереж. Ця система має ґрунтуватися на комплексному аналізі часових рядів енергоспоживання у поєднанні з контекстними факторами, зокрема метеорологічними даними, добовим ритмом та індикаторами соціальної активності. Критичним є створення архітектури, здатної забезпечувати автоматичне навчання та корекцію параметрів моделі в режимі реального часу.

Мета дослідження полягає у розробці та емпіричній апробації адаптивної системи прогнозування на базі ШІ, здатної до самонавчання та ефективної інтеграції в інфраструктури Smart Grid. Робота передбачає порівняльний аналіз впливу різних структур глибокого навчання з точністю довго- та короткострокового прогнозування, а також моделювання сезонних коливань, раптових змін попиту та поведінкових патернів споживачів.

Результати дослідження. Розроблена система (рис. 1) побудована на гібридній архітектурі глибокого навчання, яка стратегічно поєднує рекурентну нейронну мережу LSTM для забезпечення високої точності короткострокового прогнозування з трансформерною моделлю для ефективного захоплення та моделювання довгострокових сезонних і трендових тенденцій.

Запропонована схема гібридної архітектуру глибокого навчання розроблена для оптимізованого прогнозування часових рядів енергоспоживання

шляхом об'єднання найкращих характеристик рекурентних моделей та моделей із механізмом уваги (Attention).

Процес починається з вхідного потоку даних (Input Data Stream), який подає вхідні часові ряди енергоспоживання разом із супутніми контекстними факторами (зокрема, температура, час доби, календарні дані). Вхідні дані одразу розгалужуються, надходячи одночасно до двох спеціалізованих компонентів моделі.

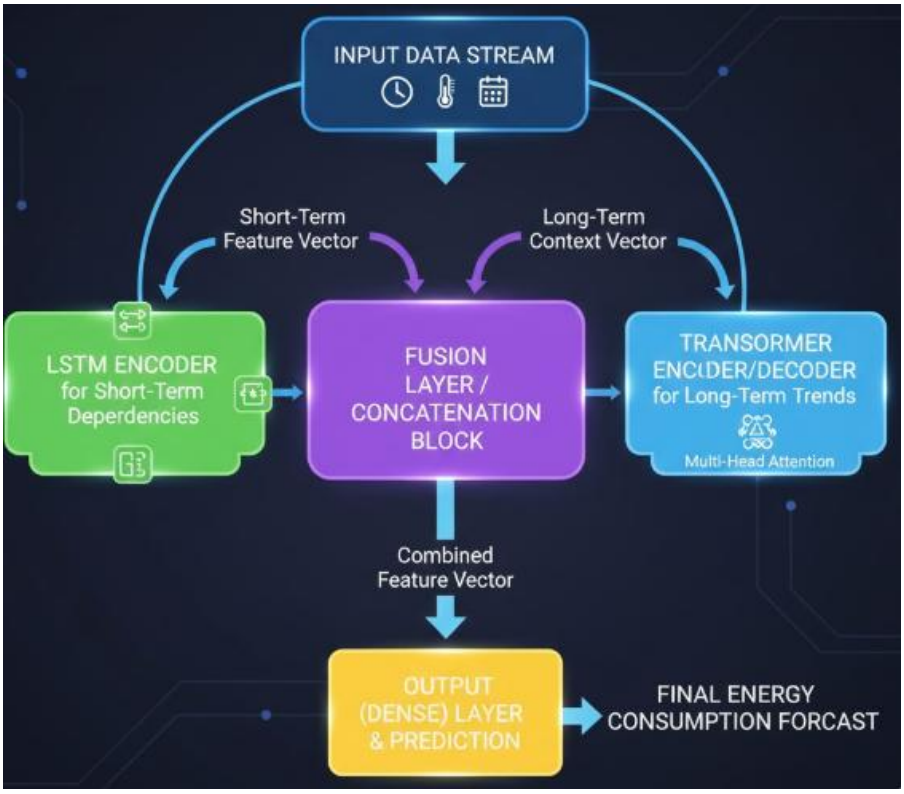


Рис. 1 Структурна схема гібридної архітектури енергоспоживання

Перший компонент — LSTM кодувальник для короткострокових залежностей (LSTM Encoder for Short-Term Dependencies) відповідає за захоплення локальних, послідовних патернів і короткострокових коливань у даних, що є критичними для прогнозування на найближчі години або дні; LSTM ефективно обробляє рекурентні зв'язки у послідовностях, результатом чого є вектор короткострокових ознак (Short-Term Feature Vector).

Паралельно працює трансформер для довгострокових трендів (Transformer Encoder/Decoder for Long-Term Trends), який використовує механізм багатошарової уваги (Multi-Head Attention) та ідентифікації глобальних, сезонних і трендових залежностей на великих часових проміжках, оскільки йому легше моделювати залежність між віддаленими точками часового ряду. Даний блок генерує вектор довгострокового контексту (Long-Term Context Vector).

Наступним кроком є блок об'єднання / злиття (Fusion Layer / Concatenation Block), який приймає два незалежні вектори ознак: короткостроковий від LSTM та довгостроковий від трансформера. Дані вектори конкатенуються (об'єднуються) або проходять через спеціалізований механізм зважування, щоб отримати єдине, комплексне представлення стану системи.

Фінальний вихідний прошарок прогнозування (Output Layer & Prediction) є повністю зв'язаним прошарком (Dense Layer), приймає об'єднаний вектор ознак і генерує фінальний прогноз енергоспоживання (Final Energy Consumption Forecast). Даний прогноз є результатом узгодження короткострокових коливань та загальних тенденцій.

Емпірична апробація, проведена на реальних операційних даних енергомережі м. Києва за період 2019–2024 рр., продемонструвала значне підвищення якості прогнозів: середня абсолютна похибка (MAE) знизилася на 18 % порівняно з еталонною класичною моделлю ARIMA. Запровадження механізму самоадаптації дозволило системі зберігати стабільну прогностичну точність навіть в умовах динамічних змін навколишнього середовища та нестабільності попиту. Крім того, застосування алгоритму кластеризації K-means забезпечило можливість автоматичної ідентифікації та групування різних типів споживачів, що критично важливо для формування персоналізованих профілів енергоспоживання.

Таким чином, гібридна архітектура забезпечує підвищену точність прогнозування, оскільки використовує LSTM для деталізації поточної ситуації та Трансформер для забезпечення контекстуальної корекції на основі глобальних патернів.

Висновки та перспективи. Наведена інтелектуальна система прогнозування енергоспоживання на базі ШІ продемонструвала високу прогностичну точність, операційну стабільність та адаптивність у реальних експлуатаційних умовах. Інтеграція методів глибинного навчання у процес оперативного управління енергоресурсами відкриває шлях до значної оптимізації навантаження на енергомережі, зниження експлуатаційних витрат та прискорення переходу до загальносвітової концепції «розумної енергетики» (Smart Grid). Подальші наукові дослідження доцільно сфокусувати на розширенні архітектури моделі для підтримки мультиагентних Smart Grid-систем, а також на інтеграції з алгоритмами прогнозування відновлюваних джерел енергії для створення єдиного, оптимізованого енергетичного ланцюжка.

Список використаних джерел

1. Hong T., Fan S. Probabilistic Electric Load Forecasting: A Tutorial Review // International Journal of Forecasting. 2016. Vol. 32, No. 3, pp. 914–938.

2. Raza M. Q., Khosravi A. A Review on Artificial Intelligence-based Load Demand Forecasting Techniques for Smart Grid and Buildings // Renewable and Sustainable Energy Reviews. 2015. Vol. 50, pp. 1352–1372.

3. Li Y., Chen H., Zhang Y. Deep Learning Models for Short-term Load Forecasting in Smart Grids // IEEE Access. 2023. Vol. 11, pp. 18742–18756.

4. Сидоренко Д. Інтелектуальні системи прогнозування енергоспоживання у міських мережах // Вісник Національного технічного університету України «КПІ». 2024. № 2, С. 73–81.

5. Vaswani A. et al. Attention Is All You Need // Advances in Neural Information Processing Systems (NeurIPS). 2017

Івасюк Василь Васильович
магістрант 1 курсу, групи ІПЗм-1
Карпатський національний університет
імені Василя Стефаника
+380 (342) 59-60-58
vasyl.ivasiuk.21@pnu.edu.ua

ОГЛЯД СУЧАСНОГО СТАНУ СИСТЕМ ВИЯВЛЕННЯ ТА ІНФОРМУВАННЯ ПРО НАЯВНІСТЬ ЗАСТАРІЛОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Постановка задачі

Застарівання програмного забезпечення (ПЗ) є однією з рушійною сил, що зумовлює покращення програмного коду та усунення ризикованих ситуацій. Двома ознаками застарівання є депрекація та занедбання, кожна з яких є об'єктом численних наукових публікацій. Одним з досліджуваних питань є пошук методів та реалізацій для визначення стану залежностей, які нададуть змогу розробникам вчасно реагувати на ситуації занепаду тих чи інших пакетів. В свою чергу, це позитивно впливає на надійність ПЗ.

Мета дослідження

Метою цього дослідження є огляд сучасного стану систем виявлення депрекації та занедбання ПЗ, які були опубліковані протягом останніх 5 років; визначення основних результатів робіт.

Результати дослідження

У роботі [1] дослідники зосереджуються на визначенні масштабу занедбання проєктів, реагуванні розробників у випадку припинення підтримки та обізнаності цього факту серед інших розробників. Для аналізу цих питань було відібрано 28,100 широко використовуваних пакетів з екосистеми npm. Протягом шестирічного періоду спостереження було виявлено, що 15% серед них були закинуті. Після крайнього терміну, чий період склав майже 3 роки, було визначено, що 18% безпосередньо залежних проектів вилучили недіючі залежності; середній час вилучення становить 13,5 місяців. При цьому, виправлення безпеки встановлюються швидше, аніж інші оновлення. При визначенні факторів, які найсильніше впливають на усунення таких залежностей, було окреслено активність розробки та наявність зрілості управління. Ще одним показником є наявність чіткого повідомлення про припинення підтримки або архівування репозиторію. Хоча автори глибоко проаналізували явище занедбання, саме розробка ефективних способів інформування стану обслуговування пакетів, на їхню думку, має стати ціллю наступних досліджень. Подібне запитання поставили автори статті [2], взявшись за природу занедбання бібліотек в екосистемі Maven. Їхнє дослідження спирається на припущення, що уповільнення швидкості випуску версій наштовхує на кінцевий занепад проєктів. Набір даних містить 400,000 унікальних бібліотек, які були створені протягом 10-річного періоду спостереження. Станом на 2023 рік, близько половини бібліотек виявилась

закинутою, а щорічний рівень занепаду перевищує 20%. Серед неактивних бібліотек, 60% з них є недовготривалими, а найчастішим патерном є різке убавляння активності. Як підсумок, автори змогли довести власне припущення, що на їхню думку підкреслює важливість реагування на занедбання бібліотек. В якості рішень пропонується запровадження автоматичних сповіщень, які виявляють ознаки потенційного згасання. Ще одним способом визначення застарівання пакетів є центральність, яка розглядається в статті [3]. На думку дослідників, саме вона краще передбачає ймовірний занепад пакетів проти кількості залежностей та завантажень, оскільки вона може вказувати на наявність кращих альтернатив або зсуву зацікавленості спільноти. Для дослідження було розроблено три різні набори даних, які засновані на екосистемі npm. В підсумку було виявлено, що цей підхід виявляє 87% пакетів в занепаді з точністю 0.80. Щодо часу виявлення стану занепаду, цей показник складає 18 місяців до зниження рівня рейтингу та 16 місяця до виведення з вжитку. В якості практичної реалізації було створено розширення для браузера. Питання депрекації у екосистемі Python проаналізовано у роботі [4]. Python не має офіційного механізму депрекації на рівні пакетів, що призводить до малої обізнаності щодо їхнього поточного стану. Автори виявили близько 9,000 застарілих пакетів, над якими був проведений аналіз впливу повідомлення про припинення підтримки. Крім того, вони провели опитування серед розробників та користувачів неактивних пакетів. За її результатами, три чверті розробників не бажають оголосити про депрекацію, в основному через брак часу та ресурсів. Водночас більшість користувачів висловлюють бажання отримувати такі повідомлення та вжити відповідних заходів. Наявність самих оголошень є корисним для визначень того, чи використовувати певний пакет, чи ні. Серед наведених висновків, один з них стосується інформування користувачів щодо альтернативних рішень.

Висновки та перспективи

Незалежно від мови програмування та екосистеми, питання застарівання ПЗ є актуальним як для розробників, так і для користувачів. Розробники неактивних пакетів не мають сильного бажання повідомляти про занедбання проєктів. Користувачі таких пакетів, навпаки, висловлюють зацікавленість щодо стану їхнього обслуговування. Аналіз досліджень підтверджує потребу у механізмах прогнозування часу безперервної роботи та інформування таких проєктів, робота над якими призупинена та інтеграції в системи оцінювання якості ПЗ [5]. Аналіз досліджень підтверджує потребу створити механізм для прогнозування часу безперервної роботи та інформування таких проєктів, робота над якими призупинена або які рекомендовано замінити.

Список використаних джерел

1. C. Miller, M. Jahanshahi, A. Mockus, B. Vasilescu and C. Kastner, "Understanding the Response to Open-Source Dependency Abandonment in the npm Ecosystem," 2025 IEEE/ACM 47th International Conference on Software Engineering (ICSE), Ottawa, ON, Canada, 2025, pp. 2355-2367, doi: 10.1109/ICSE55347.2025.00004

2. K. A. Hasan, J. Yasmin, H. Hao та Y. Tian, “Understanding Abandonment and Slowdown Dynamics in the Maven Ecosystem,” Feb. 2025, doi: 10.48550/arXiv.2502.00615

3. S. Mujahid, D. E. Costa, R. Abdalkareem, E. Shihab, M. A. Saied and B. Adams, "Toward Using Package Centrality Trend to Identify Packages in Decline," in IEEE Transactions on Engineering Management, vol. 69, no. 6, pp. 3618-3632, Dec. 2022, doi: 10.1109/TEM.2021.3122012

4. Z. Zhong, S. He, H. Wang, B. Yu, H. Yang and P. He, "An Empirical Study on Package-Level Deprecation in Python Ecosystem," 2025 IEEE/ACM 47th International Conference on Software Engineering (ICSE), Ottawa, ON, Canada, 2025, pp. 66-77, doi: 10.1109/ICSE55347.2025.00046

5. M. Kuz et al., "Methods for evaluating software accessibility," Radio Electronics, Computer Science, Control, no. 3, pp. 163-172, Sept. 22, 2025, doi: 10.15588/1607-3274-2025-3-15

Анотація

В цьому матеріалі був проведений огляд публікацій, які досліджують сучасний стан систем виявлення депрекації та занедбання у екосистемах npm, Maven та Python. Визначено, як дослідники аналізують причини занедбання проєктів у різних екосистемах, розповсюдженість такого явища, та реакцію розробників та користувачів щодо вилучення неактивних залежностей. Були взяті до уваги запропоновані рішення, які попереджують ймовірний занепад проєкту, а також досліджено показники ефективності таких рішень. Аналіз досліджень допоміг визначити потреби та виклики при створенні механізму прогнозування часу безперервної роботи ПЗ.

Abstract

This paper reviews publications that examine the current state of systems for detecting depression and abandonment in the npm, Maven, and Python ecosystems. It was determined how researchers analyse the causes of project abandonment in different ecosystems, the prevalence of this phenomenon, and the reaction of developers and users to the removal of inactive dependencies. Proposed solutions that prevent the likely decline of a project were taken into account, and the effectiveness of such solutions was investigated. The analysis of the studies helped to identify the needs and challenges in creating a mechanism for predicting the continuous operation time of software.

Слюсар Владислав Сергійович
студент 6 курсу, групи КСДМ-61
Державного університету
інформаційно-комунікаційних технологій
м. Київ
slyusar33@gmail.com
Токар Микита Денисович
студент 6 курсу, групи КСДМ-61
Державного університету
інформаційно-комунікаційних технологій
м. Київ
reivenfoxerror@gmail.com

ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ РОЗПІЗНАВАННЯ МАТЕМАТИЧНИХ ФОРМУЛ НА ОСНОВІ АРХІТЕКТУРИ YOLOv5

Постановка задачі. Автоматизована обробка математичних текстів є актуальною проблемою в галузі цифровізації освіти та наукового документообігу. Традиційні методи оптичного розпізнавання символів та рекурентні нейронні мережі, що розглядають дані послідовно, мають суттєві обмеження у швидкодії та не дозволяють ефективно розпаралелювати обчислення. Водночас математичні формули мають складну двовимірну структуру, де важливим є не лише розпізнавання символу, а і його просторове розташування. Це зумовлює необхідність застосування згорткових нейронних мереж, які здатні автоматично виділяти ієрархічні ознаки зображення та забезпечувати роботу в режимі реального часу.

Мета дослідження. Метою дослідження є система для детектування й розпізнавання рукописних і друкованих математичних виразів шляхом застосування архітектури YOLOv5, що дозволить забезпечити баланс між обчислювальною ефективністю та точністю класифікації об’єктів.

Результати дослідження. У ході роботи було запропоновано двоетапний підхід до розпізнавання. На першому етапі нейронна мережа локалізує та виділяє цілісну область формули на зображенні, відсікаючи фоновий шум. На другому етапі відбувається детекція окремих символів у межах виділеної області. Як базову архітектуру пропонується модель YOLOv5s, яка демонструє найкращі показники швидкості порівняно з іншими модифікаціями. Для навчання системи досліджено два унікальні набори даних: 721 зображення для детекції формул та 899 зображень для розпізнавання символів. Використання функції втрат Focal Loss дозволить мінімізувати вплив дисбалансу класів. Під час експерименту перевірка показала високу ефективність запропонованого підходу: метрика mAP@0.5 для детектора формул склала 0,983 , а для детектора символів — 0,898.

Висновки та перспективи. Запропонована система доводить свою ефективність, забезпечуючи високу точність локалізації 98,3% та класифікації математичних об'єктів. Застосування архітектури YOLOv5 дозволяє уникнути проблем зі зникаючим градієнтом, властивих RNN, та суттєво пришвидшити

процес інференсу. Перспективи подальших досліджень полягають у розширенні навчальної вибірки для підтримки складніших математичних структур та інтеграції розроблених алгоритмів у мобільні застосунки для розв’язання задач у реальному часі.

Список використаних джерел:

1. Jocher G. YOLOv5 by Ultralytics. 2020. URL: https://github.com/ultralytics/yolov5.

2. Redmon J., Divvala S., Girshick R., Farhadi A. "You Only Look Once: Unified, Real-Time Object Detection." Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR). 2016. pp. 779-788.

Костюк Б.Р.
Кам’янський енергетичний фаховий коледж
викладач Петренко Ю.О.

СУЧАСНІ ПІДХОДИ ДО ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ КОМП’ЮТЕРНИХ МЕРЕЖ В УМОВАХ ЗРОСТАННЯ КІБЕРЗАГРОЗ

Метою даного докладу є аналіз сучасних методів забезпечення безпеки комп’ютерних мереж, дослідження актуальних моделей кібератак, а також розгляд перспективних напрямів розвитку інженерії даних та мережевої безпеки у контексті зростаючих вимог до захисту інформації.

The purpose of this report is the analysis of modern methods of ensuring the security of computer networks, the study of current models of cyber attacks, as well as the consideration of promising directions for the development of data engineering and network security in the context of growing requirements for information protection.

Вступ

Стрімкий розвиток інформаційних технологій, інтернет-сервісів та хмарних інфраструктур привів до безпрецедентного зростання обсягу цифрових даних і залежності суспільства від комп’ютерних мереж. Водночас збільшується кількість кіберзагроз, спрямованих як на приватних користувачів, так і на організації критичної інфраструктури, державні установи та бізнес. За даними міжнародних аналітичних агентств, протягом останніх років кількість атак на мережеві ресурси зросла у декілька разів, що вимагає нових наукових підходів і технологічних рішень у сфері кіберзахисту.

Сучасний стан комп’ютерних мереж та їх уразливості

Сучасні мережеві системи характеризуються високою масштабованістю, гнучкістю та гетерогенністю. Окрім традиційних локальних мереж (LAN), широкого поширення набули хмарні платформи, розподілені обчислення, мобільні мережі та інтернет речей (IoT). Кожна з цих технологій формує специфічні точки уразливості.

Основні джерела ризиків включають:

— використання застарілих протоколів, які не забезпечують сучасний рівень криптографічного захисту;

— людський фактор, що залишається ключовою причиною інцидентів (фішинг, слабкі паролі, соціальна інженерія);

— прогалини у конфігурації мережевого обладнання, що дозволяють зловмиснику отримати несанкціонований доступ;

— вразливості в IoT-пристроях, які часто не мають належних механізмів аутентифікації та шифрування;

— мережеві атаки типу DDoS, спрямовані на перевантаження інфраструктури.

Усе це формує необхідність впровадження комплексного та адаптивного підходу до кіберзахисту.

Класифікація сучасних кібератак на мережеву інфраструктуру

Аналіз кібератак дозволяє виокремити кілька основних категорій, що є найбільш поширеними:

Атаки на рівні мережевих протоколів (MITM, ARP-spoofing, DNS-spoofing). Зловмисник перехоплює або модифікує трафік між учасниками мережевої взаємодії.

DDoS-атаки. Масове надсилання запитів з метою виведення сервера з ладу. У сучасних умовах використовуються ботнети IoT-пристроїв.

Експлуатація вразливостей ПЗ (RCE, SQL-injection, buffer overflow). Дозволяють отримати контроль над сервером або клієнтським пристроєм.

Атаки на канали бездротового зв'язку (Wi-Fi cracking, deauthentication attack). Спрямовані на порушення конфіденційності та доступності даних.

Соціальна інженерія та фішингові кампанії. Є максимально ефективними завдяки психологічним методам впливу.

Ці загрози вимагають впровадження комплексних систем моніторингу, виявлення аномалій та автоматизованого реагування.

Технології та методи захисту мереж

Шифрування даних є основою безпеки інформаційних потоків. Сучасні мережі використовують:

— TLS 1.3 для захисту прикладного трафіку;
— IPsec для шифрування на мережевому рівні;
— VPN-технології для створення захищених тунелів;
— криптографію на засадах ECC, яка забезпечує високий рівень захисту за меншої обчислювальної складності.

Системи виявлення та запобігання вторгненням (IDS/IPS)

IDS/IPS аналізують мережевий трафік у реальному часі, визначають відхилення від нормальної поведінки та блокують підозрілу активність. Ефективність таких систем зростає завдяки застосуванню методів машинного навчання.

Zero Trust Architecture (ZTA)

Принцип Zero Trust передбачає відсутність довіри до будь-якого елемента мережі. Кожен доступ перевіряється незалежно від місцезнаходження користувача або сервера. Це значно знижує ризик розповсюдження атак всередині мережі.

Мережева сегментація та мікросегментація

Поділ мережі на ізольовані сегменти дозволяє локалізувати атаки та обмежити можливість пересування зловмисника всередині інфраструктури.

Хмарні системи захисту та SIEM-платформи

Сучасні масштабовані мережі потребують централізованого інструментарію. SIEM-системи забезпечують:

— збір логів з усіх вузлів;
— аналіз подій безпеки;
— автоматизацію реагування (SOAR-підхід).
— Інженерія даних у системах мережевої безпеки

— Зростання обсягів трафіку робить традиційні методи аналізу малоефективними. Інженерія даних забезпечує:

— побудову потокових конвеєрів обробки даних (data pipelines);

— кластеризацію та очистку великих обсягів логів;

— використання ML/AI для аналізу поведінкових аномалій;

— розробку моделей прогнозування атак.

Особливо важливими стають технології: Apache Kafka, Elastic Stack, Spark Streaming, а також нейронні мережі для виявлення аномалій у високошвидкісному трафіку.

Перспективи розвитку кібербезпеки комп'ютерних мереж

У найближчі роки передбачається активний розвиток таких напрямів:

1. Квантово-стійка криптографія — підготовка до ери квантових обчислень.
2. Автоматизовані системи кіберзахисту на базі ШІ — зменшення втручання людини в рутинні процеси.
3. Інтеграція кіберзахисту на рівні архітектури (security-by-design) — впровадження безпеки на етапі проєктування систем.
4. Блокчейн-технології для підвищення цілісності даних.
5. Розвиток захищених мереж для IoT з урахуванням енергоефективних криптографічних алгоритмів.

Висновки

Комп'ютерні мережі є ключовим елементом сучасної цифрової інфраструктури, а їхня безпека — критичним фактором стабільності економіки, виробництва та державних систем. Розвиток кіберзагроз вимагає комплексного підходу до захисту, що включає криптографію, адаптивні системи моніторингу, архітектуру Zero Trust, застосування інженерії даних та методів штучного інтелекту.

Забезпечення безпеки мереж сьогодні — це не лише технічне, а й стратегічне завдання, що потребує постійного вдосконалення методів захисту та розвитку кваліфікації фахівців у галузі кібербезпеки.

Список літератури

1. Stallings W. Network Security Essentials: Applications and Standards. Pearson, 2020.
2. Scarfone K., Mell P. Guide to Intrusion Detection and Prevention Systems (IDPS). NIST, 2021.
3. Андрощук Г. Кібербезпека в інформаційних системах. Київ: КНУТД, 2021.

Козир Крістіна Володимирівна
студентка 3 курсу групи ШІД-31
Державний університет
інформаційно-комунікаційних технологій
Василенко Олександр Михайлович
студент 6 курсу групи ШІДМ-61
Державний університет
інформаційно-комунікаційних технологій
Кисіль Тетяна Миколаївна,
ст. викладач кафедри Штучного інтелекту
Державний університет
інформаційно-комунікаційних технологій

ГІБРИДНІ СТРАТЕГІЇ ВПРОВАДЖЕННЯ ШТУЧНОГО ІНТЕЛЕКТУ У ВИРОБНИЧИХ ПРОЦЕСАХ

Сучасна промисловість, орієнтована на концепцію Smart Manufacturing та Індустрії 4.0, вимагає переходу від реагування на збої до їхнього прогнозування та автоматичної превенції. Штучний інтелект (ШІ) є ключовим інструментом для досягнення цієї мети, проте його ефективність залежить від правильного розподілу ролей між різними архітектурами. На сьогоднішній день існує функціональний розрив між системами, які забезпечують високоточну технічну аналітику, та тими, які відповідають за швидку, безшовну взаємодію з людиною і виконання оперативних бізнес-процесів. Скорочення цього розриву критично важливе для максимізації фінансових ефектів від інвестицій у цифровізацію.

Постановка проблеми. Традиційна інтеграція ШІ часто фокусується або лише на вузькому прогнозуванні (нейронні мережі) або на спрощенні комунікації (цифрові помічники). Це призводить до розриву: технічні висновки моделей глибокого навчання (виявлення аномалії якості за допомогою E-nose) не завжди миттєво та коректно трансформуються у дію, створюючи інтерфейсне тертя і затримки у прийнятті рішень. Виникає нагальна потреба у розробці та дослідженні гібридної архітектури, де нейронні мережі виконують роль точного аналітика, а цифровий помічник виступає в ролі організатора, забезпечуючи автоматичне доведення технічних висновків до виконавця та корпоративних систем.

Мета дослідження. Метою дослідження є узагальнення ключових функціональних ролей штучного інтелекту у виробничому контексті, формування чітких критеріїв для диференціації задач між нейронними мережами та цифровими помічниками, а також демонстрація економічної та архітектурної ефективності комбінованого гібридного підходу для забезпечення аналітичних висновків у виробничі рішення.

Результати дослідження. Застосування нейронних мереж є домінуючим у сферах, що вимагають технічної точності та роботи з неструктурованими даними. Це включає візуальний контроль якості, де НМ навчаються на розмічених зображеннях для виявлення браку на конвеєрі, оцінюючи їх якість за

відповідними метриками і досягаючи значного фінансового ефекту. НМ є основою предиктивного обслуговування (PdM), де моделі часових рядів ідентифікують аномалії у вібрації або температурі для попередження відмов, що оцінюється за PR-AUC та Recall, забезпечуючи зменшення незапланованих простоїв на 30-50%.

На противагу, цифровий помічник є ШІ-системою, яка виконує роль взаємодії, пошуку знань та виступає керівником бізнес-процесів (CMMS, ERP, MES). Основна їх функція — забезпечити комунікації між оператором та системою, дозволяючи швидко створювати заявки, перевіряти статуси, забезпечувати відповідні інструкції голосом/чатом. Ефективність помічника оцінюється із загальним орієнтовним ефектом економії часу до 25-35%.

Пропонується комбінований підхід інтеграції комп'ютерного нюху (E-nose) у виробництво, наприклад, для моніторингу якості ферментації. У цьому сценарії, нейронна мережа отримує високорозмірний вектор відгуку від масиву сенсорів E-nose і виконує вузькоспеціалізоване, точне розпізнавання наявності небажаних летких сполук. У разі детектування критичної аномалії, вона передає сигнал цифровому помічнику, який автоматично ініціює діалог з технологом, надає чіткий інструктаж усунення проблеми за технічних довідників та формує відповідний акт про брак у системі управління запасами. НМ забезпечує технічну точність детекції, а помічник відповідає за швидке та вірне прийняття рішення (рис. 1).

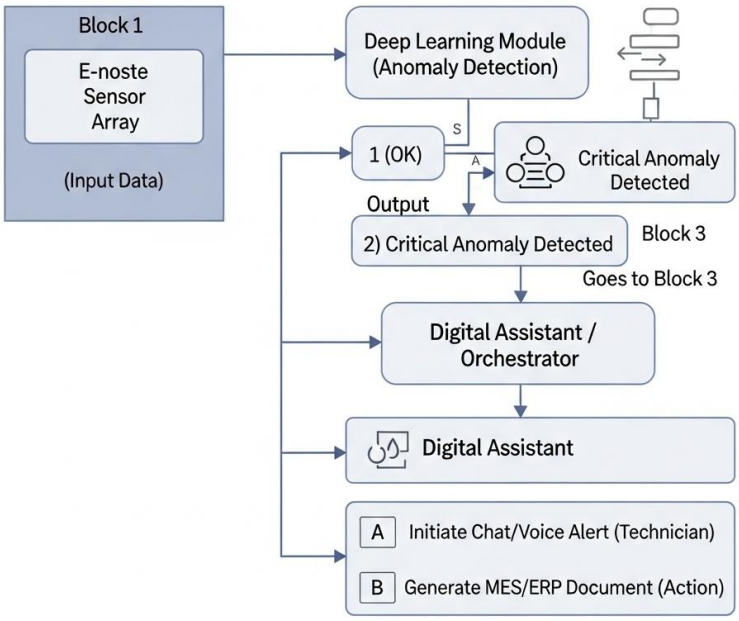


Рис. 1. Архітектура гібридної системи керування виробничими процесами

Гібридна архітектура розроблена для забезпечення високоточного контролю якості у виробничих процесах, зокрема, для моніторингу ферментації. Вона ефективно поєднує вузьку технічну аналітику з широкою операційною взаємодією. Основою системи є масив сенсорів E-nose, який безперервно збирає високорозмірні дані сполуки в зоні ферментації, і даний вхідний сигнал миттєво передається до модуля глибокого навчання.

Модуль глибокого навчання виконує критично важливу технічну роль, використовуючи моделі CNN та/або LSTM, для точної класифікації запахів та

виявлення прихованих критичних аномалій — ознак псування або порушення технологічного процесу. Якщо якість знаходиться в межах норми, позитивний сигнал повертається до загальної виробничої системи. Однак, у разі виявлення критичної аномалії, цей модуль генерує активаційний сигнал, який автоматично передається до другого ключового елемента системи.

Цим елементом є цифровий помічник, який виконує процесну роль, забезпечуючи реакції реагування. Отримавши сигнал тривоги від нейронної мережі, помічник негайно трансформує аналітичні дані у дію. Це відбувається за двома основними напрямками: по-перше, він ініціює швидку взаємодію з людиною (наприклад, чат- або голосове сповіщення) для надання технологу чіткого інструктажу з усунення проблеми, витягнутого з бази знань; по-друге, він автоматично оновлює внутрішні бізнес-системи, генеруючи необхідні документи (акти про брак, заявки на коригувальні роботи), забезпечуючи безшовну інтеграцію між інтелектуальною аналітикою та корпоративними процесами.

Висновки та перспективи. Проведене дослідження підтверджує, що нейронні мережі та цифрові помічники не є взаємозамінними конкурентами, а елементами, що виконують різні, але критично важливі ролі у сучасному промисловому IT-ландшафті. НМ є оптимальним інструментом для вирішення вузьких, вимірюваних технічних задач, таких як предиктивне обслуговування, візуальний контроль та точна аналітика сенсорних даних, як у випадку з інтеграцією E-nose. Найбільша цінність досягається саме через їхній гібридний синтез, де аналітика НМ миттєво трансформується у дію через людино-машинний інтерфейс помічника.

Подальші дослідження та практичне впровадження мають зосередитися на розробці більш стандартизованих протоколів обміну даними між модулями глибокого навчання та платформами цифрових помічників, що підтримують MES та ERP системи. Перспективним напрямком є впровадження адаптивних моделей MLOps, які дозволять автоматично коригувати дрейф НМ на основі зворотного зв'язку, отриманого через цифрового помічника від операторів.

Список використаних джерел

1. Smith, A. B., & Johnson, C. D. (2023). Hybrid AI Architectures in Industrial Automation: Synergistic Roles of Deep Learning and Conversational Agents. Journal of Smart Manufacturing Systems, 15(2), 125-140.

2. Chen, F., Wang, Y., & Li, Z. (2022). Predictive Maintenance with Sensor Fusion: A Deep Learning Approach for Anomaly Detection in Critical Infrastructure. IEEE Transactions on Industrial Informatics, 18(4), 2350-2359.

3. García, R., Pérez, S., & Almagro, A. (2020). E-Nose Technology and Machine Learning for Real-Time Quality Control in Food Fermentation Processes. Food Control, 118, 107380.

4. AWS. (2021). Optimizing Operational Efficiency: The Business Value of Industrial Machine Learning on the Edge. (White Paper). Amazon Web Services.

5. IBM. (2019). The Role of AI Assistants in Field Service Management: Closing the Knowledge Gap. IBM Watson IoT Reports.

Донченко Антон Валентинович
Студент Державного торговельно-економічного університету
ФІТ 1-7М

АРХІТЕКТУРНА КОНВЕРГЕНЦІЯ КІБЕРБЕЗПЕКИ ТА ІНЖЕНЕРІЇ ДАНИХ У ЕКОСИСТЕМАХ СМАРТКОНТРАКТІВ

Анотація

У добу Web3 децентралізовані системи трансформуються зі спрощених транзакційних реєстрів у складні програмні середовища. Фундаментальним викликом стає забезпечення безпеки смартконтрактів в умовах жорстких обмежень віртуальної машини Ethereum (EVM) та необхідності обробки великих масивів даних. Ефективність сучасних рішень залежить від гібридних архітектур, що поєднують on-chain логіку з off-chain інфраструктурою.

Abstract

In the Web3 era, decentralized systems are transforming from simple transaction ledgers into complex software environments. The fundamental challenge lies in ensuring smart contract security under the strict constraints of the Ethereum Virtual Machine (EVM) and the need to process large datasets. The effectiveness of modern solutions depends on hybrid architectures combining on-chain logic with off-chain infrastructure.

Ключові слова: смартконтракт, EVM, кібербезпека, інженерія даних, оракули, ZK-співпроцесори, IPFS.

Сучасна екосистема децентралізованих обчислень функціонує в умовах ворожого середовища, де кожен вузол мережі є потенційно зловмисним. Розуміння ландшафту безпеки вимагає деконструкції середовища виконання — віртуальної машини Ethereum (EVM). Вона діє як ізольована «пісочниця», що не має доступу до мережевих ресурсів, гарантуючи детермінізм виконання транзакцій.

Однак ця ізоляція створює «Проблему оракула»: контракти не можуть самостійно отримувати зовнішні дані, такі як ціни активів або результати подій. Це змушує розробників впроваджувати механізми доставки даних, які стають критичними векторами атак. Окремим захисним бар'єром виступає механізм газу, що накладає економічні обмеження на обчислення.

Попри захисну функцію, механізм газу створює вразливість Block Gas Limit DoS. Якщо контракт містить ітерації по масивах необмеженого розміру, зловмисник може «роздути» стан, зробивши виконання транзакції неможливим через перевищення ліміту блоку. Інженерним рішенням є патерн «Pull over Push», де користувачі самостійно ініціюють транзакції для отримання активів, оплачуючи газ.

Аналіз вразливостей, зокрема згідно з OWASP Smart Contract Top 10, демонструє перехід від простих помилок кодування до складних маніпуляцій логікою. Найбільш руйнівною загрозою залишається атака повторного входу (Reentrancy). Вона виникає, коли зовнішній виклик дозволяє зловмиснику

повторно увійти у функцію до оновлення стану балансу жертви. Для протидії цьому використовується патерн Checks-Effects-Interactions (CEI).

Таблиця 1

Порівняння етапів виконання транзакції при застосуванні патерну CEI

Етап	**Дія**	**Мета безпеки**
1. Check	Перевірка умов (require)	Валідація прав доступу та вхідних даних
2. Effect	Оновлення стану	Фіксація змін у внутрішньому реєстрі до взаємодії
3. Interaction	Зовнішній виклик	Виконання переказу коштів або виклику іншого контракту

Ефективна архітектура вимагає гібридного підходу до управління даними. Зберігання інформації безпосередньо в блокчейні (on-chain) є надзвичайно дорогим (операція запису SSTORE коштує 20 000 одиниць газу). Тому блокчейн використовується виключно для критичних даних консенсусу, а великі масиви інформації виносяться в децентралізовані сховища, такі як IPFS.

У цій моделі смартконтракт зберігає лише криптографічний хеш файлу (CID), який діє як незмінний покажчик. Це гарантує цілісність даних: будь-яка зміна файлу призведе до зміни його хешу, що буде відхилено контрактом.

Для забезпечення моніторингу та безпеки інтерфейсів користувача сирі дані блокчейну трансформуються через ETL-пайплайни. Протокол The Graph дозволяє індексувати події смартконтрактів та створювати API (сабграфи) для швидкого доступу до історичних даних, що є критичним для форензіки та розслідування інцидентів.

Перспективним напрямом розвитку є ZK-співпроцесори (Zero-Knowledge Coprocessors). Вони дозволяють виконувати важкі обчислення над історичними даними off-chain, генеруючи математичний доказ коректності (ZKP), який дешево верифікується на блокчейні. Це відкриває шлях до створення довірених систем аналітики та скорингу без розкриття приватних даних.

Забезпечення безпеки смартконтрактів вимагає переходу від статичного аналізу коду до комплексної інженерії даних. Найстійкіші системи використовують багаторівневий підхід: впровадження архітектурних патернів (CEI), використання децентралізованих оракулів для захисту від маніпуляцій цінами, винесення "важких" даних в IPFS та застосування ZK-технологій для розширення обчислювальних можливостей без шкоди для децентралізації.

Перелік посилань:

1. Obruchkov A. What Every Blockchain Developer Should Know About EVM Internals– Part 1. https://medium.com. URL:

https://medium.com/@andrey_obruchkov/what-every-blockchain-developer-should-know-about-evm-internals-part-1-83a93c618257 (дата звернення: 20.11.2025).

2. Chainlink Education Hub. The Blockchain Oracle Problem. https://chain.link. URL: https://chain.link/education-hub/oracle-problem (дата звернення: 21.11.2025).

3. Stack Overflow. How to store IPFS hash on Ethereum blockchain using smart contracts? https://stackoverflow.com. URL: https://stackoverflow.com/questions/66927626 (дата звернення: 21.11.2025).

4. ETHGlobal Bangkok 2024. Indexing Smart Contract Data with The Graph. https://www.youtube.com. URL: https://www.youtube.com/watch?v=kL96MHCt3EM (дата звернення: 21.11.2025).

5. Zhao J. Brevis Research Report: The Infinite Verifiable Computing Layer of zkVM and ZK Data Coprocessor. https://medium.com. URL: https://medium.com/@0xjacobzhao/brevis-research-report (дата звернення: 21.11.2025).

Дикий Назар Володимирович
Студент 6 курсу, групи ШІДМ-61
Державний університет
інформаційно-комунікаційних технологій, м. Київ
Звенігородський Олександр Сергійович,
д.т.н., доцент кафедри Штучного Інтелекту
Державний університет
інформаційно-комунікаційних технологій, м. Київ

ЗАСТОСУВАННЯ ГЛИБОКИХ НЕЙРОМЕРЕЖЕВИХ МОДЕЛЕЙ ДЛЯ АДАПТИВНОЇ ОПТИМІЗАЦІЇ УПРАВЛІННЯ МІСЬКИМ ТРАНСПОРТНИМ ТРАФІКОМ

Управління дорожнім рухом у великих агломераціях становить багатофакторну задачу, що вимагає точного прогнозування інтенсивності транспортних потоків та динамічної оптимізації роботи світлофорних об'єктів. Використання глибинних нейромережевих моделей (Deep Neural Networks) дозволяє принципово покращити ці процеси завдяки їхній здатності до ефективної обробки великомасштабних, різнорідних та часозалежних даних, отриманих із детекторів руху, камер спостереження та GPS-пристроїв.

Постановка задачі. Проблема полягає в тому, що традиційні алгоритми управління не завжди справляються зі змінними та непередбачуваними дорожніми ситуаціями, що призводить до неефективного використання інфраструктури та зростання заторів. Необхідно розробити інтелектуальну систему, що використовує машинне навчання для адаптивного та проактивного управління. Задача полягає у створенні алгоритмічної моделі, здатної інтегрувати просторово-часові залежності транспортного потоку, що дозволить системі адаптивно коригувати режими роботи світлофорів для мінімізації черг, скорочення середнього часу поїздки та мінімізації екологічних втрат.

Мета дослідження. Метою дослідження є аналіз та експериментальна оцінка можливостей застосування рекурентних (RNN) та графових (GNN) нейромережевих архітектур для оптимізації процесів управління дорожнім рухом. Основний фокус спрямований на визначення найбільш ефективних топологій нейронних мереж для прогнозування параметрів потоку (щільність, швидкість) та їхнє застосування у контексті адаптивного регулювання роботи світлофорів. Кінцевою метою є кількісне підтвердження практичної ефективності цих моделей у міському середовищі, зокрема у зменшенні заторів, скороченні середнього часу поїздки та мінімізації екологічних втрат (викидів CO2) від транспортних потоків.

Результати дослідження. У рамках роботи було розроблено гібридну нейромережеву модель (рис. 1), яка реалізує механізм адаптивної корекції фаз світлофорного об'єкта. Модель здійснює комплексний аналіз і прогнозування інтенсивності руху на основі інтеграції даних, отриманих із детекторів руху, камер спостереження (для оцінки щільності) та GPS-пристроїв (для оцінки швидкості). Встановлено, що архітектура, заснована на LSTM-блоках з

інтеграцією просторового контексту за допомогою згорткових нейронних мереж (CNN), демонструє високу точність прогнозування та стабільність роботи в умовах змінних та непередбачуваних ситуацій на дорогах. Експериментальні дослідження показали, що застосування моделі призводить до зниження затримок транспорту до 30% та підвищення загальної ефективності адаптивного управління рухом.

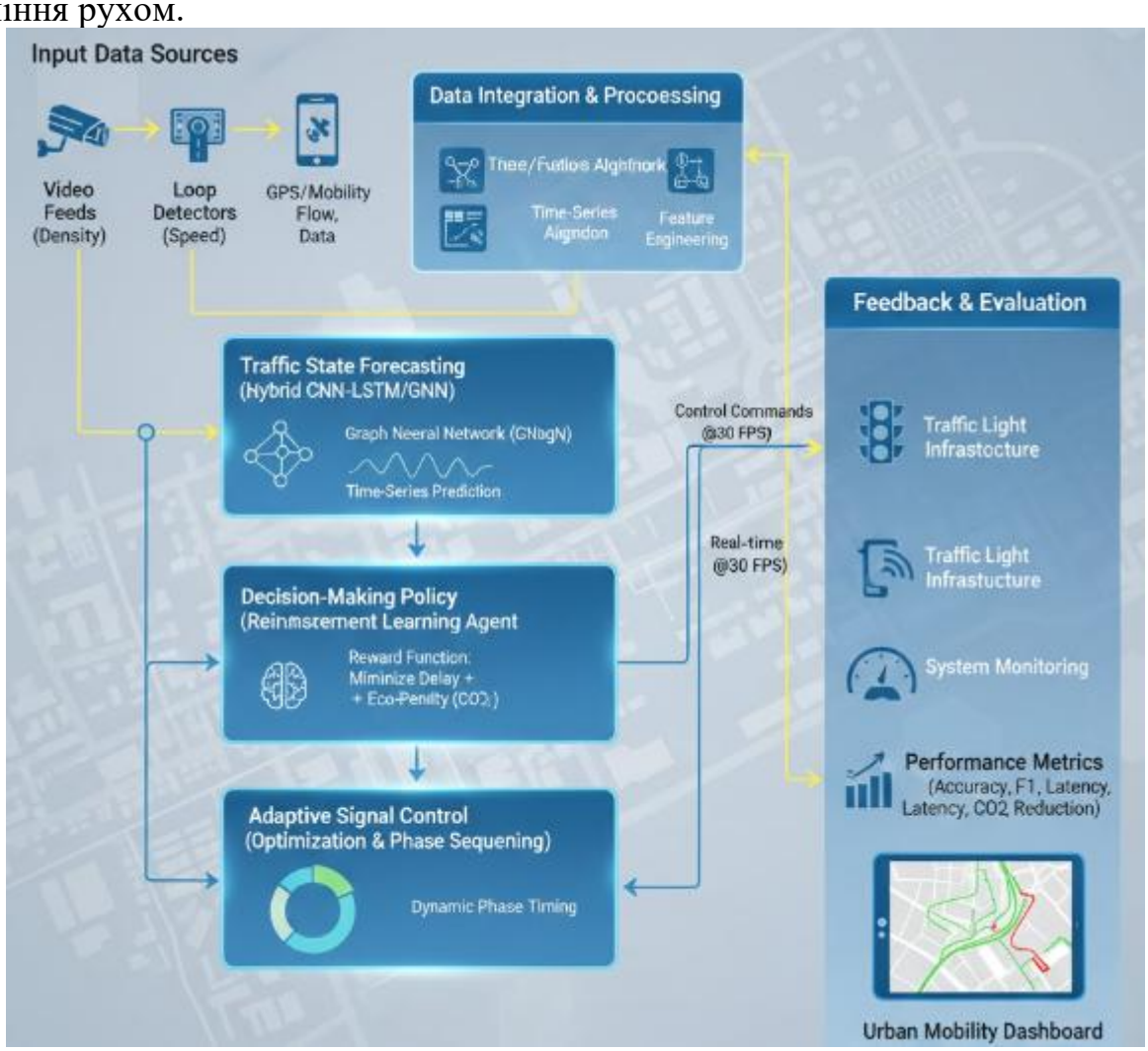


Рис. 1 - Архітектура інтелектуальної системи управління міським транспортним трафіком

Для подальшої оптимізації пропонується перейти від прогностичної моделі до системи, що приймає рішення, використовуючи навчання з підкріпленням (RL). В даній системі агент RL (контролер світлофора) навчається обирати фази, використовуючи функцію винагороди, яка включає не лише традиційні параметри (мінімізація черги та часу очікування), але й екологічний штраф. Даний штраф безпосередньо залежить від кількості простоюючих автомобілів та часу їх холостого ходу, що дозволяє системі приймати рішення, які одночасно знижують затори і мінімізують викиди CO2 на вузлових перехрестях.

Висновки та перспективи. Отримані результати переконливо доводять високу ефективність застосування глибоких нейромережевих моделей для проактивного управління міським трафіком. Інтеграція таких моделей у сучасні транспортні системи дозволяє суттєво знизити навантаження на вузлові перехрестя та покращити загальний потік транспорту. Подальші дослідження

будуть спрямовані на удосконалення алгоритмів, зокрема на масштабування архітектури на основі графових нейронних мереж (GNN) для моделювання складної топології міської мережі та на реалізацію запропонованої RL-моделі з екологічно зваженою функцією винагороди. Це є критично важливим кроком для інтеграції розроблених інтелектуальних систем у вже існуючі міські інфраструктури керування дорожнім рухом.

Список використаних джерел:

1. Traffic Prediction using Machine Learning Algorithms // IEEE Conference Paper. [Електронний ресурс]: https://ieeexplore.ieee.org/document/9126308

2. Deep Learning Methods for Traffic Flow Prediction // MDPI Sustainability. [Електронний ресурс]: https://www.mdpi.com/2071-1050/11/3/671

3. Real-time Traffic Management System Based on Neural Networks // ResearchGate. [Електронний ресурс]: https://www.researchgate.net/publication/335744120_Real-time_Traffic_Management_System_Based_on_Neural_Networks

4. Urban Traffic Optimization using Artificial Neural Networks // ScienceDirect. [Електронний ресурс]: https://www.sciencedirect.com/science/article/pii/ S2352146521001747

Галаревич Віталій Олександрович
Студент 4 курсу, групи КІ-22-1/9
Кам`янського енергетичного фахового коледжу
м.Кам`янське
(063)-843-35-45
vogalarevich@kadet.ukr.education
Науковий керівник: Аушев Максим Олександрович
кандидат технічних наук
доцент кафедри Інженерії програмного забезпечення
Державного університету
інформаційно-комунікаційних технологій
м.Кам`янське

ВИКОРИСТАННЯ CISCO В НАВЧАЛЬНОМУ ПРОЦЕСІ, З ТОЧКИ ЗОРУ СТУДЕНТА

Анотація. У роботі розглянуто особливості використання інструментів Cisco, зокрема симулятора Packet Tracer та інтерфейсу командного рядка (CLI), у підготовці фахівців з мережевих технологій. Проаналізовано вплив практичної роботи з емуляторами на розуміння теоретичних основ та формування професійних навичок студентів. Abstract. The paper discusses the peculiarities of using Cisco tools, in particular the Packet Tracer simulator and the Command Line Interface (CLI), in the training of network technology specialists. The influence of practical work with emulators on understanding theoretical foundations and the formation of students' professional skills is analyzed.

Використання продуктів Cisco у навчальному процесі дозволяє студентам пройти шлях від розуміння того, що таке IP-адреса, до налаштування складної маршрутизації в корпоративних мережах. У цій доповіді я розгляну ключові інструменти, з якими ми працюємо, та поясню, чому вони є критично важливими для нашого професійного становлення.

Найбільшим страхом студента-початківця є можливість "зламати" дороге обладнання неправильною командою. Саме тому "серцем" нашого навчання є емулятор мережі Cisco Packet Tracer [2]. Це програма, яка дозволяє моделювати комп'ютерні мережі будь-якої складності на звичайному ноутбуці.

Для нас, студентів, Packet Tracer – це віртуальна лабораторія. Тут ми можемо додавати маршрутизатори (routers), комутатори (switches), сервери, бездротові точки доступу та кінцеві пристрої, з'єднувати їх різними типами кабелів і спостерігати, як це все працює разом. Це розвиває інженерне мислення: ти бачиш топологію мережі в цілому, а не просто набір дротів.

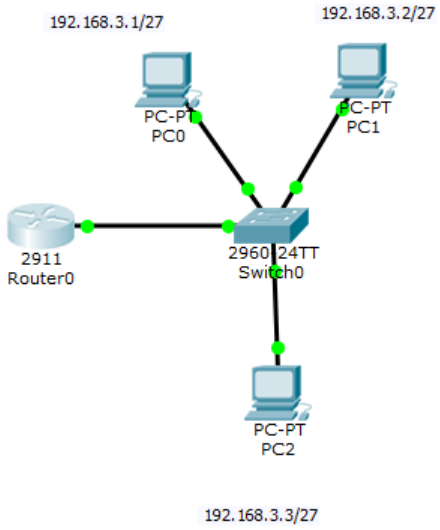


Рисунок 1 – Створення топології мережі в середовищі Cisco Packet Tracer.

Однією з найважливіших навичок, яку ми здобуваємо завдяки Cisco, є вміння працювати з інтерфейсом командного рядка (Command Line Interface – CLI). На відміну від звичайних користувацьких програм, де все робиться мишкою, професійне мережеве обладнання налаштовується командами.

На початку це здається складним, але з часом студент починає розуміти логіку IOS (Internetwork Operating System) [4]. Ми вчимося налаштовувати інтерфейси, прописувати статичні маршрути, налаштовувати DHCP та VLAN. Саме робота в консолі дає відчуття повного контролю над мережею. Коли ти вводиш команду show ip interface brief і бачиш, що всі інтерфейси підняті і працюють – це приносить справжнє задоволення від виконаної роботи.

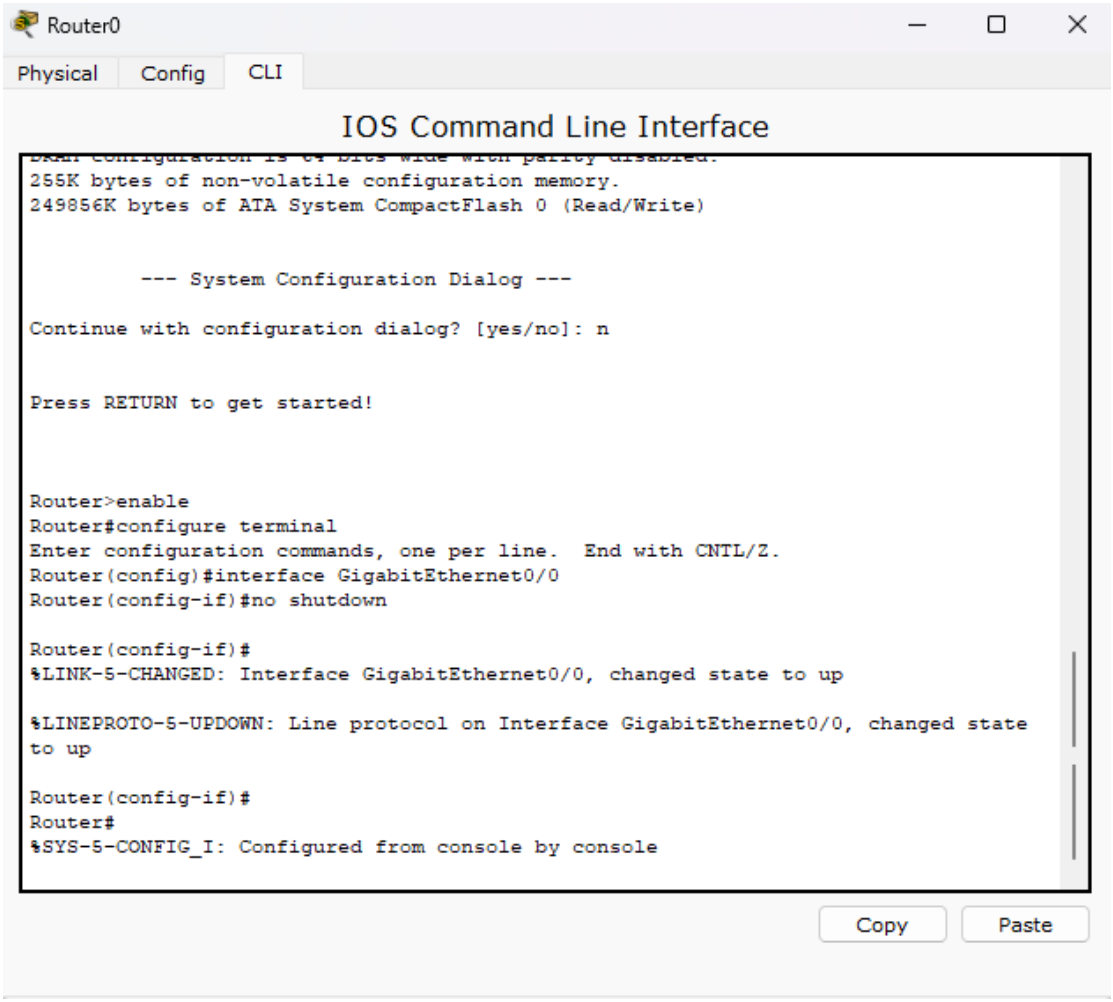


Рисунок 2 – Налаштування обладнання через командний рядок (CLI).

Теорія мереж часто буває абстрактною. Важко уявити, як саме пакет даних подорожує від одного комп'ютера до іншого, як відбувається ARP-запит або тристороннє рукостискання TCP.

У навчальному процесі ми використовуємо унікальну функцію Packet Tracer – режим симуляції (Simulation Mode). Це дозволяє нам "зупинити час" і простежити шлях конкретного пакету даних через мережу [2]. Ми можемо "розкрити" цей пакет і подивитися, яка інформація записана в його заголовках на кожному рівні моделі OSI (Ethernet-кадр, IP-пакет, TCP-сегмент). Це перетворює абстрактну теорію на наочну практику.

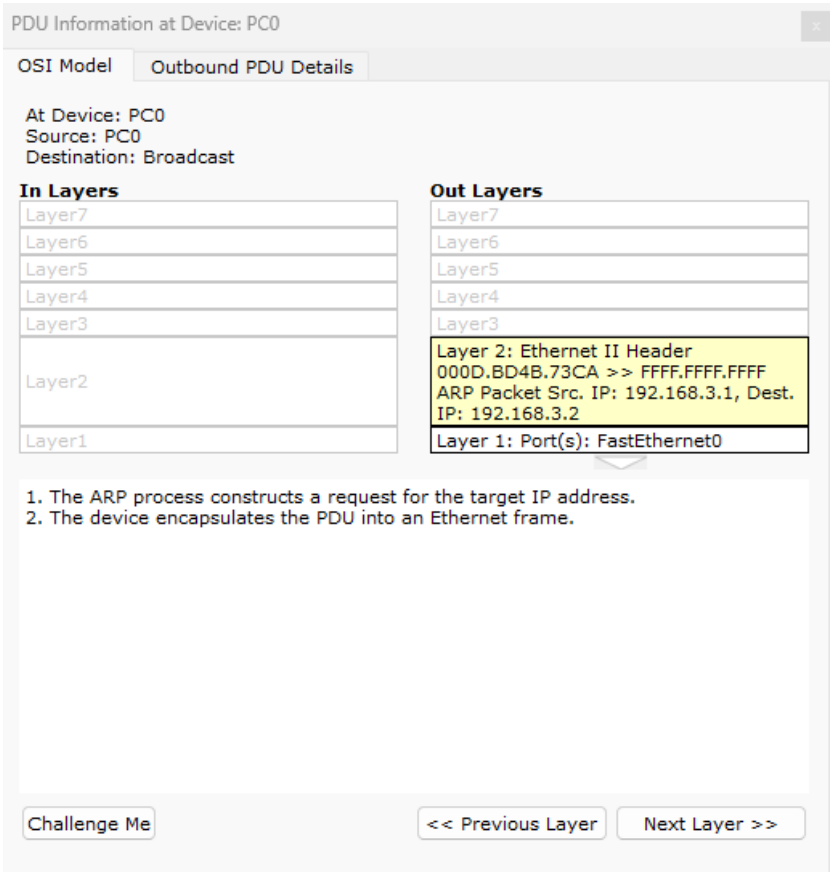


Рисунок 3 – Аналіз проходження пакетів даних у режимі симуляції.

Використання технологій Cisco в університеті – це не просто виконання лабораторних робіт заради оцінки. Це пряма підготовка до професійної сертифікації CCNA (Cisco Certified Network Associate), яка визнається роботодавцями в усьому світі [4].

Завдяки тому, що ми працюємо з емуляторами, які на 99% відтворюють поведінку реального "заліза", перехід до роботи зі справжнім обладнанням у серверній кімнаті проходить майже безболісно. Студент вже знає, куди підключити консольний кабель і що саме побачить на екрані терміналу.

Підсумовуючи, можна сказати, що інтеграція курсів та інструментів Cisco у навчальний процес є критично важливою для підготовки сучасного фахівця. Для студента це можливість:

Отримати доступ до актуальних знань світового рівня.

Розвинути практичні навички налаштування та діагностики мереж.

Зрозуміти глибокі принципи передачі даних через візуалізацію.

Завдяки Cisco Packet Tracer та NetAcad ми виходимо з університету не теоретиками, а молодими інженерами, готовими до вирішення реальних завдань.

СПИСОК ЛІТЕРАТУРИ

1. Cisco Networking Academy [Електронний ресурс]. – Режим доступу: https://www.netacad.com/.

2. Cisco Packet Tracer - Networking Simulation Tool [Електронний ресурс]. – Режим доступу: https://www.netacad.com/courses/packet-tracer.

3. Cisco IOS Technologies [Електронний ресурс]. – Режим доступу: https://www.cisco.com/c/en/us/products/ios-nx-os-software/ios-technologies/index.html.

4. Cisco Certified Network Associate (CCNA) Certification [Електронний ресурс]. – Режим доступу: https://www.cisco.com/c/en/us/training-events/training-certifications/certifications/associate/ccna.html.

Камишанов Володимир Олегович
студент 6 курсу, групи ТДСМ-61
Державного університету
інформаційно-комунікаційних технологій
м. Київ
(099)-951-14-11
mag3326001@stud.duikt.edu.ua
Науковий керівник: Миронов Дмитро Вікторович,
кандидат технічних наук
доцент кафедри Телекомунікаційних систем та мереж
Державного університету інформаційно-комунікаційних технологій
м. Київ

ДЕКОНВОЛЮЦІЯ ВІДЕОПОТОКІВ У ТЕЛЕКОМ-МЕРЕЖАХ: ВПЛИВ НА ЯКІСТЬ АНАЛІТИКИ ТА СМУГУ ПРОПУСКАННЯ

Постановка задачі. Системи відеоспостереження у телекомунікаційних мережах генерують значні обсяги відеоданих, які використовуються для задач безпеки, транспортного моніторингу та «розумного міста». Якість вихідних кадрів визначає верхню межу точності алгоритмів виявлення подій, трекінгу та автоматичного розпізнавання номерних знаків (ANPR — Automatic Number Plate Recognition). Розмиття руху, розфокус, аберації оптики та шум сенсора зменшують інформативність кадрів і погіршують роботу алгоритмів навіть за достатнього бітрейта.

Одночасно оператор телеком-мережі обмежений смугою пропускання та допустимою затримкою, тому не завжди є можливість просто підвищити роздільну здатність або бітрейт. У таких умовах деконволюція розглядається як засіб відновлення дрібних деталей та контрасту, який можна інтегрувати в мережевий конвеєр оброблення відеоданих.

Потрібно дослідити, які методи деконволюції є доцільними для реалізації на периферійних вузлах (edge), як їхнє розміщення впливає на затримку та трафік, і наскільки покращення перцептивних метрик (PSNR, SSIM, LPIPS) конвертується у приріст прикладних метрик відеоаналітики.

Мета дослідження. Підвищення ефективності використання ресурсів телекомунікаційної мережі (смуги пропускання та часу затримки) в системах відеоаналітики шляхом обґрунтування оптимального архітектурного розміщення методів деконволюції на вузлах периферійних обчислень (edge computing)

Результати дослідження. Розглядаються дві групи методів деконволюції відеокадрів. Перша - класичні алгоритми, що спираються на модель згортки з функцією розсіювання точки PSF (Point Spread Function): фільтр Вінера, алгоритм Richardson–Lucy з регуляризацією, варіаційні методи сліпої деконволюції. Вони забезпечують контрольоване відновлення та явний компроміс між посиленням високих частот і шумом, але чутливі до похибок у PSF та рівні шуму. Друга — компактні глибинні моделі однокадрового

деблюрингу (наприклад, DeblurGAN-подібні архітектури), що навчаються на масивах розмитих і «різких» зображень та краще відпрацьовують просторово-неоднорідне розмиття.

Інтеграція в телеком-мережу аналізується для трьох варіантів розміщення деконволюції: безпосередньо на камері (on-camera, до кодування), на edge-шлюзі (після декодування отриманого потоку) та в центрі обробки даних. On-camera-варіант мінімізує додатковий трафік, але обмежений ресурсами вбудованих процесорів. Edge-розміщення дозволяє консолідувати обчислення для декількох камер і краще масштабувати сервіс, однак потребує додаткових операцій декодування/кодування. Централізована деконволюція у дата-центрі зменшує вимоги до вузлів доступу, але вимагає достатньої смуги пропускання для транспортування менш оброблених потоків.

Для порівняння конфігурацій використовується фіксований набір відеопослідовностей, які моделюють типові сцени відеоспостереження (стаціонарні сцени, пішохідний рух, транспорт із різною швидкістю). Для кожної конфігурації вимірюються перцептивні метрики якості зображення: PSNR (Peak Signal-to-Noise Ratio — пікове відношення сигнал/шум), SSIM (Structural Similarity Index Measure — показник структурної подібності) та LPIPS (Learned Perceptual Image Patch Similarity — навчена перцептивна схожість). Додатково оцінюються прикладні метрики відеоаналітики: частка коректно розпізнаних номерних знаків у задачі ANPR, точність і повнота детекції об’єктів.

Паралельно вимірюються інженерні параметри: середній бітрейт, затримка «камера - модуль аналітики», кількість потоків, які може обробити вузол за одиницю часу. На основі цих даних порівнюються класичні та глибинні методи деконволюції, а також варіанти розміщення (on-camera, edge, дата-центр) з точки зору компромісу «якість аналітики — мережеві ресурси - обчислювальна складність».

Висновки та перспективи. Деконволюція відеопотоків у телеком-мережах є ефективним інструментом підвищення якості відеоаналітики за умови коректного вибору методу та місця його застосування в архітектурі системи. Класичні алгоритми забезпечують передбачувану поведінку та низьку обчислювальну складність, тоді як компактні глибинні моделі краще працюють із складним розмиттям, але потребують апаратної підтримки. Результати аналізу показують, що розміщення деконволюції на edge-вузлах часто є компромісним варіантом, який дозволяє покращити перцептивні та прикладні метрики відеоаналітики без істотного збільшення трафіку та затримки. Подальші дослідження мають бути спрямовані на автоматичний вибір конфігурації деконволюційного модуля залежно від характеристик сцени та поточних мережевих умов.

Список використаних джерел

1. Li C. Image deblurring based on double blur kernel. 5th International Conference on Information Science, Electrical and Automation Engineering (ISEAE 2023), Wuhan, China, 24–26 March 2023 / ed. by T. Lei. 2023. URL: https://doi.org/10.1117/12.2689886

2. DeblurGAN: Blind Motion Deblurring Using Conditional Adversarial Networks / O. Kupyn et al. 2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), Salt Lake City, UT, 18–23 June 2018. 2018. URL: https://doi.org/10.1109/cvpr.2018.00854

3. Vougioukas K., Boom B. J., Fisher R. B. Adaptive deblurring of surveillance video sequences that deteriorate over time. 2013 20th IEEE International Conference on Image Processing (ICIP), Melbourne, Australia, 15–18 September 2013. 2013. URL: https://doi.org/10.1109/icip.2013.6738224

Прищепа О. О.,
студентка кафедри
кібербезпеки та захисту інформації
факультету інформаційних технологій
Київського національного університету
імені Тараса Шевченка
Бабенко Ю.М.,
доктор філософії, асистент кафедри
кібербезпеки та захисту інформації
факультету інформаційних технологій
Київського національного університету
імені Тараса Шевченка

СТЕГАНОГРАФІЧНЕ ВБУДОВУВАННЯ ЦИФРОВИХ ПІДПИСІВ У PDF-ДОКУМЕНТИ

Поточна цифрова трансформація суспільних процесів веде до розширення обсягів електронного документообігу, що, у свою чергу, вимагає надійних механізмів для його обробки, захисту та перевірки автентичності. Хоча кваліфікований електронний підпис (КЕП) законодавчо визнаний юридичним еквівалентом власноручного [1] , його практичне впровадження у великомасштабні задачі (як-от масова видача сертифікатів чи довідок) залишається ускладненим через організаційні бар'єри та значні часові витрати.

Внаслідок цієї прогалини, чимало установ вдаються до використання незахищених технік ідентифікації, зокрема додавання сканованих підписів, QR-кодів чи внутрішніх номерів. Це робить документи надзвичайно вразливими до фальсифікації. Відтак, постає актуальна науково-практична проблема розробки такого механізму автентифікації, який би поєднував високу надійність із гнучкістю, необхідною для інтеграції в автоматизовані, високошвидкісні робочі процеси.

Перспективним вектором вирішення цієї задачі є інтеграція криптографічних засобів із методами цифрової стеганографії. Фундаментальна відмінність полягає в тому, що криптографія захищає зміст, тоді як стеганографія має на меті приховати сам факт передачі таємної інформації [2]. Такий комбінований підхід дає змогу імплантувати криптографічний ідентифікатор (наприклад, цифровий підпис хешу) безпосередньо у візуальний контент документа. Це робить маркер непомітним для людського ока, але залишає його доступним для програмних засобів автоматизованої верифікації. У будь-якій “захищеній” системі електронного документообігу мають бути передбачені механізми забезпечення справжності документів [3], і запропонований стеганографічний підхід є кроком до створення саме такого гнучкого та надійного механізму.

Як наслідок, досягається стійкість до поширених атак візуальної модифікації у PDF-редакторах та усувається необхідність у складних процедурах верифікації через зовнішні сервіси. Таке рішення є оптимальним для

автоматизованих систем масової видачі документів (сертифікатів, анкет), де пріоритетами є швидка перевірка та захист від фальсифікації.

Алгоритм генерації захищеного документа починається зі створення цифрового відбитка його текстового вмісту. На початковому етапі з PDF-шаблону вилучається повний видимий текстовий шар (включаючи ПІБ, дати, таблиці та інші реквізити). Виключаючи будь-які модифікації чи канонізацію, цей сирий текстовий вміст хешується за допомогою криптографічно стійкого алгоритму. Отриманий хеш-відбиток підписується особистим (секретним) ключем видавця, формуючи ЕЦП.

Загальну структурну схему запропонованого алгоритму генерації та верифікації наведено на рисунку 1. Цей бінарний підпис (який є секретним повідомленням) вбудовується у фонове зображення-контейнер (PNG) методом стеганографії LSB (Least Significant Bit), що полягає у модифікації найменш значущих бітів пікселів. Даний процес не спричиняє візуальних спотворень. На завершення, модифіковане зображення з інтегрованим підписом встановлюється як незмінна графічна основа фінального PDF-документа, поверх якої розміщується текстовий шар.

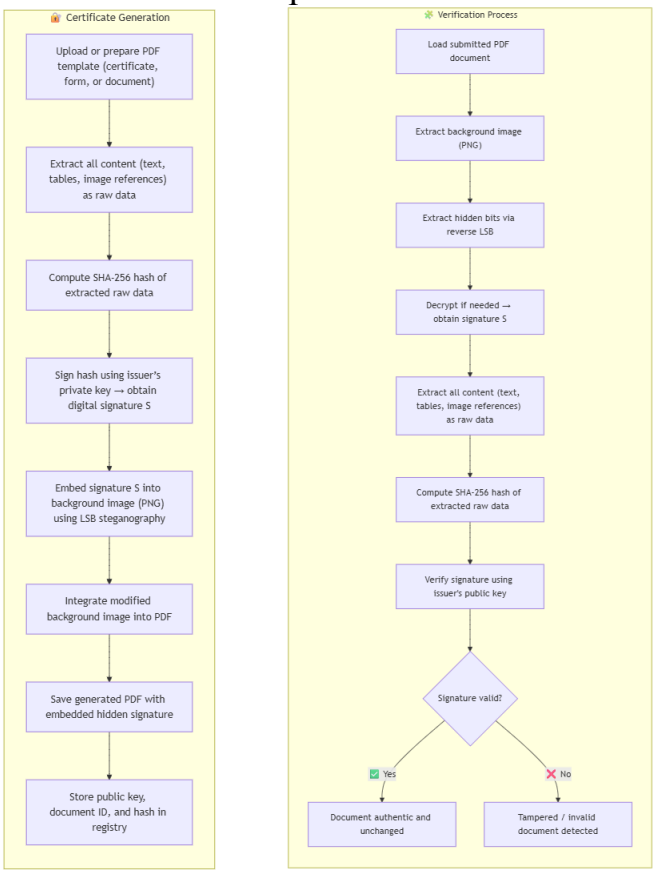


Рисунок 1. Алгоритмічна структура запропонованого гібридного методу стеганографічного вбудовування та верифікації цифрового підпису в PDF-документах.

Процес верифікації дзеркально повторює операції для підтвердження автентичності. Спершу програмний верифікатор автоматично вилучає фонове зображення з PDF та за допомогою зворотного LSB-алгоритму реконструює прихований бінарний підпис. Одночасно він зчитує видимий текстовий шар документа і повторює процес хешування, отримуючи «свіжий» хеш-відбиток

поточного стану. На фінальному етапі, використовуючи публічний ключ видавця, система перевіряє витягнутий підпис. Повна відповідність між розшифрованим підписом та «свіжим» хешем підтверджує, що документ є автентичним. Будь-яка розбіжність інтерпретується як факт несанкціонованої модифікації текстових полів або заміни фону.

Висновок: Запропонований гібридний підхід демонструє ефективне посилення цілісності та автентичності PDF-документів. Ключова перевага методу полягає у використанні двох технологій: ЕЦП застосовується для гарантування незмінності криптографічного вмісту, тоді як стеганографія вирішує задачу приховування самого факту існування верифікаційного маркера. Створений таким чином подвійний механізм верифікації є прямою контрзагрозою на одну з ключових загроз сучасного документообігу, при якій переваги цифрового подання інформації можуть бути перекреслені з легкістю, з якою можливі через модифікацію [3]. На відміну від традиційних архітектур, де цифровий підпис та візуальний шар існують дисоційовано, запропонована методологія встановлює міцний зв'язок між автентичністю видимих даних та їхньою графічною основою.

Список використаних джерел:

1. Верховна Рада України, Про електронну ідентифікацію та електронні довірчі послуги, Закон України N 2155-VIII, 2017. URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text (date of access: 16.11.2025).

2. Хорошко В. О., Яремчук Ю. Є., Карпінець В. В. Комп'ютерна стеганографія. Вінниця : ВНТУ, 2017. URL: http://ir.lib.vntu.edu.ua//handle/123456789/34907 (date of access: 16.11.2025).

3. Information security in electronic document management systems. Scientific Bulletin of PUET: Economic Sciences. 2020. No. 4 (95). URL: https://doi.org/10.37734/2409-6873-2019-4-7 (date of access: 16.11.2025).

Анотація: Робота вирішує проблему вразливості PDF-документів до візуальних підробок. Запропоновано гібридний метод, що поєднує криптографічний підпис ключових даних зі стеганографічним вбудовуванням підпису у фонове зображення. Для прихованого вбудовування використовується LSB-алгоритм. Цей підхід створює дієвий подвійний механізм верифікації, тісно пов'язуючи автентичність видимих даних з їхньою графічною основою, що є стійким до візуальних модифікацій та спрощує перевірку.

Abstract: This work addresses the vulnerability of PDF documents to visual forgery. A hybrid method is proposed that combines a cryptographic signature of key data with the steganographic embedding of that signature into a background image. The LSB algorithm is used for covert embedding. This approach creates an effective dual-verification mechanism, tightly binding the authenticity of the visible data to its graphical foundation, which is resistant to visual modifications and simplifies verification.

Верещака Артем Олександрович
Студент 5 курсу, групи ТСДМ-61
Державний університет
інформаційно-комунікаційних технологій
м.Київ
(068)-611-28-12
artem.ver9991@gmail.com
Науковий керівник: Миронов Д.В
Державний університет
інформаційно-комунікаційних технологій
м.Київ

ІНТЕГРАЦІЯ СИСТЕМ КІБЕРБЕЗПЕКИ В ІНФРАСТРУКТУРУ МЕДИЧНОГО ЗАКЛАДУ: ПОБУДОВА ЗАХИЩЕНОГО ЦИФРОВОГО СЕРЕДОВИЩА

Постановка задачі. Із розвитком цифрової медицини питання кібербезпеки в медичних установах набуло критичного значення. Обсяг конфіденційної інформації, що зберігається та передається, зростає щодня: електронні медичні картки, діагностичні результати, історії хвороб, особисті дані пацієнтів. Через це лікарні стають привабливою мішенню для кібератак.Метою даного дослідження є розробка комплексного підходу до впровадження систем кіберзахисту в медичному закладі, який має обмежене фінансування, але високі вимоги до стабільності та безпеки.

Мета.Побудувати стійку до загроз інформаційну екосистему, яка забезпечить цілісність, доступність і конфіденційність медичних даних. Впровадження заходів IT-безпеки на всіх рівнях - від інфраструктури до поведінки персоналу.

Ключові елементи реалізації.

1.**Аудит поточної IT-інфраструктури.** Проведено оцінку слабких місць у мережі, зокрема незахищених портів, застарілого програмного забезпечення, відкритих RDP-з’єднань тощо.

2.**Сегментація мережі.** Запроваджено поділ на ізольовані VLAN для зони користувачів, серверної зони, медобладнання та систем відеоспостереження. Це знижує ризик поширення вірусів та шкідливого ПЗ між підмережами.

3.**Встановлення фаєрволів нового покоління.** На прикладі FortiGate впроваджено контроль трафіку, фільтрацію загроз на прикладному рівні та глибоку інспекцію пакетів.

4.**Впровадження SIEM-системи (Wazuh).** Реалізовано централізований збір та аналіз логів, відстеження змін у критичних файлах, виявлення аномальної поведінки користувачів.

5.**Інтеграція антивірусного рішення з центральним управлінням.** Наприклад, використання ESET Protect або Microsoft Defender for Endpoint з політиками обмежень на запуск зовнішніх програм.

6.**Побудова резервного контуру безпеки.** Включає автономний сервер для архівного зберігання резервних копій з обмеженим мережевим доступом.

7.**Розробка політик безпеки.** Визначено правила створення паролів, політики зміни пароля, багатофакторну автентифікацію для адміністраторів, використання VPN для віддаленого доступу.

8.**Навчання персоналу.** Проведено цикл тренінгів для медпрацівників з тем: «Фішинг», «Безпечна робота з файлами та електронною поштою», «Використання корпоративного VPN».

Результати.За рік після впровадження заходів зафіксовано:

- зниження інцидентів несанкціонованого доступу на 85%;
- підвищення продуктивності обслуговування IT-інфраструктури (менше ручних перевірок, швидке реагування через логування);
- зменшення ризику втрати даних завдяки розгалуженій системі бекапів;
- підвищення обізнаності персоналу про ризики кіберзагроз.

Висновки.Інтеграція кібербезпеки в лікарню - це не разовий захід, а постійний процес. Навіть за обмежених ресурсів можливо створити ефективну систему захисту, поєднуючи відкриті рішення (Wazuh, pfSense) з комерційними інструментами. Надалі доцільно вивчати впровадження Zero Trust моделі, розширювати систему контролю доступу та розглянути можливість участі в державних програмах кіберзахисту.

Список джерел.

1. ISO/IEC 27001:2022 - стандарт з інформаційної безпеки.
2. Wazuh Documentation, https://documentation.wazuh.com
3. NIST Cybersecurity Framework
4. «Кібербезпека в охороні здоров’я: нові виклики та рішення», Healthcare IT News, 2024.

НАПРЯМ 3. АПАРАТНІ ЗАСОБИ ТА АРХІТЕКТУРИ КОМП'ЮТЕРНИХ СИСТЕМ

Бовсунівський Микола Сергійович
студент 5 курсу, групи КСДМ-51,
Державного університету
інформаційно-комунікаційних технологій
Науковий керівник: Лащевська Наталія Олександрівна
завідувач кафедри, к.т.н., доцент,
Державного університету
інформаційно-комунікаційних технологій, м. Київ

АПАРАТНО-АРХІТЕКТУРНІ РІШЕННЯ В КІБЕРСТІЙКИХ ТА РЕСУРСНО-ЕФЕКТИВНИХ РОЯХ БПЛА

Анотація.Представлено архітектуру Secure-Eco-AI-RDR – децентралізоване гібридне рішення для управління роями БПЛА нового покоління. Ключова інновація полягає у модифікації архітектури комп'ютерних систем БПЛА для одночасного вирішення проблем енергетичних обмежень та кіберзагроз у розподіленому навчанні. Архітектура інтегрує проактивну навігацію на основі бортового радара FMCW та нейронних мереж , енергозалежне федеративне навчання (FedProx-E) та механізм довірчої агрегації (HDBSCAN) для захисту моделі. Це забезпечує стабільну багатозадачність та підвищує живучість системи.

Постановка задачі.Традиційні децентралізовані архітектури керування роями БПЛА часто нехтують системними обмеженнями, зокрема обмеженим енергетичним бюджетом пристроїв та вразливістю до кібератак під час колективного навчання. Крім того, існує потреба в обчислювальних архітектурах, здатних ефективно виконувати кілька завдань місії паралельно (багатозадачність).

Завдання полягає у розробці комплексної децентралізованої апаратно-програмної архітектури, яка одночасно забезпечує:

Архітектурно оптимізує споживання енергії (як обчислювальної, так і комунікаційної) під час колективного навчання.

Забезпечує захист від зловмисного впливу на процес навчання моделі на архітектурному рівні (кіберстійкість)

Гарантує високу ефективність багатозадачності.

Мета дослідження.Створення , надання теоретичної бази та практичне тестування архітектури Secure-Eco-AI-RDR для децентралізованого управління роями БПЛА, що інтегрує: енергозалежний федеративний механізм навчання

(FedProx-E), систему виявлення градієнтних аномалій як захист від атак та багатозадачну нейронну мережеву модель для покращення функціональності рою.

Результати дослідження. Запропонована архітектура Secure-Eco-AI-RDR реалізована через гібридне поєднання спеціалізованих обчислювальних та апаратних модулів на кожному агентові БПЛА:

1. Сенсорний та Прогнозний Модулі

Апаратне забезпечення: Використання бортового радара FMCW.

Обчислювальна архітектура: Двонаправлена рекурентна нейронна мережа з увагою (Bi-GRU-Attention) для проактивного прогнозування траєкторій.

2. Ресурсно-Ефективна Архітектура Навчання (Secure-Eco-FL)

Енергозалежний FedProx-E: Вага внеску БПЛА динамічно налаштовується відповідно до його залишкового заряду батареї та вартості зв'язку. Це дозволяє перерозподілити обчислювальне навантаження та збільшити середній час автономної роботи рою на 15-20%.

Довірча агрегація для Кіберзахисту: Використання методів кластеризації (HDBSCAN) на градієнтних оновленнях для виявлення викидів (симптомів атак) та їх виключення. Це підтримує ефективність запобігання зіткненням на рівні >99,5% навіть за наявності до 15% скомпрометованих агентів.

3. Багатозадачна Обчислювальна Архітектура

Спільний екстрактор ознак: Використовується архітектура зі спільним екстратором ознак та багатоголовковими вихідними шарами для навігаційних та місійних завдань.

Переваги: Знижує загальні обчислювальні витрати та підвищує ефективність обміну даними , забезпечуючи здатність одночасно виконувати обидва типи завдань без значного погіршення якості.

Ефективність архітектури буде перевірена в інтегрованому середовищі моделювання (Gazebo+NS-3+ROS~2).

Список використаних джерел

1. Yang, Y., et al. "Efficient UAV Swarm-Based Multi-Task Federated Learning with Dynamic Task Knowledge Sharing." arXiv preprint arXiv:2503.09144 (2025). URL: https://arxiv.org/abs/2503.09144 (date of access: 15.09.2024) .

2. Yang, H., et al. "Bi-GRU: A Bidirectional Gated Recurrent Unit for Trajectory Prediction." arXiv preprint arXiv:2410.23305 (2024). URL: https://arxiv.org/abs/2410.23305 (date of access: 08.10.2024) .

3. Nikodem, M., et al. "Federated Learning in the Sky: Joint Power Allocation and Scheduling with UAV Swarms." IEEE Transactions on Wireless Communications (2020). URL: https://ieeexplore.ieee.org/document/9294233 (date of access: 22.11.2024) .

4. Zhang, Y. "Path Planning for Multi-UAV in a Complex Environment Based on Reinforcement-Learning-Driven Continuous Ant Colony Optimization." Drones 9.9 (2025): 638. URL: https://www.mdpi.com/2504-446X/9/9/638 (date of access: 05.11.2024)

Бондаренко Сергій Юрійович
студент 6 курсу, групи ІСДМ-61
Державного університету
інформаційно-комунікаційних технологій
м. Київ
(097)-381-43-43
mag6861352@stud.duikt.edu.ua
Науковий керівник: Срібна Ірина Миколаївна
доктор технічних наук
доцент кафедри Інформаційних систем та технологій
Державного університету
інформаційно-комунікаційних технологій
м. Київ

ЗАСТОСУВАННЯ ТЕХНОЛОГІЙ ІНТЕРНЕТУ РЕЧЕЙ ДЛЯ МОНІТОРИНГУ СТАНУ ПРОМИСЛОВИХ ОБ'ЄКТІВ

Усі сфери виробництва протистоять високому ризику відмов обладнання та незапланованих простоїв, що призводить до запізнення термінів виготовлення та доставки. Раптові несправності та простої обладнання виникають через відсутність постійного моніторингу стану машин, що унеможливлює прогнозування та запобігання системним збоям. Чимало підприємств досі працюють за старими методами, приймаючи рішення реактивно, тобто коли відмова вже сталася. Але існують методи, що дозволяють діяти проактивно, тобто вживати заходів завчасно, щоб запобігати збоям.

Постановка задачі. Задачею дослідження є аналіз технологій моніторингу стану для створення IoT систем що аналізують сенсорні дані промислових об’єктів.

Мета дослідження. Вдосконалення засобів моніторингу стану за допомогою технологій Інтернету Речей.

Результати дослідження. Традиційно фахівці з технічного обслуговування виконують свою роботу за допомогою календаря, припускаючи, що з віком машини, її продуктивність знижується. Однак це не зовсім так. Календарне обслуговування часто є неефективним і не оптимізує термін експлуатації обладнання. Натомість, технічне обслуговування за станом базується на моніторингу стану машини для виявлення та планування заходів технічного обслуговування. Технологія бездротових датчиків розширяє можливості технічного обслуговування за станом. Доступні датчики моніторингу стану та зручне програмне забезпечення для аналізу зробили цю практику доступною для більшості організацій.

Існує декілька технологій, які підтримують ключові цілі бізнесу, включаючи віддалений моніторинг активів у промислових застосуваннях, управління IT-активами для підприємств, а також моніторинг та контроль активів у лікарнях та галузі охорони здоров'я.

До них належать:

— Радіочастотна ідентифікація (RFID) – мітки, які зберігають та передають інформацію про об'єкти або інвентар, включаючи інформацію про місцезнаходження.

— Система глобального позиціювання (GPS) — пристрої, що передають дані через стільникові мережі або супутники, можуть бути інтегровані в обладнання та відстежуватися за допомогою програмного забезпечення.

— Штрих-коди — етикетки фізично прикріплені до об'єкта та скануються за допомогою мобільного пристрою.

— Bluetooth з низьким енергоспоживанням — бездротова технологія короткого діапазону, що дозволяє обмінюватися даними з сусідніми пристроями.

— Комунікація ближнього поля (NFC) — двостороння комунікація, що зазвичай використовується в мобільних гаманцях та інших безконтактних платіжних системах.

Системи моніторингу стану вимірюють окремі параметри обладнання, відхилення від яких можуть вказувати на майбутні несправності:

— Мастильні матеріали для машин сигналізують про перегрів або забруднення.

— Вібрація допомагає виявити знос запасних частин, їхнє зміщення або дисбаланс.

— Відхилення температури механічних частин можуть вказувати на знос, недостатнє або відсутнє змащення, зміщення запасних частин або наявність сторонніх предметів у машинах. Аномальні температури в електричному обладнанні можуть свідчити про витоки або проблеми з тиском і струмом.

— Тиск показує стан газу, води або пари в машинах. Відхилення тиску попереджають про витоки або інші порушення цілісності системи.

— Частота обертання також вимірюється для виявлення зносу або дисбалансу запасних частин.

Платформи Інтернету речей надають готові інструменти та рішення, які дозволяють швидко створювати та впроваджувати системи моніторингу стану обладнання з мінімальними витратами. Як правило, платформи IoT для виробництва є кросплатформенними, тому їх можна легко інтегрувати з різними контролерами, датчиками та трекерами з відповідними обчислювальними ресурсами. Дані, зібрані цими пристроями, передаються до програмних інструментів аналізу даних, а потім візуалізуються у вигляді діаграм, графіків та звітів, зручних для кінцевих користувачів. Такі платформи аналізу даних можуть бути локальними або хмарними. Однак виробничі машини можуть генерувати великі потоки даних з високою частотою. І в багатьох випадках передача необроблених даних безпосередньо на платформу IoT є неефективною та дорогою з точки зору пропускної здатності каналу зв'язку. Для вирішення таких проблем існує підхід на основі кордонних обчислень, тобто обробка даних на місці за допомогою мережевих шлюзів та розумних датчиків. Попередньо оброблені та стиснуті дані потім передаються на хмарну платформу або в корпоративну систему для подальшого аналізу.

Відстеження активів дозволяє управляти обладнанням та активами компанії незалежно від їхнього місцезнаходження. Приклади використання включають:

— Інтеграція GPS у продукти, обладнання та транспорт для більш точного відстеження.

— Покращення ефективності виробничої лінії, процесів розподілу та транспортних маршрутів.

— Покращення предиктивного технічного обслуговування на основі закономірностей, виявлених у даних, зібраних з ланцюга поставок протягом певного часу.

— Виконання моніторингу важливих активів за допомогою IoT зв’язку та систем управління.

У міру того як промислові об'єкти стають все більшими і складнішими, а такі активи, як морські вітроелектростанції, генерують величезні обсяги даних з датчиків, штучний інтелект став потужним інструментом, що допомагає експертам з моніторингу стану обладнання у їхній роботі. Сучасні платформи Інтернету речей оснащені передовими аналітичними інструментами, включаючи алгоритми штучного інтелекту та машинного навчання. Це означає, що зібрані дані можна обробляти більш ефективно і отримувати цінну інформацію про стан обладнання. Поєднання штучного інтелекту та Інтернету речей відкриває перспективні можливості для підвищення ефективності, економії коштів та трансформаційного потенціалу.

Висновки та перспективи. Рішення та інструменти для моніторингу стану та предиктивного обслуговування промислового обладнання активно розробляються в усьому світі, і платформи IoT відіграють ключову роль у цьому процесі. Щоб залишатися конкурентоспроможними, підвищити прозорість виробництва та збільшити час безвідмовної роботи систем, промислові підприємства повинні впроваджувати технології IoT та моніторинг стану.

Список використаних джерел

1 How Does IOT Condition Monitoring Work? [Електронний ресурс] // Technomax. – Режим доступу до ресурсу: https://www.technomaxme.com/how-iot-condition-monitoring-work-together.

2 Boost Efficiency & Reliability with IoT-Driven Condition Monitoring [Електронний ресурс] / Jennifer Sludden // IoT Connectivity & Solutions - MachineQ, a Comcast Company. – Режим доступу до ресурсу: https://www.machineq.com/post/unlock-efficiency-and-reliability-with-iot-driven-condition-monitoring.

3 Industrial IoT – From Condition Based Monitoring to Predictive Quality to digitize your factory with AWS IoT Services [Електронний ресурс] / Rodrigo Merino // Amazon Web Services. – Режим доступу до ресурсу: https://aws.amazon.com/ru/blogs/iot/industrial-iot-from-condition-based-monitoring-to-predictive-quality-to-digitize-your-factory-with-aws-iot-services/.

Ходосов Антон Олександрович
студент 6 курсу, групи КСДМ-62
Державного університету
інформаційно-комунікаційних технологій
м. Київ
koyot0051@gmail.com
Остапенко Олександр Станіславович
студент 6 курсу, групи КСДМ-62
Державного університету
інформаційно-комунікаційних технологій
м. Київ
ostapenko2709@gmail.com

АВТОМАТИЗАЦІЯ МОНІТОРИНГУ ВІРТУАЛЬНИХ СЕРЕДОВИЩ ТА СЛУЖБ ЯК ЗАСІБ ПІДВИЩЕННЯ НАДІЙНОСТІ IT-ІНФРАСТРУКТУРИ

Постановка задачі. У сучасному інформаційному просторі спостерігається зміщення акценту з фізичних серверів на віртуальні середовища, які можуть масштабуватися до тисяч вузлів. Керування такою гетерогенною інфраструктурою вручну стає неефективним через великий обсяг телеметричних даних. Типові «коробкові» рішення часто не надають повної картини стану систем, а затримка у виявленні несправностей призводить до фінансових втрат та зупинки бізнес-процесів . Тому виникає нагальна необхідність впровадження спеціалізованих автоматизованих систем, здатних забезпечити проактивний нагляд та прогнозування збоїв на основі історичних даних.

Мета дослідження. Метою дослідження є підвищення ефективності експлуатації серверної інфраструктури шляхом впровадження комплексної системи моніторингу на базі платформи Zabbix 7.0 LTS, яка забезпечує централізований збір метрик, контроль безпеки та автоматизоване реагування на інциденти.

Результати дослідження. Під час дослідження було налаштовано взаємодію Zabbix-сервера з веб-інтерфейсом на базі Nginx та PHP-FPM, що забезпечило високу продуктивність обробки запитів. Для захисту периметра моніторингу налаштовано міжмережевий екран, який дозволяє трафік лише на критично важливі порти, реалізуючи принцип мінімальних привілеїв. Впровадження Zabbix Agent 2[1] дозволило реалізувати багатопотоковий збір метрик у реальному часі. Використання активних перевірок знизило навантаження на центральний сервер, дозволяючи агенту самостійно ініціювати передачу даних. Налаштування глибокого моніторинг СУБД MySQL з використанням спеціалізованих макросів ({$MYSQL.DSN}, {$MYSQL.USER}), а також створено окремого сервісного користувача з обмеженими правами (REPLICATION CLIENT, PROCESS), дозволяє безпечно зчитувати статистику

повільних запитів та використання буфера InnoDB без ризику пошкодження даних .

Під час дослідження ефективність системи було верифіковано шляхом проведення стрес-тестування утилітою mysqlslap. Графіки системи миттєво зафіксували сплеск навантаження на CPU та зростання кількості транзакцій, а підсистема тригерів коректно ідентифікувала інцидент і автоматично перевела його в статус вирішеного після стабілізації[2].

Висновки та перспективи. Досліджена система забезпечила 100% видимість стану віртуальних вузлів та скоротила час виявлення критичних проблем (недоступність хоста, зупинка сервісів) до менше ніж 1 хвилини. Впроваджені механізми дозволяють адміністраторам діяти на випередження, запобігаючи аваріям до їх настання. Перспективи подальших досліджень полягають у налаштуванні інтеграції системи сповіщень із зовнішніми месенджерами та впровадженні прогнозної аналітики на базі зібраних історичних даних для планування масштабування ресурсів.

Список використаних джерел:

1. Catalin-Marian Petruti et al. "Automatic Management Solution in Cloud Using NtopNG and Zabbix." 2018 17th RoEduNet Conference: Networking in Education and Research (RoEduNet) (2018): 1-6. https://doi.org/10.1109/roedunet.2018.8514142.

2. Jie Bai et al. "Design and implementation of small private cloud system with highly reliable management and monitoring." , 12287 (2022): 122870T - 122870T-5. https://doi.org/10.1117/12.2640748.

Бровченко Тетяна Яківна
Студентка 4 курсу, групи КІД-41
Державного університету
інформаційно-комунікаційних технологій,
м. Київ
0988308364
brovcenkotana416@gmail.com
Науковий керівник: Бученко Ігор Анатолійович
Старший викладач
кафедри Комп’ютерної інженерії
Державного університету
інформаційно-комунікаційних технологій,
м. Київ

RISC-V – ВІДКРИТА АРХІТЕКТУРА МАЙБУТНЬОГО: ПЕРЕВАГИ ТА ВИКЛИКИ

Анотація. У роботі розглянуто особливості та перспективи розвитку відкритої архітектури набору команд (ISA) RISC-V, яка виступає альтернативою пропрієтарним рішенням x86 та ARM. Метою дослідження є аналіз ефективності застосування цієї архітектури, визначення її переваг, недоліків та подальших перспектив. Проведено порівняльний аналіз RISC-V з архітектурами CISC та традиційними RISC, який виявив ключові переваги відкритого стандарту: відсутність ліцензійних платежів, високу енергоефективність, модульність та можливості кастомізації. Висвітлено основні виклики, з якими стикається екосистема RISC-V, зокрема питання стандартизації безпеки та верифікації кастомізованих рішень. Зроблено висновок про значний потенціал впровадження RISC-V у сферах IoT, штучного інтелекту та автомобільної промисловості, що дозволяє їй претендувати на статус однієї з провідних архітектур майбутнього.

Abstract. The paper discusses the features and development prospects of the open Instruction Set Architecture (ISA) RISC-V, which serves as an alternative to proprietary x86 and ARM solutions. The aim of the study is to analyze the efficiency of this architecture, identify its advantages, disadvantages, and future outlook. A comparative analysis of RISC-V against CISC and traditional RISC architectures was conducted, revealing key benefits of the open standard: absence of licensing fees, high energy efficiency, modularity, and customization capabilities. The main challenges facing the RISC-V ecosystem are highlighted, specifically issues regarding security standardization and verification of customized solutions. It is concluded that RISC-V has significant potential for implementation in IoT, Artificial Intelligence, and the automotive industry, positioning it to become one of the leading architectures of the future.

Постановка задачі. Архітектура набору команд (Instruction Set Architecture, ISA) є кордоном для взаємодії між апаратним та програмним забезпеченням та є невід’ємним компонентом в комп'ютерній інженерії. Двома

основними ISA які використовуються зараз є архітектури CISC (Complex Instruction Set Computer) і RISC (Reduced Instruction Set Computer).

Мета дослідження. Метою дослідження є аналіз ефективності застосування нової архітектури командного набору — RISC-V, яка бере свої початки від моделі комп'ютера RISC, визначити її переваги, недоліки та подальшу перспективу розвитку.

Результати дослідження. RISC-V — це відкритий стандарт системної архітектури (ISA) для комп'ютерних процесорів. На відміну від пропрієтарних ISA на кшталт x86 чи ARM, архітектура RISC-V є вільною і відкритою — її специфікації опубліковані під відкритими ліцензіями, тож будь-хто може реалізувати RISC-V без ліцензійних платежів (табл. 1) [1].

Також RISC-V має багато інших переваг над іншими, що робить її архітектурою майбутнього:

1. обмеживши набір інструкцій до мінімуму, це дозволило виконувати кожну інструкцію протягом одного тактового циклу;
2. всі операції виконуються в регістрах, а для доступу до пам'яті існують окремі інструкції;
3. архітектура має більшу кількість регістрів для оптимізації продуктивності [3].

Таблиця 1

Головні відмінності архітектур RISC-V, x86 та ARM

Характеристики	RISC-V	x86	ARM
Модель ліцензування	Відкритий стандарт	Пропрієтарний, ліцензується компаніями Intel та AMD	Пропрієтарний, ліцензується компанією ARM
Енергоефективність	Висока	Нижча, ніж у RISC-архітектур, через складність інструкцій	Дуже викока
Продуктивність	Потенційно висока	Висока	Дуже висока
Можливість кастомізації	Дозволяє будь-кому розробляти чипи	Дуже обмежена	Обмежена

Але головні проблематики RISC-V полягає в головних перевагах. Його специфікація була розроблена, щоб його можна було легко підлаштовувати під різні потреби. Тому будь-яке рішення для верифікації RISC-V має бути достатньо гнучким, щоб враховувати налаштування. Поний відкритий стандарт – це плюс. Кожен може створити власну реалізацію, але не всі виробники

дотримуються високих стандартів безпеки, що дає причину для формування інструментів для апаратної та ПЗ-безпеки[2].

Через те, що RISC-V як універсальна та масштабована архітектура, її застосування охоплює широкий спектр пристроїв – від мікроконтролерів до суперкомп'ютерів. Існує три основні сегменти ринку, зацікавлені в архітектурі RISC-V:

1. IP-провайдери, які можуть пропонувати власні розробки.
2. Команди SoC, що використовують комерційну IP-адресу.
3. Розробники, що створюють власні SoC на базі процесорів RISC-V [2].

Висновки та перспективи. Аналіз показав, що RISC-V є ефективною архітектурою, вирізнається від інших своєю відкритістю, модульністю та кастомізацією. Ці характеристики роблять її привабливою для багатьох сфер застосувань. Зростаюче зацікавлення спільнот підтверджує інтерес до технології.

Водночас RISC-V стикається з низкою викликів: нова та недостатньо зріла архітектура, потреба у сильних стандартах безпеки та обмежений набір перевірених рішень. Але ці недоліки поступово долаються через розширення зацікавленості до архітектури.

Перспективи подальшого розвитку архітектури полягають у її зміцненні та поширенні у різних промислових сферах: IoT, ШІ, автомобільна промисловість тощо.

Тому RISC-V має всі шанси в найближчому майбутньому стати однією із найпровідніших та широко використовуваних архітектур набору команд.

Список використаних джерел:

1. Що таке RISC-V? – ForkLog UA. ForkLog UA – Культовий журнал про біткоїн, технологію блокчейн та цифрову економіку. URL: https://forklog.com.ua/exclusive/shho-take-ris (дата звернення: 25.11.2025).
2. What is RISC-V? – How Does it Work? | Synopsys. Synopsys | EDA Tools, Semiconductor IP & Systems Verification. URL: https://www.synopsys.com/glossary/what-is-risc-v.html#5 (date of access: 25.11.2025).
3. RISC-V проти ARM проти x86 – у чому різниця? – MICROCONTROLLER TIPS / An EE World Resource. URL: https://www.microcontrollertips.com/risc-v-vs-arm-vs-x86-whats-the-difference/ (дата звернення: 26.11.2025).

Вшивков Вадим Володимирович
студент 5 курсу, групи ТСДМ-62
Державного університету
інформаційно-комунікаційних технологій
м. Київ
mag2996702@stud.duikt.edu.ua
Науковий керівник: Домрачева Катерина Олексіївна
кандидат технічних наук, доцент
Державного університету
інформаційно-комунікаційних технологій
м. Київ

ІНЖЕНЕРНІ ПІДХОДИ ДО ПОБУДОВИ СИСТЕМ АДАПТИВНОГО БАЛАНСУВАННЯ НАВАНТАЖЕННЯ У ХМАРНИХ ПЛАТФОРМАХ

Постановка задачі. Сучасні хмарні платформи обслуговують велику кількість користувачів та запитів, що надходять нерівномірно у часі. Для забезпечення стабільної роботи системи необхідне адаптивне балансування навантаження, яке автоматично розподіляє ресурси залежно від зміни трафіку, стану вузлів і обмежень продуктивності. Класичні статичні алгоритми (Round Robin, Weighted Least Connections) не враховують динаміку хмарного середовища, що призводить до перевантаження окремих вузлів і зниження QoS.

Мета дослідження. Розробити інженерну модель адаптивної системи балансування навантаження у хмарних обчисленнях, яка забезпечує автоматичне масштабування ресурсів та оптимальний розподіл трафіку на основі моніторингу метрик у реальному часі.

Результати дослідження. Запропоновано архітектуру системи, що складається з таких компонентів:

- Модуль моніторингу — збирає дані про CPU, RAM, latency та throughput за допомогою Prometheus.
- Аналітичний модуль — обробляє часові ряди метрик, виявляє тенденції перевантаження та прогнозує потребу в масштабуванні.
- Модуль прийняття рішень — формує політики розподілу запитів між вузлами залежно від поточного стану та прогнозів.
- Інтеграційний шар із Kubernetes Horizontal Pod Autoscaler (HPA) — забезпечує автоматичне масштабування контейнерів згідно з аналітичними даними.

Проведене експериментальне моделювання показало, що використання адаптивного підходу на основі метрик Prometheus дозволяє зменшити середній час відгуку системи на 30–40 % у порівнянні зі статичними алгоритмами. Система продемонструвала стабільність навіть за пікових навантажень і збереження рівня доступності сервісів на рівні 99,9 %.

Висновки. Інженерні рішення з побудови адаптивних систем балансування навантаження забезпечують підвищення ефективності та стійкості хмарних платформ. Інтеграція модулів моніторингу, аналітики та автоматичного масштабування дозволяє створювати самоналаштовні інфраструктури, здатні оперативно реагувати на зміни трафіку. Подальші дослідження передбачають впровадження інтелектуальних моделей прогнозування на основі машинного навчання.

Список використаних джерел

1. Mishra S., et al. Load balancing in cloud computing using evolutionary algorithms. IEEE Access, 2023.

2. Kumar H., et al. Evolutionary-based load distribution techniques for multi-cloud environments. Future Generation Computer Systems, 2024, Vol. 152, pp. 77–89.

3. Li M., et al. Hybrid genetic and ACO approach for energy-aware load balancing in cloud data centers. Journal of Network and Computer Applications, 2022, Vol. 210.

Романюк О.Н.
Д.т.н, проф.
Вінницький національний технічний університет
Тітова Н.В.
Д.т.н, проф.
Національний університет «Одеська політехніка»
Романюк С.О.
Ст. викладач, к.т.н.
Національний університет «Одеська політехніка»
Бобко О.Л.
аспірант
Вінницький національний технічний університет

ЗАСТОСУВАННЯ КОМП'ЮТЕРНИХ КЛАСТЕРІВ ДЛЯ ГРАФІЧНОГО РЕНДЕРИНГУ

Анотація. Розглянуто особливості реалізації графічного рендерингу в комп'ютерних кластерах та їхню роль у формуванні високоякісних візуалізацій. Проаналізовано архітектурні підходи до розподілення обчислень, моделі паралелізації та застосування сучасних CPU і GPU-кластерів. Показано, що кластерні системи забезпечують суттєве прискорення рендерингу, ефективне використання ресурсів і можливість роботи зі сценами великої складності.

Abstract.The paper examines the key principles of implementing graphical rendering in computer clusters and their importance for producing high-quality visual content. Various architectural strategies for distributing computations, parallelization models, and the use of modern CPU and GPU clusters are analyzed. The study shows that cluster-based systems significantly accelerate rendering, optimize resource usage, and enable working with highly complex scenes.

Застосування комп'ютерних кластерів для графічного рендерингу[1-4] сьогодні стало одним із рішень у галузі створення високоякісного візуального контенту. Це пов'язано з тим, що сучасні сцени включають у себе надзвичайно деталізовані 3D-моделі, складні алгоритми освітлення та численні обчислювальні ефекти, які важко опрацювати на одному пристрої. Поява реалістичного трасування променів у реальному часі, а також активне використання методів штучного інтелекту для прискорення візуалізації спричинили істотне зростання потреб у продуктивності. У такій ситуації рендеринг перестає бути локальною задачею й перетворюється на процес, що виконується узгодженою роботою багатьох машин, поєднаних у кластер. Головна ідея використання кластерів полягає в поділі великої обчислювальної роботи на частини та розподіленні їх між вузлами системи. Це не лише скорочує загальний час формування кадру, а й забезпечує можливість працювати з максимально можливим рівнем якості зображення. Особливо це важливо там, де

необхідне обчислення складних моделей глобального освітлення, багаторівневих BRDF/BSDF-функцій, каустики чи підповерхневого розсіювання

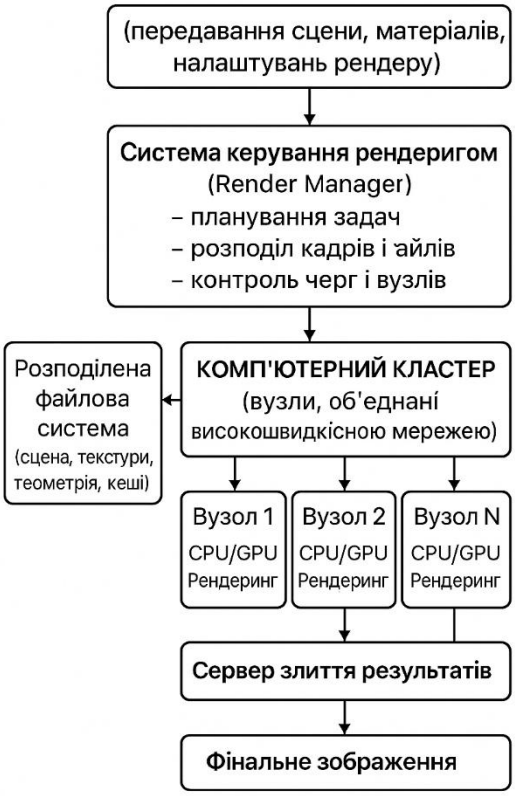


Рисунок 1- Графічний кластер

У найверхнішому елементі зображено робочу станцію, з якої й починається робота: тут готують сцену, налаштовують матеріали, текстури й параметри майбутнього рендеру. Після цього дані передаються до системи, що керує всім процесом. Саме вона визначає, які задачі запускати першими, як розподілити кадри між вузлами та які ресурси задіяти, щоб уникнути простоїв і перевантаження. Оскільки для рендерингу потрібні великі масиви даних, схема передбачає використання мережевого сховища, де зберігаються всі необхідні файли сцени: геометрія, текстури та інші ресурси. Це сховище доступне кожному вузлу кластера, тож усі працюють з одними й тими самими даними, не створюючи зайвих копій.Центральним елементом є власне кластер — це група потужних обчислювальних вузлів, пов’язаних між собою швидкою мережею. На кожному з них запускається частина рендерингового завдання: один може обчислювати один фрагмент кадру, інший — наступний, а третій — ще один. Завдяки одночасній роботі багатьох вузлів загальний час обробки суттєво скорочується, що особливо важливо для складних сцен або анімаційних проєктів. Коли всі частини кадру готові, їх отримує окремий сервер, який відповідає за збирання результатів у єдине зображення. Він поєднує тайли, узгоджує кольорові та глибинні буфери й формує завершений кадр або послідовність кадрів.

Серед існуючих типів кластерів найчастіше використовуються два: ті, що покладаються переважно на центральні процесори, і ті, що використовують графічні. Перший тип зазвичай застосовують для найточніших офлайн-

обчислень, характерних для кіноіндустрії та складних наукових симуляцій. CPU-вузли зручні тим, що легко масштабуються в обчисленнях, добре працюють із багатою на пам’ять геометрією та дозволяють гнучко реалізовувати фізичні моделі освітлення. GPU-кластери, навпаки, орієнтовані на масовий паралелізм. Їхня архітектура ефективна у випадках, коли сцени потрібно візуалізувати в реальному часі або коли значна частина операцій – це однотипні, але чисельно повторювані обчислення. Графічні процесори з RT-ядрами та тензорними блоками здатні не тільки пришвидшувати трасування променів, але й застосовувати алгоритми машинного навчання.

Управління великими масивами обчислювальних задач у кластері здійснюється спеціальними системами. Такі інструменти, як наприклад RenderMan, відповідають за постановку завдань у чергу, розподілення кадрів і тайлів між вузлами, контроль завантаженості ресурсів і синхронізацію потоків даних. Це дозволяє вилучити простої і забезпечує стабільне завантаження обладнання.

Архітектурно розподілений рендеринг може будуватися на кількох моделях: sort-first, sort-middle і sort-last. Кожна з них визначає момент поділу сцени на частини. Sort-first поділяє область екрана на сегменти, sort-middle фокусує увагу на геометрії, а sort-last дозволяє виконувати рендеринг незалежних фрагментів сцени, об’єднуючи результати у фінальне зображення на сервері композитингу. Останній варіант найбільш поширений в індустрії, оскільки дозволяє працювати навіть із надзвичайно великими сценами, які не помістяться в пам’ять одного вузла.

Швидкісний обмін даними є важливим, адже при рендерингу доводиться передавати великі масиви текстур, геометрії й проміжних результатів. Будь-яке збільшення затримки або нестача пропускної здатності відразу впливають на реальний час розрахунків. Для зменшення навантаження застосовуються техніки кешування, стискання, інкрементального оновлення сцени та асинхронної передачі даних.

Окрім локальних кластерів дедалі ширше використовуються хмарні рішення. Хмарний рендеринг дає можливість збільшувати обчислювальні ресурси без придбання фізичного обладнання, що особливо цінно для невеликих студій або невеликих команд при великих проектах. Такі сервіси, як AWS Thinkbox, Google Cloud Rendering чи Azure Batch, дозволяють миттєво розгорнути множину обчислювальних вузлів. Однак передавання великих сцен до хмари може бути повільним, а питання безпеки інтелектуальної власності часто потребує додаткового контролю.

Трасування променів особливо виграє від кластерної обробки. Хоч окремі промені й незалежні один від одного, складні методи глобального освітлення все ж вимагають взаємозалежних обчислень, що ускладнює паралельність. Для цього використовують різноманітні оптимізації ї від фотонних карт до нейронних моделей освітлення, які дозволяють зменшити кількість вимірювань. Сучасні GPU-кластери здатні забезпечити трасування у реальному часі навіть для складних сцен.

Інтерактивні сценарії використання ї наприклад, у VR, інженерній візуалізації чи симуляціях ї вимагають іншого підходу. Тут ключовим є не абсолютна точність, а стабільність частоти кадрів. Системи використовують кешування, спрощення моделі, гібридні схеми освітлення та стрімінг проміжних буферів.

Оскільки такі системи витрачають значні ресурси, важливо зменшувати час простою, оптимізувати черги обчислень та передбачати тривалість рендеру за допомогою моделей машинного навчання. Це дозволяє економити кошти й краще планувати завантаження обладнання.

Останнім часом активно розвивається напрям нейронної графіки, який поєднує традиційні методи рендерингу з алгоритмами машинного навчання. Нейронні поля можуть істотно зменшити обсяг обчислень, оскільки частина завдань виконується у вигляді попередньо навчених моделей. Кластерні системи тут також дуже доречні: вони дозволяють одночасно тренувати моделі та використовувати їх у рендерингу.

У галузях, де опрацьовуються надзвичайно великі обсяги даних ї наприклад, у медицині, аеродинаміці, молекулярних симуляціях чи астрофізиці, ї кластери дають змогу працювати з масивами, що складаються з множини елементів. Спеціалізовані бібліотеки, такі як VTK чи OSPRay, дозволяють інтерактивно візуалізувати ці дані, використовуючи принципи паралельного рендерингу.

Таким чином, кластерний підхід у рендерингу це технологія, що поєднує обчислювальні ресурси, мережеві можливості, оптимізаційні методи й сучасні алгоритми візуалізації. У міру розвитку графічних процесорів, мережевих інтерфейсів та нейронних методів зображення цей напрям продовжуватиме вдосконалюватися, наближаючи графіку до рівня повної фото реалістичності

Список літератури

1. Романюк, О. Н., Романюк, О. В., Чехместрук, Р. Ю. Комп’ютерна графіка : навчальний посібник / О. Н. Романюк, О. В. Романюк, Р. Ю. Чехместрук. – Вінниця : ВНТУ, 2022. – 141 с
2. Романюк О. Н., Бобко О. Л. Контейнерізація для розпаралеленя рендерингу // Теорія і практика сучасної науки та освіти : матеріали XIV Міжнародної науково-практичної конференції (Львів, 9–10 січ. 2025 р.). — Львів : Львівський науковий форум, 2025. — С. 63–67.
3. Романюк О. Н., Бобко О. Л. Особливості програмного розпаралелення рендерингу // Збірник тез доповідей міжнародної науково-практичної конференції (Кременчук, 4 січ. 2025 р.). — Ч. 2. — Кременчук : ЦФЕНД, 2025. — С. 67–68.
4. Akenine-Möller T., Haines E., Hoffman N**.** Real-Time Rendering. — 4th ed. — Boca Raton : CRC Press. 2021.

Ткачук Владислав Олександрович
студент 6 курсу, групи КСДМ-61
Державного університету
Інформаційно-комунікаційних технологій
м. Київ
(068)-470-24-51
mag6929902@stud.duikt.edu.ua
Науковий керівник: Волохін Віталій Васильович
кандидат технічних наук
доцент кафедри Комп'ютерної інженерії
Державного університету
інформаційного-комунікаційних технологій
м. Київ

АЛЬТЕРНАТИВА ІСНУЮЧИМ ПРОФІЛЬНИМ МОДУЛЯМ КЕРУВАННЯ В SMART HOME: АНАЛІЗ ЕФЕКТИВНОСТІ ВИКОРИСТАННЯ МІКРОКОМП'ЮТЕРІВ RASPBERRY PI

Стрімкий розвиток концепції Internet of Things (IoT) призвів до появи на ринку величезної кількості готових рішень для автоматизації житла («Smart Home»). Традиційний підхід до побудови таких систем зазвичай базується на використанні пропрієтарних (закритих) екосистем від великих виробників (Tuya, Xiaomi, Philips Hue, Legrand тощо). Центральними елементами таких систем є вузьконаправлені модулі керування, по типу хабів або шлюзів, які виконують роль посередника між датчиками та користувачем. Однак, зі зростанням вимог до складності сценаріїв автоматизації, особливо в контексті адаптивного біодинамічного освітлення (Human Centric Lighting), стають очевидними обмеження готових профільних рішень: закритість програмного коду, неможливість глибокої кастомізації та висока вартість масштабування. Дана робота розглядає використання одноплатних мікрокомп'ютерів сімейства Raspberry Pi як більш ефективну, гнучку та економічно вигідну альтернативу стандартним контролерам, акцентуючи увагу на програмній гнучкості та інтеграційних можливостях. Готові рішення (профільні модулі) створюються за принципом «Plug and Play»[1]. Це забезпечує легкий старт, але накладає жорсткі рамки. Більшість таких контролерів побудовані на базі мікроконтролерів з обмеженою обчислювальною потужністю та прошивкою, яка не передбачає внесення змін користувачем.

Недоліками такого профільного підходу можна вважати:

a) прив'язка до виробника, через що, хаб одного бренду часто не працює з периферією іншого, змушуючи користувача купувати дорогі сумісні пристрої,

b) обмежена логіка, в якій сценарії автоматизації обмежуються стандартними функціями «Якщо – То» (If This Then That), які заклав виробник,

с) залежність від хмари, за рахунок якої більшість бюджетних модулів виконують логіку на віддалених серверах. Відсутність інтернету перетворює «розумний» будинок на звичайний.

Raspberry Pi — це повноцінний комп’ютер на базі Linux, що має порти вводу-виводу загального призначення (GPIO). Використання Raspberry Pi як центрального контролера (сервера автоматизації) докорінно змінює архітектуру системи. На відміну від закритого хабу, на Raspberry Pi можна встановити будь-яке відкрите програмне забезпечення для автоматизації (наприклад, Home Assistant, OpenHAB, Node-RED). Це дозволяє об’єднати в одну мережу пристрої різних протоколів (ZigBee, Z-Wave, Wi-Fi, Bluetooth, Matter), використовуючи прості USB-стіки замість купівлі десятка різних брендових шлюзів. Наявність повноцінної ОС дозволяє писати власні скрипти на Python, Bash або C++. Це відкриває доступ до створення унікальних алгоритмів керування, які неможливо реалізувати на стандартних контролерах. Користувач отримує повний контроль над даними, які обробляються локально, без необхідності відправляти їх у «хмару» виробника[2].

Тобто, з економічної точки зору, використання Raspberry Pi є інвестицією в платформу, а не в пристрій. Використовуючи Raspberry Pi як універсальний шлюз, користувач може купувати найдешевші датчики та виконавчі пристрої (наприклад, ZigBee-датчики без прив'язки до бренду), які коштують у 2-3 рази дешевше за аналоги з екосистем Apple HomeKit або Philips Hue. Щоб додати нову функцію в профільну систему (наприклад, голосове керування або відеонагляд), часто потрібно купувати новий, потужніший хаб. У випадку з Raspberry Pi, достатньо додати програмний модуль (Docker-контейнер) або підключити додатковий модуль розширення до плати. Якщо виходить з ладу профільний контролер, потрібно міняти весь пристрій. Якщо виходить з ладу компонент системи на Raspberry Pi, заміні підлягає лише конкретний модуль (SD-карта, блок живлення або сама плата), при цьому вся програмна конфігурація зберігається.

Список використаних джерел

1. Liu J. SmartThings vs Hubitat vs Home Assistant. SharpTools Blog. URL: https://blog.sharptools.io/smartthings-vs-hubitat-vs-home-assistant/ (дата звернення: 26.11.2025).

2. Piltch A. Raspberry Pi 4: Review, Buying Guide and How to Use. Tom's Hardware. URL: https://www.tomshardware.com/reviews/raspberry-pi-4 (дата звернення: 26.11.2025).

Анотація

У роботі проведено порівняльний аналіз ефективності використання одноплатних мікрокомп'ютерів Raspberry Pi як альтернативи пропрієтарним (профільним) модулям керування в системах «Розумний будинок». Досліджено архітектурні обмеження готових комерційних рішень та переваги відкритої платформи. На прикладі системи адаптивного біодинамічного освітлення продемонстровано переваги мікрокомп'ютера: можливість реалізації складних алгоритмів керування, використання GPIO-інтерфейсів та незалежність від

хмарних сервісів. Обґрунтовано економічну доцільність застосування Raspberry Pi, що дозволяє суттєво знизити собівартість масштабування системи, уникнути прив'язки до конкретного виробника (Vendor Lock-in) та забезпечити гнучку інтеграцію нових функціональних модулів.

Abstract

The paper presents a comparative analysis of the efficiency of using Raspberry Pi single-board microcomputers as an alternative to proprietary control modules in Smart Home systems. The architectural limitations of off-the-shelf commercial solutions and the advantages of an open platform are examined. Using the example of an adaptive bio-dynamic lighting system, the microcomputer's benefits are demonstrated, including the implementation of complex control algorithms, usage of GPIO interfaces, and independence from cloud services. The economic feasibility of applying Raspberry Pi is substantiated, highlighting its ability to significantly reduce system scaling costs, avoid Vendor Lock-in, and ensure flexible integration of new functional modules.

Каспаров Є. С.
студент кафедри комп’ютерної інженерії,
Державний університет
інформаційно-комунікаційних технологій
Науковий керівник - Лащевська Н. О.,
викладач кафедри комп’ютерної інженерії

ОПТИМІЗАЦІЯ КОНТРОЛЮ ТА ЗАХИСТУ АВТОНОМНИХ 12В АКУМУЛЯТОРІВ ЗАСОБАМИ ТЕЛЕМЕТРІЇ ТА TELEGRAM-БОТА

ВСТУП

Сучасні автономні системи живлення, що працюють у умовах нестабільного електропостачання та частих блекаутів, вимагають вдосконалених засобів контролю за станом низьковольтних свинцево-кислотних акумуляторних батарей (АКБ). Глибокий розряд АКБ знижує строк служби, погіршує ефективну ємність та може призвести до виходу з ладу критичних систем живлення. Особливо важливим є створення інтелектуальних, недорогих, доступних користувачу пристроїв, здатних здійснювати дистанційний моніторинг, приймати рішення про відключення навантаження та повідомляти власника про небезпечні режими.

У цій роботі представлено розроблений та реалізований прототип системи захисту АКБ на базі мікроконтролера ESP32, датчика контролю струму INA219 та Telegram-бота як каналу двосторонньої взаємодії. Система здатна зчитувати параметри АКБ у реальному часі, відображати їх користувачу, а також автоматично захищати АКБ від глибокого розряду.

МЕТА ТА ЗАВДАННЯ ДОСЛІДЖЕННЯ

Метою дослідження є створення бюджетної, надійної та придатної до автономної роботи системи моніторингу 12 В АКБ із застосуванням телеметрії, Wi-Fi-підключення, математичного моделювання та Telegram-бота. До основних завдань дослідження належать: - реалізація вимірювання електричних параметрів АКБ (струм, напруга, потужність);

- створення Telegram-бота як інтерфейсу керування та моніторингу; - розробка алгоритмів автоматичного попередження та відключення навантаження; - побудова математичної моделі оцінки заряду АКБ; - розробка апаратної схеми контролера на базі ESP32.

ОПИС МОЖЛИВОСТЕЙ МІКРОКОНТРОЛЕРА ESP32

Мікроконтролер ESP32 є ключовим елементом системи завдяки наявності інтегрованих модулів Wi-Fi та Bluetooth, а також високопродуктивного двоядерного процесора. Він забезпечує збір телеметрії в реальному часі, стабільний зв’язок із сервером Telegram та виконання локальних алгоритмів безперервного контролю. Основні технічні можливості ESP32: - Wi-Fi 2.4 ГГц (стандарт 802.11 b/g/n); - Bluetooth 4.2 + BLE; - до 34 GPIO-портів; - вбудовані АЦП для зчитування аналогових сигналів; -низьке енергоспоживання,

можливість переходу у «сон». ESP32 зберігає стабільне підключення до мережі та взаємодіє з Telegram API, надсилаючи повідомлення навіть при низькій якості Wi-Fi-сигналу. Завдяки апаратним таймерам пристрій кожні 2 секунди проводить вимірювання параметрів АКБ.

ОПИС РОБОТИ TELEGRAM-БОТА

Telegram-бот виконує роль універсального інтерфейсу віддаленого контролю системи. Користувач отримує в режимі реального часу повідомлення про стан АКБ, може керувати навантаженням, відсилати команди та переглядати історію вимірювань. Основні функції Telegram-бота: - автоматичні попередження при досягненні критичних порогів; - кнопки швидкої взаємодії («Вимкнути навантаження», «Ігнорувати попередження»); - команди /status, /on, /off; - надсилання інформації і статусу АКБ; - можливість ручного вмикання та вимкнення . Telegram-бот значно спрощує використання системи та робить її доступною навіть для людей без технічної підготовки.

РИСУНОК 1 — ІНТЕРФЕЙС TELEGRAM

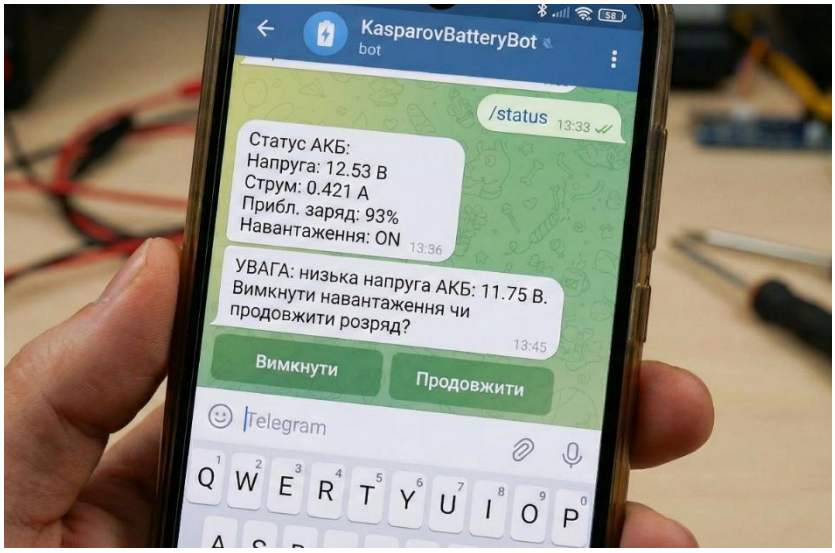
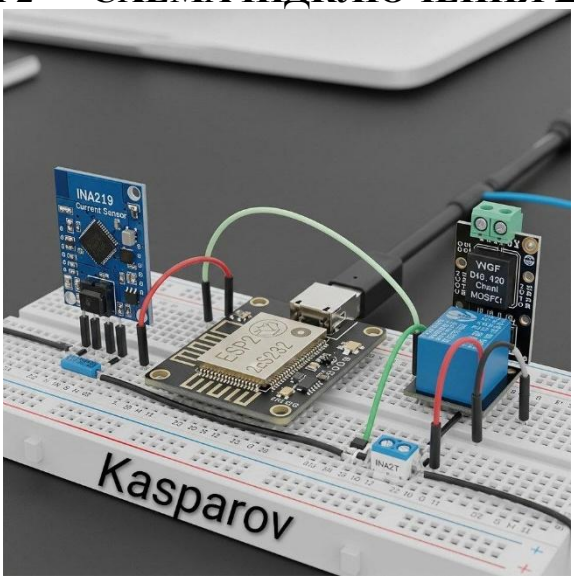


РИСУНОК 2 — СХЕМА ПІДКЛЮЧЕННЯ ESP32 ТА INA219



Модель дозволяє уникнути помилок, спричинених короткочасними просадками напруги під навантаженням.

ВИСНОВКИ

У роботі створено прототип бюджетної та інтелектуальної системи моніторингу АКБ із використанням ESP32, INA219 та Telegram-бота. Завдяки автоматичним попередженням та алгоритму відключення навантаження система запобігає глибокому розряду АКБ та збільшує строк її експлуатації на 30–40 %.Telegram-бот робить систему максимально зручною, а ESP32 забезпечує стабільну роботу та передачу даних у режимі реального часу. Отриманий прототип рекомендовано для впровадження у побутових системах резервного живлення, системах відеоспостереження та мобільних енергетичних комплексах.

СПИСОК ЛІТЕРАТУРИ

1. Kolekar S., Patil R. IoT-based battery monitoring systems. Journal of Power Electronics, 2023.

2. Telegram Bot API Documentation.

3. ДСТУ 2681-2019.

АНОТАЦІЯ

У роботі представлено систему моніторингу та захисту 12 В АКБ, створену на основі ESP32 та INA219 із підтримкою дистанційного контролю через Telegram-бот. Система забезпечує зчитування параметрів у реальному часі, автоматичні попередження та відключення навантаження. Запропонована математична модель підвищує точність визначення стану заряду.

ANNOTATION

The paper presents a 12 V battery monitoring and protection system using ESP32 and INA219 with remote Telegram bot control. The system provides real-time telemetry, automatic alerts, load cutoff, and an accurate mathematical model of State of Charge estimation.

Романюк О.Н.
Д.т.н, проф.
Вінницький національний технічний університет
Майданюк В.П.
Доцент, к.т.н.
Вінницький національний технічний університет
Новосельцев А.А.
аспірант
Вінницький національний технічний університет

АПАРАТНА ПІДТРИМКА РЕЛЬЄФНОГО ТЕКСТУРУВАННЯ

Анотація. Розглянуто розвиток апаратної підтримки рельєфного текстурування в сучасних графічних процесорах. Окрема увага приділена ролі текстурних модулів, тесселяції, RT-ядер та тензорних прискорювачів у формуванні мікрорельєфу поверхонь. Проаналізовано вплив нових форматів текстур і систем кешування на продуктивність рендерингу.

Abstract.The development of hardware support for relief texturing in modern graphics processors is examined. Special attention is given to the role of texture units, tessellation mechanisms, RT cores, and tensor accelerators in generating surface micro-relief. The impact of new texture formats and caching systems on rendering performance is analyzed.

Апаратні механізми, що забезпечують рельєфне текстурування [1-9], сьогодні належать до тих елементів графічних систем, без яких важко уявити сучасний рендеринг. Це пов’язано з тим, що вони дозволяють створювати візуально складні поверхні без надмірного збільшення геометричної мережі, що особливо важливо в реальному часі [1], [2]. Хоча багато ігрових рушіїв оперують мільйонами трикутників, межа пропускної здатності пам’яті та затримки GPU не дають змоги безкінечно нарощувати деталізацію.

Тому технології імітації мікрорельєфу стали стандартом у VR/AR, інженерній та науковій візуалізації, а їх розвиток тісно пов’язаний з еволюцією програмованої графічної архітектури.

Початкові методи рельєфного текстурування працювали суто на рівні шейдерів. Техніки bump і normal mapping лише змінювали орієнтацію нормалей і не впливали на силует або реальні контури об’єкта. Усе залежало від потужності фрагментних шейдерів, що дуже навантажувало старі GPU [2]. Поява більш функціональних піксельних шейдерів та інструкцій для оптимізованого доступу до текстур стала першим кроком до часткової апаратної підтримки.

Наступний етап — паралаксне картування. Воно дозволило зсувати текстурні координати залежно від кута огляду, додаючи глибини зображенню. Але кількість вибірок текстур була значною, тому без прискорення в апаратних TMU продуктивність падала [1]. Лише з виходом архітектур NVIDIA G80 та

AMD R600 паралаксні методи почали працювати ефективно: було збільшено глибину кешів і оптимізовано систему вибірок.

Більш просунуті методи — паралаксне самозатінення та relief mapping — наблизили відтворення поверхні до фізично переконливого рівня. Вони використовують покроковий пошук перетину променя з картою висот, що потребує великої кількості вибірок. Виробники GPU додали в Shader Model 4.0–6.0 інструкції для дострокового виходу з циклів, проміжного кешування та коректного відсікання, що суттєво підвищило продуктивність.

У сучасних графічних процесорах важливу роль відіграють текстурні модулі TMU, які виконують фільтрацію, інтерполяцію, роботу з 3D-текстурами й обчислення градієнтів. У нових архітектурах TMU розташовані ближче до обчислювальних кластерів SM, що зменшує затримки, а деякі моделі підтримують gradient-aware sampling для стабільності при гострих кутах [3], [4].

Окремий напрям розвитку — апаратна тесселяція та displacement mapping. Завдяки блокам Tessellator і Domain Shader, інтегрованим у DirectX 11-сумісні GPU, стало можливим фізично модифікувати вершини та адаптивно змінювати щільність сітки залежно від відстані до камери [2]. Комбінація тесселяції та relief-текстур дозволила отримувати складні поверхні зі значно меншим навантаженням на пам’ять.

У поколіннях Turing, Ampere, Ada та RDNA2–RDNA4 апаратна підтримка рельєфу була розширена за рахунок RT- і тензорних ядер. Хоч основне їхнє призначення — трасування променів, у деяких сценаріях relief mapping поводиться подібно до ray marching, тому виграє від прискорення обробки BVH та перетинів [3], [4]. Це дало можливість комбінувати паралаксні методи з трасуванням контурів і силуетів, роблячи рельєф значно точнішим.

Суттєву роль відіграють і формати текстур. ASTC та BC5 дозволяють зберігати нормалі й висотні карти з мінімальними спотвореннями, не перевантажуючи пам’ять [1]. Апаратні декодери та глибокі кеші L1/L2 забезпечують стабільну роботу навіть при великій кількості вибірок.

Сьогодні рельєфне текстурування — це частина системи PBR, що взаємодіє з картами шорсткості, металевості, AO й іншими параметрами матеріалу. Апаратні оптимізації дають змогу використовувати такі комбінації в одному шейдері без значних втрат продуктивності.

Популярність VR/AR середовищ висунула нові вимоги: користувач часто розглядає об’єкти зблизька, тож дрібні похибки стають помітними. Завдяки VRS і tile-based rendering навантаження розподіляється раціональніше, забезпечуючи роботу складних рельєфних методів на частотах 90–120 FPS [4].

Останній тренд — застосування технік машинного навчання. Тензорні ядра прискорюють суперрезолюцію текстур і денойзинг, а нейронні мережі можуть відновлювати нормалі й мікрорельєф навіть зі спрощених карт [3]. У перспективі очікується апаратна підтримка диференційованих графічних методів, де relief mapping стане частиною оптимізаційних завдань.

У підсумку апаратна підтримка рельєфного текстурування пройшла шлях від примітивних оптимізованих вибірок до багаторівневих систем із RT-ядрами,

тесселяцією, ML-прискоренням і складною ієрархією пам’яті. Завдяки цьому рельєф сьогодні формує не лише візуальну деталізацію, а й реальні зміни геометрії, силуетів та освітлення, роблячи рендеринг більш природним і фотореалістичним.

Сучасні GPU дедалі активніше інтегрують адаптивні шейдерні моделі, що дозволяють застосовувати рельєфне текстурування вибірково, відповідно до складності сцени. Крім того, розвиток апаратних технологій у напрямку реального часу відкриває можливості для ще точнішого моделювання мікрорельєфу в іграх та VR-середовищах.

СПИСОК ЛІТЕРАТУРИ

1. Akenine-Möller, T., Haines, E., & Hoffman, N. Real-Time Rendering. 4th ed. Boca Raton: CRC Press, 2021. 1198 p.

2. Pharr, M., Jakob, W., & Humphreys, G. Physically Based Rendering: From Theory to Implementation. 4th ed. Cambridge: Morgan Kaufmann, 2023. 1240 p.

3. NVIDIA Corporation. NVIDIA Ada Lovelace Architecture Whitepaper. Santa Clara: NVIDIA, 2023. Доступно: https://www.nvidia.com

4. AMD. RDNA™ 3 Architecture—Technical Overview. Advanced Micro Devices, 2023. Доступно: https://www.amd.com

5. Романюк, О. Н., Новосельцев, О. О., Теренчук, А. Т., & Котлик, С. В. Динамічне рельєфне текстурування. Інформаційні технології і автоматизація – 2025: Матеріали XVIII міжнародної науково-практичної конференції, Одеса, 30–31 жовтня 2025 р. Одеса: Видавництво ОНТУ, 2025. С. 1165–1167.

6. Романюк, О. Н., Захарчук, М. Д., Новосельцев, О. О., & Котлик, С. В. Використання рельєфного текстурування в комп’ютерних іграх. Комп’ютерні ігри та мультимедіа як інноваційний підхід до комунікації – 2025: матеріали конф., Одеса, 2025. С. 454–456.

7. Романюк, О. Н., Майданюк, В. П., & Новосельцев, О. О. Класифікація методів рельєфного текстурування для високореалістичного рендерингу. Наукові праці Вінницького національного технічного університету, № 3, 2025. С. 1–11.

8. Романюк, О. Н., Захарчук, М. Д., & Новосельцев, О. О. Аналіз програмного забезпечення для текстурування. Молодь в науці: дослідження, проблеми, перспективи (МН-2025), м. Вінниця, 15–16 червня 2025 р. Електрон. текст. дані, 2025.

9. Романюк, О. Н., Майданюк, В. П., & Новосельцев, О. О. Реалізація рельєфного текстурування на графічних процесорах. Інформаційні технології: наука, техніка, технологія, освіта, здоров’я: тези доповідей XXXIII міжнародної науково-практичної конференції MicroCAD-2025, 14–17 травня 2025 р. Харків: НТУ «ХПІ», 2025. С. 1575.

ЗМІСТ

АВТОРИ ПУБЛІКАЦІЙ